ID: 339375
Cookbook: browseurl.jbs
Time: 21:53:38
Date: 13/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

Copyright null 2021

Copyright null 2021

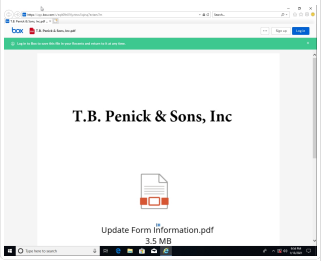
Analysis Report https://app.box.com/s/eqit09n816yvtnx…

Overview

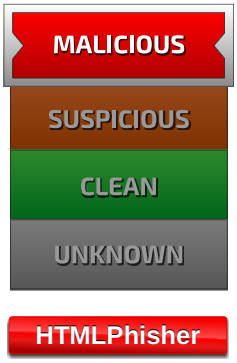
General Information

Sample URL:	http://https://app.box.com/s/eqit09n816yvtnxs1iqirsq7ectaev7m
Analysis ID:	339375

Most interesting Screenshot:



Detection

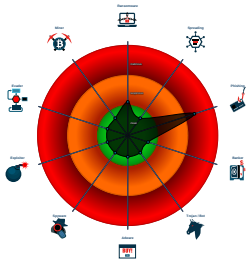


Score:	60
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Yara detected HtmlPhish_10
- Phishing site detected (based on log…
- HTML body contains low number of …
- HTML title does not match URL
- Invalid 'forgot password' link found

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 5696 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5612 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5696 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

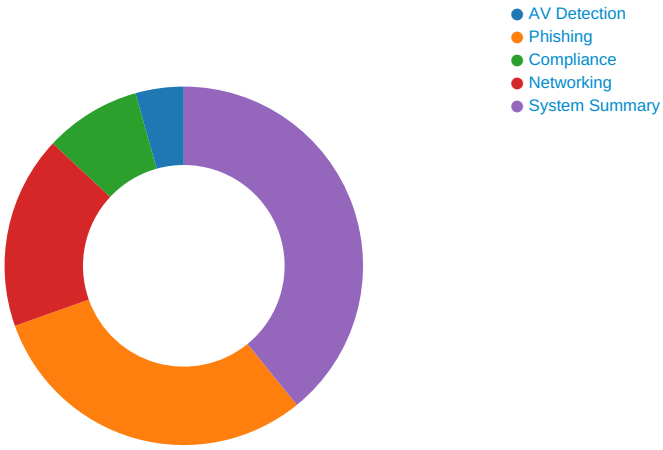
Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\Ortiz[1].htm	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Phishing:

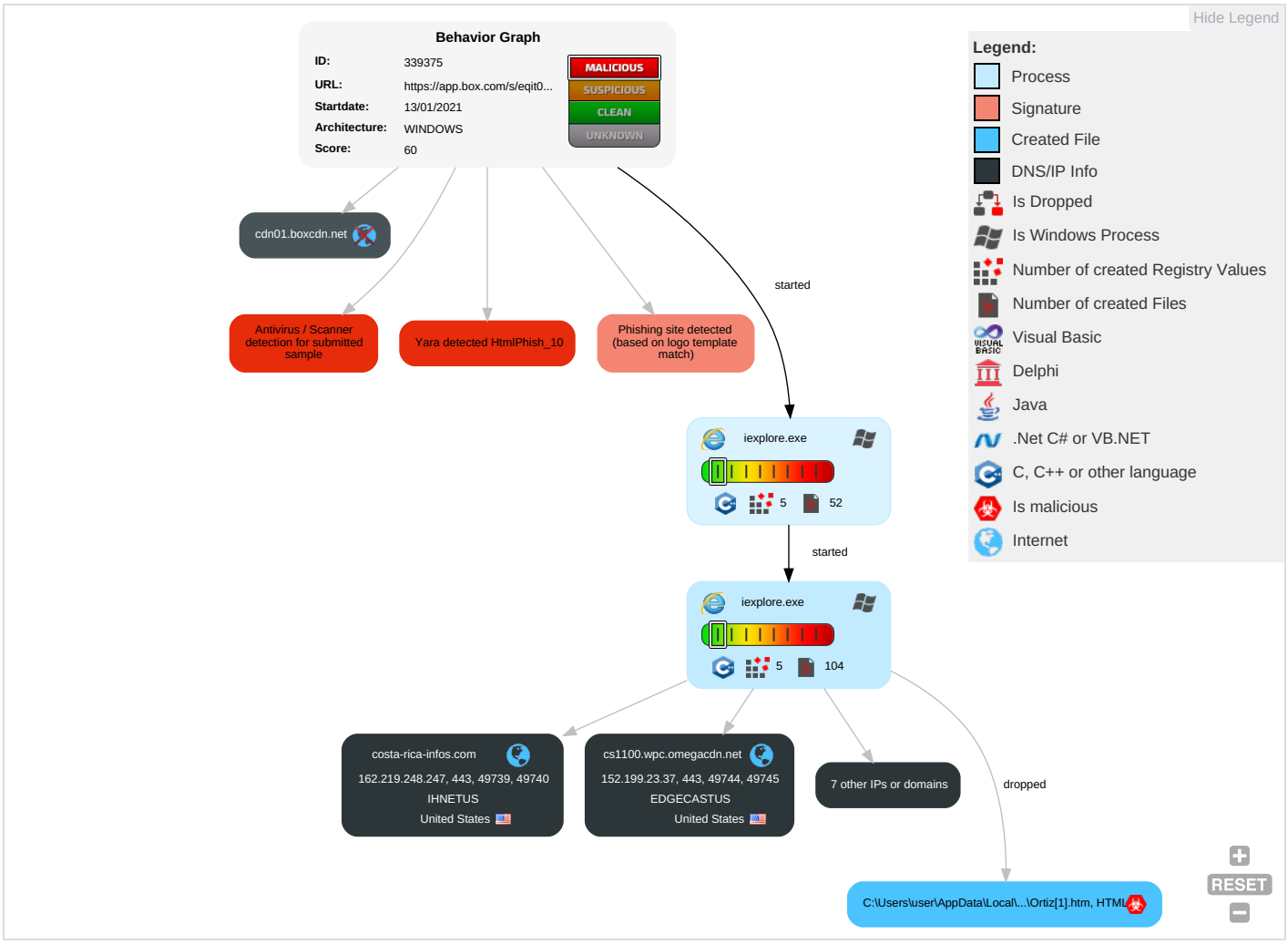
Yara detected HtmlPhish_10

Phishing site detected (based on logo template match)

Mitre Att&ck Matrix

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

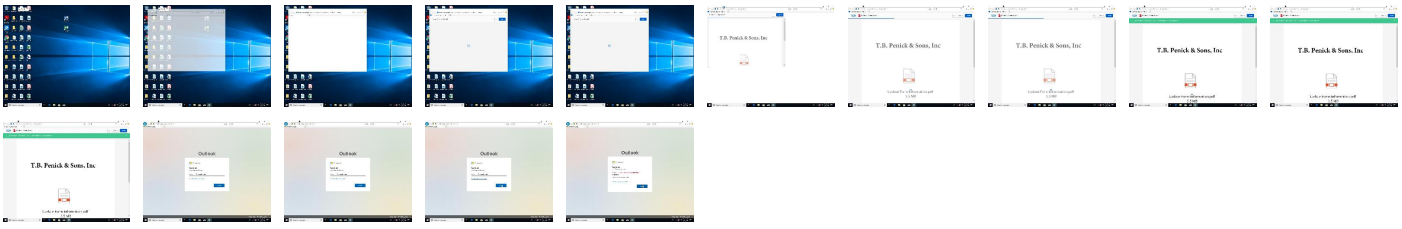
Behavior Graph

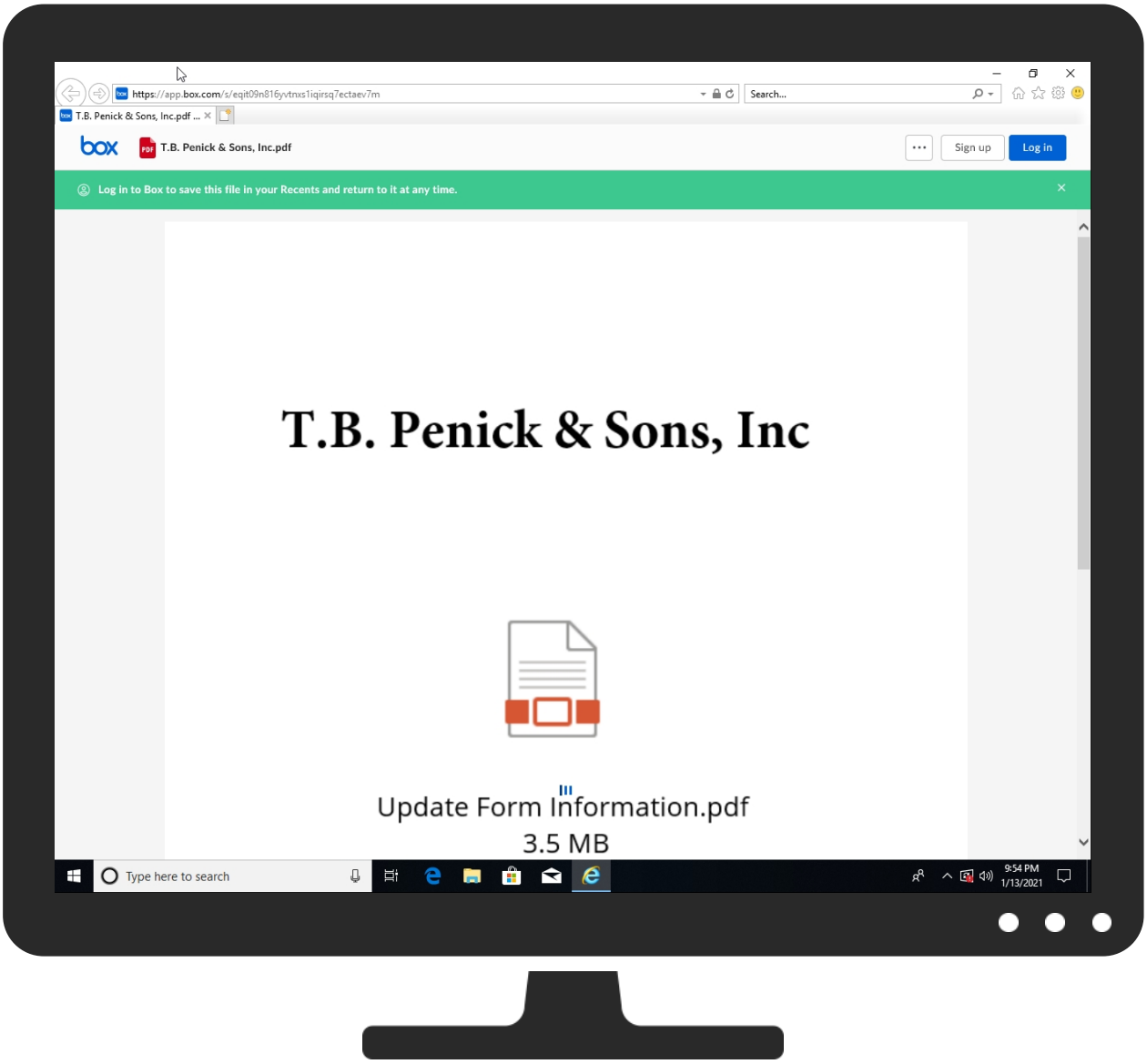


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://app.box.com/s/eqit09n816yvtnxs1iqirsq7ectaev7m	0%	Virustotal		Browse
http://https://app.box.com/s/eqit09n816yvtnxs1iqirsq7ectaev7m	0%	Avira URL Cloud	safe	
http://https://app.box.com/s/eqit09n816yvtnxs1iqirsq7ectaev7m	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
cs1100.wpc.omegacdn.net	0%	Virustotal		Browse
costa-rica-infos.com	0%	Virustotal		Browse
aadcdn.msftauth.net	0%	Virustotal		Browse
cdn01.boxcdn.net	0%	Virustotal		Browse

Copyright null 2021

URLs

Source	Detection	Scanner	Label	Link
http://https://aadcdn.msftauth.net/ests/2.1/content/images/picker_more_7568a43cf440757c55d2e7f51557ae1f.svg	0%	Avira URL Cloud	safe	
http://https://cdn01.boxcdn.net/_assets/img/favicons/notification-favicon-EHWWyP.ico	0%	Avira URL Cloud	safe	
http://https://app.box.ca-infos.com/Debbie/Ortiz/$Sign	0%	Avira URL Cloud	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/images/backgrounds/2_bc3d32a696895f78c19df6c717586a5d.s	0%	Avira URL Cloud	safe	
http://https://cdn01.boxcdn.net/fonts/1.0.2/lato/Lato-Regular.woff2)	0%	Avira URL Cloud	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/images/ellipsis_635a63d500a92a0b8497cdc58d0f66b1.svg	0%	Avira URL Cloud	safe	
http://https://costa-rica-infos.com/Debbie/Ortiz/q7ectaev7m	0%	Avira URL Cloud	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/images/picker_account_aad_9de70d1c5191d1852a0d5aac28b44	0%	Avira URL Cloud	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/images/arrow_left_a9cc2824ef3517b6c4160dcf8ff7d410.svg	0%	Avira URL Cloud	safe	
http://https://cdn01.boxcdn.net/_assets/img/favicons/browserconfig-fdBReK.xml	0%	Avira URL Cloud	safe	
http://https://cdn01.boxcdn.net/_assets/img/favicons/apple-touch-icon-57x57-fLlEpj.png	0%	Avira URL Cloud	safe	
http://https://cdn01.boxcdn.net/fonts/1.0.2/lato/Lato-Bold.woff2)	0%	Avira URL Cloud	safe	
http://https://cdn01.boxcdn.net/_assets/img/favicons/apple-touch-icon-144x144-va9pYs.png	0%	Avira URL Cloud	safe	
http://https://cdn01.boxcdn.net/_assets/img/favicons/apple-touch-icon-76x76-ZVGnRV.png	0%	Avira URL Cloud	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/images/microsoft_logo_ee5c8d9fb6248c938fd0dc19370e90bd.	0%	Avira URL Cloud	safe	
http://https://cdn01.boxcdn.net/_assets/img/favicons/notification-favicon-16x16-Ou5N87.png	0%	Avira URL Cloud	safe	
http://https://costa-rica-infos.com/Debbie/Ortiz/$Sign	0%	Avira URL Cloud	safe	
http://https://cdn01.boxcdn.net/enduser/app.8f4ad58129.css	0%	Avira URL Cloud	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/images/ellipsis_96f69d0cefd8a8ba623a182c351ccc64.png	0%	Avira URL Cloud	safe	
http://https://cdn01.boxcdn.net/_assets/img/favicons/android-chrome-192x192-96i97M.png	0%	Avira URL Cloud	safe	
http://jedwatson.github.io/classnames	0%	Avira URL Cloud	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/images/applogos/53_8b36337037cff88c3df203bb73d58e41.png	0%	Avira URL Cloud	safe	
http://https://cdn01.boxcdn.net/_assets/img/favicons/safari-pinned-tab-jyt2W4.svg	0%	Avira URL Cloud	safe	
http://https://cdn01.boxcdn.net/_assets/img/favicons/favicon-96x96-XU7UE1.png	0%	Avira URL Cloud	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico	0%	URL Reputation	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico	0%	URL Reputation	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico	0%	URL Reputation	safe	
http://https://cdn01.boxcdn.net/_assets/img/favicons/apple-touch-icon-152x152-r5tWgh.png	0%	Avira URL Cloud	safe	
http://https://cdn01.boxcdn.net/_assets/img/favicons/apple-touch-icon-60x60-Uv0qzu.png	0%	Avira URL Cloud	safe	
http://https://cdn01.boxcdn.net/_assets/img/favicons/apple-touch-icon-72x72-7aVqne.png	0%	Avira URL Cloud	safe	
http://https://cdn01.boxcdn.net/_assets/img/favicons/favicon-16x16-_kQSW4.png	0%	Avira URL Cloud	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico~	0%	URL Reputation	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico~	0%	URL Reputation	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico~	0%	URL Reputation	safe	
http://https://app.box.cRoot	0%	Avira URL Cloud	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico~(	0%	URL Reputation	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico~(	0%	URL Reputation	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico~(	0%	URL Reputation	safe	
http://https://costa-rica-infos.com/Debbie/Ortiz/#q7ectaev7m	0%	Avira URL Cloud	safe	
http://https://cdn01.boxcdn.net/fonts/1.0.2/lato/Lato-Bold.woff)	0%	Avira URL Cloud	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/images/ellipsis_grey_2b5d393db04a5e6e1f739cb266e65b4c.s	0%	Avira URL Cloud	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/images/picker_account_add_56e73414003cdb676008ff7857343	0%	Avira URL Cloud	safe	
http://https://app.box.c	0%	Avira URL Cloud	safe	
http://https://cdn01.boxcdn.net/fonts/1.0.2/lato/Lato-woff.css	0%	Avira URL Cloud	safe	
http://https://raincrosspub.com/Debbie/Ortiz/)	0%	Avira URL Cloud	safe	
http://https://cdn01.boxcdn.net/_assets/img/favicons/apple-touch-icon-114x114-busq-D.png	0%	Avira URL Cloud	safe	
http://https://cdn01.boxcdn.net/_assets/img/favicons/manifest-rw1AEP.json	0%	Avira URL Cloud	safe	
http://https://costa-rica-infos.com/Debbie/Ortiz/)	0%	Avira URL Cloud	safe	
http://https://cdn01.boxcdn.net/_assets/img/favicons/notification-favicon-96x96-TOQ9Kg.png	0%	Avira URL Cloud	safe	
http://https://cdn01.boxcdn.net/_assets/img/favicons/notification-favicon-32x32-brwW_W.png	0%	Avira URL Cloud	safe	

Copyright null 2021

Source	Detection	Scanner	Label	Link
http://https://cdn01.boxcdn.net/_assets/img/favicons/apple-touch-icon-120x120-K-u4U5.png	0%	Avira URL Cloud	safe	
http://https://costa-ricsta-rica-infos.com/Debbie/Ortiz/	0%	Avira URL Cloud	safe	
http://https://cdn01.boxcdn.net/fonts/1.0.2/lato/Lato-Regular.woff)	0%	Avira URL Cloud	safe	
http://https://cdn01.boxcdn.net/_assets/img/favicons/mstile-144x144-pllCM8.png	0%	Avira URL Cloud	safe	
http://https://cdn01.boxcdn.net/_assets/img/favicons/favicon-32x32-VwW37b.png	0%	Avira URL Cloud	safe	
http://www.box.com)	0%	Avira URL Cloud	safe	
http://https://cdn01.boxcdn.net/_assets/img/favicons/apple-touch-icon-180x180-tV001c.png	0%	Avira URL Cloud	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/images/ellipsis_grey_5bc252567ef56db648207d9c36a9d004.p	0%	Avira URL Cloud	safe	
http://https://cdn01.boxcdn.net/_assets/img/favicons/favicon-yz-tj-.ico	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cs1100.wpc.omegacdn.net	152.199.23.37	true	false	• 0%, Virustotal, Browse	unknown
api.box.com	185.235.236.197	true	false		high
public.boxcloud.com	185.235.236.200	true	false		high
cdnjs.cloudflare.com	104.16.18.94	true	false		high
app.box.com	185.235.236.201	true	false		high
costa-rica-infos.com	162.219.248.247	true	false	• 0%, Virustotal, Browse	unknown
code.jquery.com	unknown	unknown	false		high
aadcdn.msftauth.net	unknown	unknown	false	• 0%, Virustotal, Browse	unknown
cdn01.boxcdn.net	unknown	unknown	false	• 0%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://costa-rica-infos.com/Debbie/Ortiz/	true		unknown
http://https://app.box.com/s/eqit09n816yvtnxs1iqirsq7ectaev7m	false		high

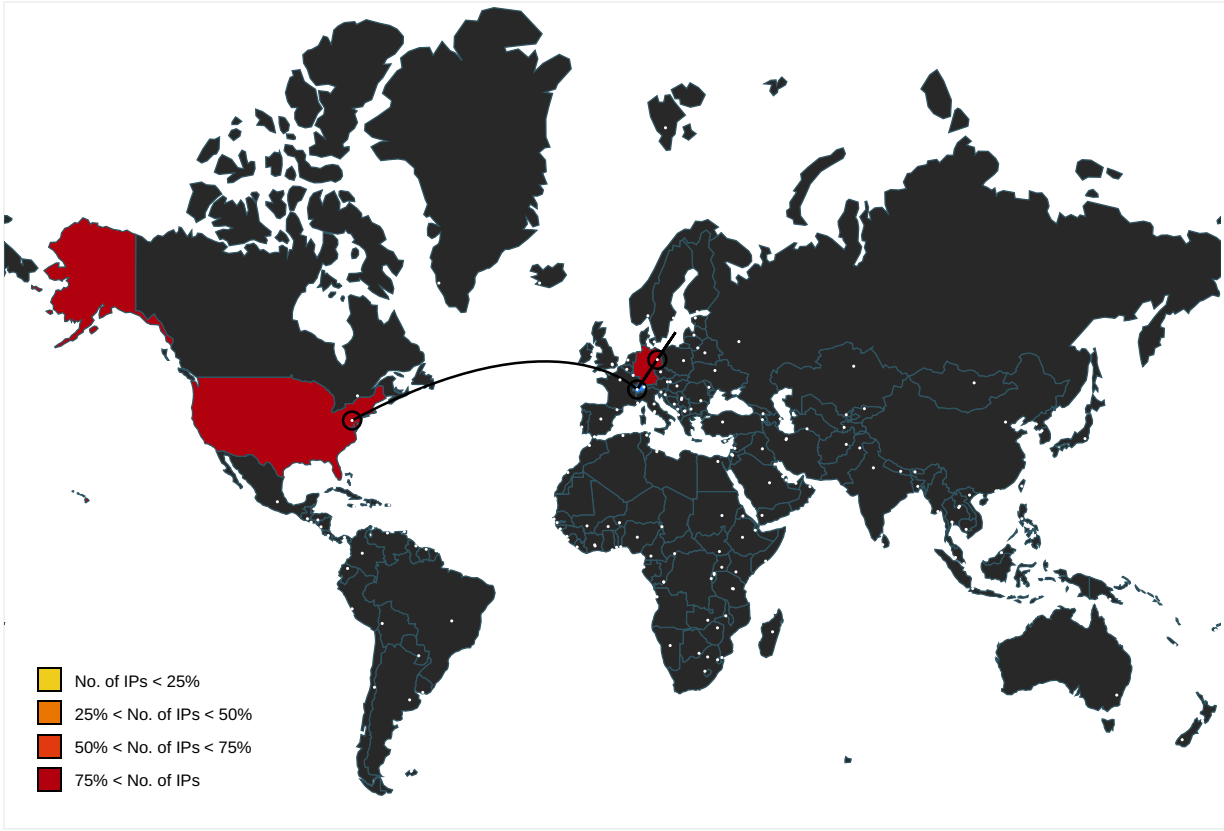
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://fontawesome.io	font-awesome[1].css.2.dr	false		high
http://https://aadcdn.msftauth.net/ests/2.1/content/images/picker_more_7568a43cf440757c55d2e7f51557ae1f.svg	Ortiz[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdn01.boxcdn.net/_assets/img/favicons/notification-favicon-EHWWyP.ico	eqit09n816yvtnxs1iqirsq7ectaev7m[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://github.com/zloirock/core-js	core.min[1].js.2.dr	false		high
http://https://app.box.ca-infos.com/Debbie/Ortiz/$Sign	{F6FBA45E-562C-11EB-90E6-ECF4BB82F7E0}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://app.box.cos.com/Debbie/Ortiz/q7ectaev7mRoot	{F6FBA45E-562C-11EB-90E6-ECF4BB82F7E0}.dat.1.dr	false		high
http://https://aadcdn.msftauth.net/ests/2.1/content/images/backgrounds/2_bc3d32a696895f78c19df6c717586a5d.s	Ortiz[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdn01.boxcdn.net/fonts/1.0.2/lato/Lato-Regular.woff2)	messagecenter~preview-components~uploads-manager-enduser.23ae1c6583[1].css.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://aadcdn.msftauth.net/ests/2.1/content/images/ellipsis_635a63d500a92a0b8497cdc58d0f66b1.svg	Ortiz[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://app.box.com/s/eqit09n816yvtnxs1iqirsq7ectaev7m	~DFF6C89A18730061FE.TMP.1.dr	false		high
http://https://costa-rica-infos.com/Debbie/Ortiz/q7ectaev7m	~DFF6C89A18730061FE.TMP.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://aadcdn.msftauth.net/ests/2.1/content/images/picker_account_aad_9de70d1c5191d1852a0d5aac28b44	Ortiz[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://app.box.com/s/eqit09n816yvtnxs1iqirsq7ectaev7mXT.B.	~DFF6C89A18730061FE.TMP.1.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://aadcdn.msftauth.net/ests/2.1/content/images/arrow_left_a9cc2824ef3517b6c4160dcf8ff7d410.svg	Ortiz[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdn01.boxcdn.net/_assets/img/favicons/browserconfig-fdBReK.xml	eqit09n816yvtnxs1iqirsq7ectaev7m[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://app.box.com/s/eqit09n816yvtnxs1iqirsq7ectaev7meqit09n816yvtnxs1iqirsq7ectaev7mRoot	{F6FBA45E-562C-11EB-90E6-ECF4BB82F7E0}.dat.1.dr	false		high
http://https://cdn01.boxcdn.net/_assets/img/favicons/apple-touch-icon-57x57-fLlEpj.png	eqit09n816yvtnxs1iqirsq7ectaev7m[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdn01.boxcdn.net/fonts/1.0.2/lato/Lato-Bold.woff2)	messagecenter~preview-components~uploads-manager-enduser.23ae1c6583[1].css.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdn01.boxcdn.net/_assets/img/favicons/apple-touch-icon-144x144-va9pYs.png	eqit09n816yvtnxs1iqirsq7ectaev7m[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdn01.boxcdn.net/_assets/img/favicons/apple-touch-icon-76x76-ZVGnRV.png	eqit09n816yvtnxs1iqirsq7ectaev7m[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://aadcdn.msftauth.net/ests/2.1/content/images/microsoft_logo_ee5c8d9fb6248c938fd0dc19370e90bd.	Ortiz[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdn01.boxcdn.net/_assets/img/favicons/notification-favicon-16x16-Ou5N87.png	eqit09n816yvtnxs1iqirsq7ectaev7m[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://costa-rica-infos.com/Debbie/Ortiz/$Sign	~DFF6C89A18730061FE.TMP.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdn01.boxcdn.net/enduser/app.8f4ad58129.css	eqit09n816yvtnxs1iqirsq7ectaev7m[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://aadcdn.msftauth.net/ests/2.1/content/images/ellipsis_96f69d0cefd8a8ba623a182c351ccc64.png	Ortiz[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdn01.boxcdn.net/_assets/img/favicons/android-chrome-192x192-96i97M.png	eqit09n816yvtnxs1iqirsq7ectaev7m[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://costa-rica-infos.com/Debbie/Ortiz/	~DFF6C89A18730061FE.TMP.1.dr	false		unknown
http://jedwatson.github.io/classnames	preview[1].js.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://aadcdn.msftauth.net/ests/2.1/content/images/applogos/53_8b36337037cff88c3df203bb73d58e41.png	Ortiz[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdn01.boxcdn.net/_assets/img/favicons/safari-pinned-tab-jyt2W4.svg	eqit09n816yvtnxs1iqirsq7ectaev7m[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdn01.boxcdn.net/_assets/img/favicons/favicon-96x96-XU7UE1.png	eqit09n816yvtnxs1iqirsq7ectaev7m[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdnjs.cloudflare.com/ajax/libs/font-awesome/4.7.0/css/font-awesome.css	Ortiz[1].htm.2.dr	false		high
http://https://aadcdn.msftauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico	imagestore.dat.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://cdn01.boxcdn.net/_assets/img/favicons/apple-touch-icon-152x152-r5tWgh.png	eqit09n816yvtnxs1iqirsq7ectaev7m[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdn01.boxcdn.net/_assets/img/favicons/apple-touch-icon-60x60-Uv0qzu.png	eqit09n816yvtnxs1iqirsq7ectaev7m[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://code.jquery.com/jquery-3.1.1.min.js	Ortiz[1].htm.2.dr	false		high
http://https://cdn01.boxcdn.net/_assets/img/favicons/apple-touch-icon-72x72-7aVqne.png	eqit09n816yvtnxs1iqirsq7ectaev7m[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdn01.boxcdn.net/_assets/img/favicons/favicon-16x16-_kQSW4.png	eqit09n816yvtnxs1iqirsq7ectaev7m[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://aadcdn.msftauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico~	imagestore.dat.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://app.box.cRoot	{F6FBA45E-562C-11EB-90E6-ECF4BB82F7E0}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://app.box.cos.com/Debbie/Ortiz/#q7ectaev7mRoot	{F6FBA45E-562C-11EB-90E6-ECF4BB82F7E0}.dat.1.dr	false		high
http://https://aadcdn.msftauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico~(	imagestore.dat.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://costa-rica-infos.com/Debbie/Ortiz/#q7ectaev7m	~DFF6C89A18730061FE.TMP.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdn01.boxcdn.net/fonts/1.0.2/lato/Lato-Bold.woff)	messagecenter~preview-components~uploads-manager-enduser.23ae1c6583[1].css.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://aadcdn.msftauth.net/ests/2.1/content/images/ellipsis_grey_2b5d393db04a5e6e1f739cb266e65b4c.s	Ortiz[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://fontawesome.io/license	font-awesome[1].css.2.dr	false		high
http://https://aadcdn.msftauth.net/ests/2.1/content/images/picker_account_add_56e73414003cdb676008ff7857343	Ortiz[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://app.box.com/s/eqit09n816yvtnxs1iqirsq7ectaev7mRoot	{F6FBA45E-562C-11EB-90E6-ECF4BB82F7E0}.dat.1.dr	false		high
http://blog.stevenlevithan.com/archives/parseuri	preview[1].js.2.dr	false		high
http://https://app.box.c	{F6FBA45E-562C-11EB-90E6-ECF4BB82F7E0}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://feross.org	preview[1].js.2.dr	false		high
http://https://github.com/derek-watson/jsUri	preview[1].js.2.dr	false		high
http://https://cdn01.boxcdn.net/fonts/1.0.2/lato/Lato-woff.css	eqit09n816yvtnxs1iqirsq7ectaev7m[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://raincrosspub.com/Debbie/Ortiz/)	T.B.%20Penick%20&%20Sons,%20Inc[1].pdf.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://support.box.com	preview[1].js.2.dr	false		high
http://https://cdn01.boxcdn.net/_assets/img/favicons/apple-touch-icon-114x114-busq-D.png	eqit09n816yvtnxs1iqirsq7ectaev7m[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdn01.boxcdn.net/_assets/img/favicons/manifest-rw1AEP.json	eqit09n816yvtnxs1iqirsq7ectaev7m[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://costa-rica-infos.com/Debbie/Ortiz/)	T.B.%20Penick%20&%20Sons,%20Inc[1].pdf.2.dr	false	• Avira URL Cloud: safe	unknown
http://rock.mit-license.org	core.min[1].js.2.dr	false		high
http://https://cdn01.boxcdn.net/_assets/img/favicons/notification-favicon-96x96-TOQ9Kg.png	eqit09n816yvtnxs1iqirsq7ectaev7m[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdn01.boxcdn.net/_assets/img/favicons/notification-favicon-32x32-brwW_W.png	eqit09n816yvtnxs1iqirsq7ectaev7m[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdn01.boxcdn.net/_assets/img/favicons/apple-touch-icon-120x120-K-u4U5.png	eqit09n816yvtnxs1iqirsq7ectaev7m[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://costa-ricsta-rica-infos.com/Debbie/Ortiz/	{F6FBA45E-562C-11EB-90E6-ECF4BB82F7E0}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdn01.boxcdn.net/fonts/1.0.2/lato/Lato-Regular.woff)	messagecenter~preview-components~uploads-manager-enduser.23ae1c6583[1].css.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdn01.boxcdn.net/_assets/img/favicons/mstile-144x144-pllCM8.png	eqit09n816yvtnxs1iqirsq7ectaev7m[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdn01.boxcdn.net/_assets/img/favicons/favicon-32x32-VwW37b.png	imagestore.dat.2.dr, eqit09n816yvtnxs1iqirsq7ectaev7m[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://www.box.com)	preview[1].js.2.dr	false	• Avira URL Cloud: safe	low
http://https://cdn01.boxcdn.net/_assets/img/favicons/apple-touch-icon-180x180-tV001c.png	eqit09n816yvtnxs1iqirsq7ectaev7m[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://aadcdn.msftauth.net/ests/2.1/content/images/ellipsis_grey_5bc252567ef56db648207d9c36a9d004.p	Ortiz[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdn01.boxcdn.net/_assets/img/favicons/favicon-yz-tj-.ico	eqit09n816yvtnxs1iqirsq7ectaev7m[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.235.236.200	unknown	Germany		33011	BOXNETUS	false
185.235.236.197	unknown	Germany		33011	BOXNETUS	false
185.235.236.201	unknown	Germany		33011	BOXNETUS	false
152.199.23.37	unknown	United States		15133	EDGECASTUS	false
104.16.18.94	unknown	United States		13335	CLOUDFLARENETUS	false
162.219.248.247	unknown	United States		33494	IHNETUS	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	339375
Start date:	13.01.2021
Start time:	21:53:38
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 30s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://app.box.com/s/eqit09n816yvtnxs1iqirsq7ectaev7m
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:	16
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

Copyright null 2021

Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal60.phis.win@3/71@9/6
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browsing link: https://costa-rica-infos.com/Debbie/Ortiz/
Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, ielowutil.exe, SgrmBroker.exe, backgroundTaskHost.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 40.88.32.150, 104.43.139.144, 88.221.62.148, 104.18.103.56, 104.16.74.20, 13.88.21.125, 23.210.248.85, 209.197.3.24, 51.132.208.181, 152.199.19.161, 92.122.213.194, 92.122.213.247, 8.248.135.254, 67.26.73.254, 67.27.158.254, 67.26.75.254, 67.27.233.254, 2.20.142.209, 2.20.142.210, 51.103.5.186, 51.104.139.180, 52.155.217.156 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, cds.s5x3j6q5.hwcdn.net, arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, wns.notify.windows.com.akadns.net, arc.msn.com, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcoleus15.cloudapp.net, par02p.wns.notify.windows.com.akadns.net, go.microsoft.com, emea1.notify.windows.com.akadns.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, auto.au.download.windowsupdate.com.c.footprint.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, fs.microsoft.com, ie9comview.vo.msecnd.net, displaycatalog.md.mp.microsoft.com.akadns.net, aadcdnoriginneu.azureedge.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.net, aadcdnoriginneu.ec.azureedge.net, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, cdn01.boxcdn.net.cdn.cloudflare.net, skypedataprdcolwus15.cloudapp.net, cs9.wpc.v0cdn.net • Report size getting too big, too many NtCreateFile calls found. • Report size getting too big, too many NtDeviceIoControlFile calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\T8DRMTJ1\app.box[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):	2068
Entropy (8bit):	5.034734471390268
Encrypted:	false
SSDEEP:	48:0YvES8OMEaNOMEaNOMEaNOMEaNOQSoMEaNOMEatMEatGMEatVMEatLMEatLl:fz8OEOEOEOEO3oEOwwGwVwLwLl
MD5:	248C797A0BD7D6267D71DD1AAD3FBCB6
SHA1:	EB8B098EC8B393BB66695087B187CA85026DB181
SHA-256:	76403BEF97CFA888921CBFD21227EE658FCFD153B2B00907B0FDB62B98C0FD8F
SHA-512:	656CCF604913482425E29DA0B2C0948776310EA61C95600ED56AFE7B3AA21691E260B3F62F0E8F76A226798651AC2BB1020B82939A90C78732138A79A93C5459
Malicious:	false
Reputation:	low
Preview:	<root></root><root></root><root><item name="key" value="value" ltime="3145836224" htime="30861881" /></root><root></root><root></root><root></root><root><item name="localStore/0/TestKey" value="testValue" ltime="3179106224" htime="30861881" /></root><root><item name="localStore/0/bcu-uploads-reachability-cached-results" value="{}" ltime="3179106224" htime="30861881" /></root><root><item name="localStore/0/bcu-uploads-reachability-cached-results" value="{}" ltime="3179106224" htime="30861881" /></root><root><item name="localStore/0/bcu-uploads-reachability-cached-results" value="{}" ltime="3179106224" htime="30861881" /></root><root><item name="localStore/0/bcu-uploads-reachability-cached-results" value="{}" ltime="3179106224" htime="30861881" /><item name="localStore/0/TestKey" value="testValue" ltime="3213506224" htime="30861881" /></root><root><item name="localStore/0/bcu-uploads-reachability-cached-results" value="{}" ltime="3179106224" htime="30861881" /></root><root><item name="lo

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{F6FBA45C-562C-11EB-90E6-ECF4BB82F7E0}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8601028840668317
Encrypted:	false
SSDEEP:	192:rgZzZf2o9WEtpifhSIzMIgBZGD7sfoS1jX:rQVOoUQGgdamh
MD5:	0C03D465816B46F6F249A49305EA9A16
SHA1:	F6B431C343E5D1C4E6910BB25D8EAB8D1F03DC6B
SHA-256:	36861B48DE2CF980C6CCE07185F09FA16023D7626D6AB66520D0A66001C6A94D
SHA-512:	971687176328FDB98A62DAC62B0E1CAE895DC415D5FB2309168FBA30C7FB66FE8A1ADCC85F7B2B1BEDD9CB89F11B741695DE83064979435C51580F168701156
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\{F6FBA45E-562C-11EB-90E6-ECF4BB82F7E0}.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\{F6FBA45E-562C-11EB-90E6-ECF4BB82F7E0}.dat	
Category:	modified
Size (bytes):	57720
Entropy (8bit):	2.1641429835997923
Encrypted:	false
SSDEEP:	384:raekYThQQEqQ1b1bY1gE19390gBgFBbpOom6orVRiDdQ:HQluLl+Do
MD5:	27787C20C8B039CDBC26E1CCD9E1918E
SHA1:	CF6227D4E985D50DA0754BBCE6C4D6516DF68D46
SHA-256:	982CEED61739C5A6E4CDE26A37BA96A966B5665226DB73E821046EA1CA781F28
SHA-512:	F79FBB2D482939988307CCEE2D11C03588165522264F49880F693E38BA6A8E90FB4E206B8CB8BDF7F565B49B8F4AFB564EB289881808DFAE27617543AFC42D37
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\{FE4053F8-562C-11EB-90E6-ECF4BB82F7E0}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5653879890518512
Encrypted:	false
SSDEEP:	48:IwvGcpr3GwpaOG4pQqGrapbS8rGQpKOlxG7HpRZsTGIpG:rlZhQu6cBS8FAOlgTZ4A
MD5:	38062DCCCAB8B8AFDF406C2AE5CE9D6E
SHA1:	E6014926BB3674A956BBE31C906BEE2A2484EA53
SHA-256:	2503B7F193EF93D2532559BF55B29EF201D7177227EF5251882083EF72C643A8
SHA-512:	521A09DD3FB5F43272B179EBD444AEDB203CA56B4AF3A6680071891350F19E17555BA9551E2DA724F28FAFA9DEFB4087649249D8B21E1F73BF7CF09B566CE8A
Malicious:	false
Reputation:	low
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\po60zt0\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	modified
Size (bytes):	19835
Entropy (8bit):	3.629036560960156
Encrypted:	false
SSDEEP:	48:1mF2C2djvA3bc9ENhkb7J5HKJ5AKJ5IKJ5Ygyyyyyyyyyyyyyyy IKJ5KvKJ5/QQQQc:kQvA3QENhkbtIjjgb9QQQQQ9
MD5:	BD0A00448C31C203EF015E7F7EE23827
SHA1:	EE9EFADBE0728A8F3BA9D3228F3CD3DA02F0389B
SHA-256:	47AA891372095DC862F8E5E90057F6FDA6C77DF956463B87B97C8497D132978B
SHA-512:	332C69E02DCF7CAD3925272BACB0E92D83CDFDC8C6418B2E6DCBA94E57E4350E1F0F39C0BD7EE5F168FE7F60C47BFC8F24C4A90207BC854E9C4C2D5CE51A902
Malicious:	false
Reputation:	low
Preview:	F.h.t.t.p.s.:././.c.d.n.0.1...b.o.x.c.d.n...n.e.t./._.a.s.s.e.t.s./.i.m.g./.f.a.v.i.c.o.n.s./.f.a.v.i.c.o.n.-.3.2.x.3.2.-.V.w.W.3.7.b...p.n.g.....PNG.....IHDR... ... .D.....gAMA.....a.....sRGB..... cHRM..z&.....u0...`.:....p..Q<....PLTE....a..a..a..a..a..a..a..a..a..a..a..a..a..a..a..a..a..a..a..a..a..a..a..a..a..a..a..a..a..a..a..a..a..`._.H..w...i...../~.....2..._.1~..d..n..`..m..f..c..a.....!u..^."u.....g...j.....q.E....G.....F.....g..{.....U.....A...h..r..... u..h.:.....e.....b...].j.....q.....}.....n.G.....b...d..v..r.. t....+{.i..z..\.....*z.....h..&x.@.....$w.c.....y.....a...n.D.....t.....a..p...j..%w.f...E...e..h.V.....=..Q..e../}...?...b..p.Y....tRNS... 78.-.....)..*...6...&..W.w....IDAT8.c```dbfa..X.....\.X.../.##.#;..N .. .!....10..S .. *.O..(.+7>...)...@V^AQ...%e.9..T..5d!f..bW.....#+#...."...T&.o.W`hdlbjfnaiemckg....,....&

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\Lato-Bold[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 118272, version 1.0
Category:	downloaded
Size (bytes):	118272
Entropy (8bit):	**7.99139950884202**
Encrypted:	**true**
SSDEEP:	3072:EweDun1n2Uub4GgrWSPqJWREerzJmXVVoYckqW0:jb9ubaiSiJ4zYVmYv0
MD5:	AEBA3FDF0CDB79BC1D33688D3E39B592

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\Lato-Bold[1].woff	
SHA1:	E3A34C01880116194309B7225A9CBF8001D23407
SHA-256:	2D198961EFB291734102AC4281C4E004628960C80B7C378DD8E034D4B7425AD2
SHA-512:	E9024FABDEEE3BCC345FE51E461E80A1F898EEB17B9561D7DC0BBA4D85F28AD485BCB9C140276534C30047A1D8D8C36AA3989D2C29276D00AA3186219EA2C291
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn01.boxcdn.net/fonts/1.0.2/lato/Lato-Bold.woff
Preview:	wOFF.....m.....FFTM.....p.\MGDEF.....7...8.}..GPOS.....>...GSUB.....,...FA..sOS/2...<...`...`kQ..cmap.....x.!>cvt ...x...o....B...fpgm..... ..gasp.....glyf.....K...<.head...(...2...6..qihhea...\...!...$....hmtx.....$KqKAloca.....(....maxp...x... ... .Q..name.....&.Bpost.....(.[rK.prep...T.....o.i:webf..... .....`.V.....=.....y.....x.c`d``..b...`b`e`dj..f.6.f.v.o.F...._.&.?.I...,`U..j%.H.x...|L....9.M...UQ..U.U..UQTmmT{]mUUQ.U\WUU-....%B..XJ.1FBD.dD"&R%.!T}~.93m.....x...3. .....B.Bx.ab.p.....{....N...h3n...p...R.....#n.x...Q..!..'....o.&<Dc.Rx..l#:.n...$..1b..$..9.x.x.!..zOQ{.C.78..*....K.{.C>\.!.t...~....99.!...\....Y...N~...6..E;t."z.~h7L..c.o".v.M.....:K..... ..b...;Z.r..h.'....a}...=.....m.A5....:G.g/....{*;...[G...A.....vo....{O.~....v..>.}.....s.../v_..}..f.....3..s.....W.W...p.....G.G{.N..<zy....1.....=....1

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\Lato-Regular[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 119132, version 1.0
Category:	downloaded
Size (bytes):	119132
Entropy (8bit):	**7.991532245734968**
Encrypted:	**true**
SSDEEP:	3072:pECjkMzGFzkgGdoAiZzixFwotRAE9urcBQbtF0roFS:pECjVzIGYZ4Fpx9urUQbtFeoFS
MD5:	3E4A4FC6317C4C2CF35D7C77EC1789C3
SHA1:	40EA0D8678B92988824193587F707E3AEDC4591F
SHA-256:	607EC0A4A29F6A4607F6E0A3CF486E50322DDF66F1F1870150CB69A7061E978D
SHA-512:	F7D639520F4C3A3539AD7506EC1CEBED8107C2A264316FE0E98A15132ACCFE6212A22391F4A7203B6D8304B3222B603F0137BA9ACAC7478F217363EEF4556DE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn01.boxcdn.net/fonts/1.0.2/lato/Lato-Regular.woff
Preview:	wOFF.....\.....FFTM.....p.\MGDEF.....7...8.x..GPOS.....z...b...GSUB...x...,...FA..sOS/2....._...`i...cmap.....x.!>cvt .....r....?9..fpgm...T..... ..gasp.....glyf.....a..?.head.....1...6..qfhhea.....!...$....hmtx.....C.2loca.....-&maxp..... ... .L..name.....hpost.....'....)prep.....o.i:webf...T... .....`.V.....=.....y.....x.c`d``..b...`b`e`dj..f.6.f.v.o.F...._.&.?.^.F...*..i..C.x...|M.....!.<.fEI.USS\TcVUTT.E.UUu.RUUWCM5W.U5....Ap".H"b.l.'!..j..g.....o_..Yg...z.z...Jv\..!<. .p..{_....cG.....h1..q.E'.B.!..!...I.s.....W.).T.....a.7QO4...x.-D[.Y....`1B....1M...1v...;E.D;..c.....b.....;.....v^..^...M..&.F.f...u.]Eo..$....7.Vi...&W9]..au}F].T....[>.t.....+..F j.X.^U...jzu}.._W...OS.....M.;.].k.fQ..../.K.h.f..\.vr..... ..#]G..s..:.u.k..\.E..]W..s...u..!.c..\3]s\.\.....r.....-.-..[...n....w.....n...p.....nS..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\Ortiz[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	116336
Entropy (8bit):	5.3816220537602755
Encrypted:	false
SSDEEP:	1536:Yhuhw+ExmazA/PWrF7qvEAFiQcpmNtuhPyJRp7xvnXE1Esns8lR:Yt4wyJjZnXE1Esns8H
MD5:	3752C84E2D4118729A264E7629A62E88
SHA1:	22C6C7C155B63E6F566BF554406A5F0780C3F800
SHA-256:	94860511EBE34294BA25E9D70248BA9855B1743CF7CB88796605494C130582D5
SHA-512:	BFCBFC34FD403CD7CBE119C697E1D71AF7F83E83C2BAD190852502C2CEC0669D117AAFB824BB0422667DAEC66D819F7FC40205AFB94C09CB4376572972CAE03
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_10, Description: Yara detected HtmlPhish_10, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\Ortiz[1].htm, Author: Joe Security
Reputation:	low
IE Cache URL:	http://https://costa-rica-infos.com/Debbie/Ortiz/
Preview:	<html dir="ltr" lang="en">.. <meta charset="utf-8">.. <link href="https://aadcdn.msftauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico" rel="shortcut icon">.. <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/font-awesome/4.7.0/css/font-awesome.css" integrity="sha256-NuCn4IvuZXdBaFKJOAcsU2Q3ZpwbdFisd5dux4jkQ5w=" crossorigin="anonymous">.. <style>... html{font-family:sans-serif;-ms-text-size-adjust:100%;-webkit-text-size-adjust:100%}body{margin:0}article,aside,details,figcaption,figure,footer,header,hgroup,main,menu,nav,section,summary{display:block}audio,canvas,progress,video{display:inline-block;vertical-align:baseline}audio:not([controls]){display:none;height:0}[hidden],template{display:none}a{background-color:transparent}a:active,a:hover{outline:0}abbr[title]{border-bottom:1px dotted}b,strong{font-weight:bold}dfn{font-style:italic}h1{font-size:2em;margin:.67em 0}mark{background:#ff0;color:#000}small{font-size:80%}sub,sup{font-size:75%

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\as-security~change-current-user-role-modal~collaborators~collection-detail-page~content-explorer-mod~244fdb54.62c4dbb45d[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):	41476
Entropy (8bit):	5.4953420117379155

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\as-security~change-current-user-role-modal~collaborators~collection-detail-page~content-explorer-mod~244fdb54.62c4dbb45d[1].js	
Encrypted:	false
SSDEEP:	384:D/CXDeUxEk4s4xb268LYhyqYvfGTW8QWoK7aHFIXZhq4f/RW94sPRugXhkUF5no7:DK6ls4xi6CcQ5SPq2iCBS3HTC
MD5:	2C4E0E745D87E29FA3168DCD5F24C8F0
SHA1:	64BA2ADC0283238AC85AAD12ACAB1178D72161D8
SHA-256:	64211F7C333CF4953DA868F56097DA1EEE6690F8C825C90D88852DDC89FBAAB2
SHA-512:	8062C78BA09A28C03BA98E8591F32F9716519B1D61197C2BC6708E4BC20264C4189ACECCC4B6DF96E867F6D65F856A889D7FCFEEE064AB5A1799FEA0374C475
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn01.boxcdn.net/enduser/as-security~change-current-user-role-modal~collaborators~collection-detail-page~content-explorer-mod~244fdb54.62c4dbb45d.js
Preview:	(window.webpackJsonp=window.webpackJsonp||[]).push([["as-security~change-current-user-role-modal~collaborators~collection-detail-page~content-explorer-mod~244fdb54","redux-form"],{"+2+ffwlNqK":function(t,e,n){"use strict";var r=n("0HdwK5vH5Z");e.__esModule=!0,e.default=function(t){if((!o&&0!==o||t)&&i.default){var e=document.createElement("div");e.style.position="absolute",e.style.top="-9999px",e.style.width="50px",e.style.height="50px",e.style.overflow="scroll",document.body.appendChild(e),o=e.offsetWidth-e.clientWidth,document.body.removeChild(e)}return o};var o,i=r(n("75K7zeGrYS"));t.exports=e.default},"+JPL/cuRJc":function(t,e,n){t.exports={default:n("+SFKZfGj63"),__esModule:!0}},"+SFKZfGj63":function(t,e,n){n("AUvmEmPtAX"),n("wgeUepA6S/"),n("adOz4zfAgb"),n("dl0quHMrQ4"),t.exports=n("WEpklf3dyC").Symbol},"+plKfkdWim":function(t,e,n){n("ApPDsGgrfM"),t.exports=n("WEpklf3dyC").Object.getPrototypeOf},"0HdwK5vH5Z":function(t,e){t.exports=function(t){return t&&t.__esModule?t:{default:t}}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\content[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, big-endian, direntries=5, xresolution=74, yresolution=82, resolutionunit=1], baseline, precision 8, 724x1024, frames 3
Category:	downloaded
Size (bytes):	45284
Entropy (8bit):	7.004577680285548
Encrypted:	false
SSDEEP:	768:FBSiCes1UAtC4gRJB0ni+3kiNOw/O7xLu720f:lCeGPq7Ctk2lgxLOFf
MD5:	D380903C7DBD5DD60A1A0B9B58EEE5CF
SHA1:	E622295ABEC0E5A0AB4F29EA08E360EF92F83BF4
SHA-256:	7F5DD8581F35873C861F85B91EE2F9B82C0CBAD80230AA5A1F00F1A7983174F1
SHA-512:	317F9EFD369B87EFD7CADB9CAEC2A1EF94C81515F0A74FC84B786FC64A8AC5B6AFC66B1B86AD420FB2A6AB02DA63A437023DFC20243AAB46289EE53DC71F4C93
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://public.boxcloud.com/api/2.0/internal_files/763455691544/versions/814624764367/representations/jpg_1024x1024/content/?access_token=1!97Twn8u3D91RqwQZUohppX6yb5-Xl8Bjdm7Mav-aBZY0vFki9CUxp0PFD8ETJWSNQv3j-LFhHnlWmAp0VDXKjd4ZYI_VSquQCYho5RhFH52j-zwhtQH_YuRdOeekOFacWv3Vn16CkBiEsnsFU7X8LMJcpDJndtbsq1Wj2q7ceyciNPyJ1RZtxRmMS-UciR7P_sYnMjB631sTkC2zXSuGzPpa5Am6Q7BDfA_Fip4pibQNv1ltkue-ZkOZCsYFIMVOmME_A6RjSYkMrRKnmZstdJ7F7kTow93CFxU06z3BQJNLOcR7cULvcPGqHGlDCm7JzdAZbj-qOA3BfYP9-k8yjDmXXGqd_nsVcLBJLO37bYBqSR7mKgvxQs_aF5CNQ_xoJxAB_mNWCkwwhBX_aT274plh7CoEQ2CPXdVqHAIjLMXwzmtMyeF5_wHGXPHsIAtH9ElyTKjq1-LUXWybr_ChD8RkJFHzgrmKodCuBnG_5khJtvKnyVIX7_0_OC0oNovo2s3NugzZDN4rSGv0M7Q-stWEkNe1bFO5GgmrKxavPC4LFJOWUc5Kv4Ti-mquFek.&shared_link=https%3A%2F%2Fapp.box.com%2Fs%2Feqit09n816yvtnxs1iqirsq7ectaev7m&box_client_name=box-content-preview&box_client_version=2.61.0
Preview:	......JFIF.............Exif..MM.*................J..........R.(......................i........Z............................0232..................9...........0100...............ASCII...pdfWidth:595.50pts,pdfHeight:842.25pts,numPages:1....C...C...b.......................!.1..."AQW.a.......#28UVqu......67BTbtv.35r...$%Rsw...&S.'(4CDEF....................................H.........................!1...AST..5Qr......"4a...26s..3R..BCb.....&...........?...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\favicon_a_eupayfgghqiai7k9sol6lg2[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 6 icons, 128x128, 16 colors, 72x72, 16 colors
Category:	downloaded
Size (bytes):	17174
Entropy (8bit):	2.9129715116732746
Encrypted:	false
SSDEEP:	24:QSNTmTFxg4lyyyyyyyyyyyyyio7eeeeeeeeekzgsLsLsLsLsLsQZp:nfgyyyyyyyyyyyyynzQQQQQO
MD5:	12E3DAC858061D088023B2BD48E2FA96
SHA1:	E08CE1A144ECEAE0C3C2EA7A9D6FBC5658F24CE5
SHA-256:	90CDAF487716184E4034000935C605D1633926D348116D198F355A98B8C6CD21
SHA-512:	C5030C55A855E7A9E20E22F4C70BF1E0F3C558A9B7D501CFAB6992AC2656AE5E41B050CCAC541EFA55F9603E0D349B247EB4912EE169D44044271789C719CD0
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://aadcdn.msftauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico
Preview:	.............h(..f...HH..........(..00......h....6.. ....=..............@.........(....A..(..................(.................................."P......................................"""""""""""""""""""""""""""""""" ...333333333333333333333333333333"""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\font-awesome[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	troff or preprocessor input, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	37414
Entropy (8bit):	4.82325822639402
Encrypted:	false
SSDEEP:	768:mmMtI+A4CSIDqvnI+YTBrFPvVrJjhiRAiiEL:mXtI+A4GDUI+Y9rpVljhiIEL
MD5:	C495654869785BC3DF60216616814AD1
SHA1:	0140952C64E3F2B74EF64E050F2FE86EAB6624C8
SHA-256:	36E0A7E08BEE65774168528938072C536437669C1B7458AC77976EC788E4439C
SHA-512:	E40F27C1D30E5AB4B3DB47C3B2373381489D50147C9623D853E5B299364FD65998F46E8E73B1E566FD79E97AA7B20354CD3C8C79F15372C147FED9C913FFB10
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdnjs.cloudflare.com/ajax/libs/font-awesome/4.7.0/css/font-awesome.css
Preview:	/*!. * Font Awesome 4.7.0 by @davegandy - http://fontawesome.io - @fontawesome. * License - http://fontawesome.io/license (Font: SIL OFL 1.1, CSS: MIT License). */./* FONT PATH. * ---------- */.@font-face {. font-family: 'FontAwesome';. src: url('../fonts/fontawesome-webfont.eot?v=4.7.0');. src: url('../fonts/fontawesome-webfont.eot?#iefix&v=4.7.0') format('embedded-opentype'), url('../fonts/fontawesome-webfont.woff2?v=4.7.0') format('woff2'), url('../fonts/fontawesome-webfont.woff?v=4.7.0') format('woff'), url('../fonts/fontawesome-webfont.ttf?v=4.7.0') format('truetype'), url('../fonts/fontawesome-webfont.svg?v=4.7.0#fontawesomeregular') format('svg');. font-weight: normal;. font-style: normal;.}..fa {. display: inline-block;. font: normal normal normal 14px/1 FontAwesome;. font-size: inherit;. text-rendering: auto;. -webkit-font-smoothing: antialiased;. -moz-osx-font-smoothing: grayscale;.}./* makes the font 33% larger relative to the icon container */..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\messagecenter~preview-components~uploads-manager-enduser.23ae1c6583[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):	532
Entropy (8bit):	4.880037129828671
Encrypted:	false
SSDEEP:	12:sUNV0yu7JGW7QtiXMGiJyhXMGiJMQdUEu3WrmXMGMhXMGO:sQCQACJyhCJrdl1mshu
MD5:	F2129188D79DCC9425F90ABCCC0B59A7
SHA1:	7E59C068211D195C19C91FE2581BB359FEA828B8
SHA-256:	CBB9726F5F3DCA04530F69D2B6C0B60B22E79BA8A0800167EA6AB365B19C95A0
SHA-512:	EE40B6383A6394FB528C77C90366412A8BC2BF3FD6AE688FDA33521185680EDFA2232C3EFBC4074DC555976A5DADACC44C6B411A0AFF767B5C67CBAD6E5B0B8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn01.boxcdn.net/enduser/messagecenter~preview-components~uploads-manager-enduser.23ae1c6583.css
Preview:	@font-face{font-weight:400;font-family:Lato;font-style:normal;src:local("Lato Regular"),local("Lato-Regular"),url(https://cdn01.boxcdn.net/fonts/1.0.2/lato/Lato-Regular.woff2) format("woff2"),url(https://cdn01.boxcdn.net/fonts/1.0.2/lato/Lato-Regular.woff) format("woff")}@font-face{font-weight:700;font-family:Lato;font-style:normal;src:local("Lato Bold"),local("Lato-Bold"),url(https://cdn01.boxcdn.net/fonts/1.0.2/lato/Lato-Bold.woff2) format("woff2"),url(https://cdn01.boxcdn.net/fonts/1.0.2/lato/Lato-Bold.woff) format("woff")}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\pdf_viewer.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	assembler source, ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	7106
Entropy (8bit):	4.86865545119897
Encrypted:	false
SSDEEP:	48:HBSkOWlpuR/cRez1Zw+jkRgHGZooZeRWLxZEzpuDdZfcd7Zq0w5FFw6VFM6oFKoB:hFjp+5jwLzjmQp4LgXzQuWZqzIoSF5
MD5:	8CE5E0CD4EE723D76683E50A1A3A6C6B
SHA1:	43D9D8CEECAA52C55735CBBF46DA3AE27146018D
SHA-256:	5179C456D56674CA0C710DBC43C90DDF2710C716779D53B94BF2A018F31154DA
SHA-512:	C364D2829CE09DD139D3906BE765AD5692EFCB06570CF774A19B8B66370B2FA1B0085FAC889594CF822A67F542BDC13F11514F9BE40F0910684C395C2142963C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn01.boxcdn.net/platform/preview/third-party/doc/2.16.0/pdf_viewer.min.css
Preview:	.textLayer{position:absolute;left:0;top:0;right:0;bottom:0;overflow:hidden;opacity:.2;line-height:1}.textLayer>span{color:transparent;position:absolute;white-space:pre;cursor:text;transform-origin:0 0}.textLayer .highlight{margin:-1px;padding:1px;background-color:#b400aa;border-radius:4px}.textLayer .highlight.begin{border-radius:4px 0 0 4px}.textLayer .highlight.end{border-radius:0 4px 4px 0}.textLayer .highlight.middle{border-radius:0}.textLayer .highlight.selected{background-color:#006400}.textLayer ::-moz-selection{background:#00f}.textLayer ::selection{background:#00f}.textLayer .endOfContent{display:block;position:absolute;left:0;top:100%;right:0;bottom:0;z-index:-1;cursor:default;-webkit-user-select:none;-moz-user-select:none;-ms-user-select:none;user-select:none}.textLayer .endOfContent.active{top:0}.annotationLayer section{position:absolute}.annotationLayer .buttonWidgetAnnotation.pushButton>a,.annotationLayer .linkAnnotation>a{position:absolute;font-size:1em;top:0;left:0;widt

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\preview-components~shared-file.036fa94865[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):	31106
Entropy (8bit):	5.404444723561215
Encrypted:	false
SSDEEP:	768:1j6foykcFKC/uRMQK9QZWTx7mA44c2d5YdVywTI:xgHiC/cu95To+c2dMTI
MD5:	81A4E9BF376814968ADA78905E39D8DB
SHA1:	7A30C05118B8723C66EF6E7F8F5A2A5116E0D374
SHA-256:	D9912016553DA753EE9624D8CDD0D689100550CF27A821E3508129EA54B28339
SHA-512:	5B06652F9569031D54060406C84D28D148FBC65F1B8C2468D27FCB48429C84BEC8D09F92CC39C0B832115F6F24B7D70D142A63C8A5F94DEEFA052065BDE258A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn01.boxcdn.net/enduser/preview-components~shared-file.036fa94865.js
Preview:	(window.webpackJsonp=window.webpackJsonp||[]).push([["preview-components~shared-file"],{"0pk5DGk/OM":function(e,t,n){"use strict";var o=n("/MKjzBatqn"),r=n("q9wI8Vu9Ou"),i=n("zXsyuZZv6G"),a=n("q1tIBJhxTW"),s=n("JRPeW/Ew/U"),l=(n("JPcvh7FMFD"),n("VzvVVBGVbW")),d=n("ZEDLez+ZlJ"),u=n("DtrrBg37C6"),c=n("BBtKKuFpIS"),p=n("1En/ASmD05"),f=n("0sbS2nMEFU"),w=n("wnhEk9N3Ty");function b(){return(b=Object.assign||function(e){for(var t=1;t<arguments.length;t++){var n=arguments[t];for(var o in n)Object.prototype.hasOwnProperty.call(n,o)&&(e[o]=n[o])}return e}).apply(this,arguments)}function v(e,t){if(null==e)return{};var n,o,r=function(e,t){if(null==e)return{};var n,o,r={},i=Object.keys(e);for(o=0;o<i.length;o++)n=i[o],t.indexOf(n)>=0||(r[n]=e[n]);return r}(e,t);if(Object.getOwnPropertySymbols){var i=Object.getOwnPropertySymbols(e);for(o=0;o<i.length;o++)n=i[o],t.indexOf(n)>=0||Object.prototype.propertyIsEnumerable.call(e,n)&&(r[n]=e[n])}return r}var h=function(e){var t=e.anonymousDownload,n=e.canDo

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\promise[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):	17766
Entropy (8bit):	5.2198826239136595
Encrypted:	false
SSDEEP:	384:SIwhnclwyn6OjSJ78IWrwOJ/ugy+GxMfF/jXBsvfKzyducywYMC9XD0APEi:4cuyU8JwJ3mtjXBMfPlE0AMi
MD5:	B669DFC7109AB90A425DB6A9349E92F5
SHA1:	0EF23DF3B07C637DB6DDF6766EFC8A2A528C1C0E
SHA-256:	977A170836C79F74599A27B28F7A487ABB29EBB5E50EB0CD303FB70617A1CE13
SHA-512:	8E924EA1878D4DAF827B9D1B2DC901AE9E4EF8C2FC4301FA732F2EBA1DD4E4E668EE76FA43B490A43917BFB7529C71D0BB6B9EAC5C569FBBCB08C6178CC6ECF8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn01.boxcdn.net/polyfills/core-js/2.5.3/es6/promise.js
Preview:	!function(t){function n(e){if(r[e])return r[e].exports;var o=r[e]={i:e,l:!1,exports:{}};return t[e].call(o.exports,o,o.exports,n),o.l=!0,o.exports}var r={};n.m=t,n.c=r,n.d=function(t,r,e){n.o(t,r)||Object.defineProperty(t,r,{configurable:!1,enumerable:!0,get:e})},n.n=function(t){var r=t&&t.__esModule?function(){return t.default}:function(){return t};return n.d(r,"a",r),r},n.o=function(t,n){return Object.prototype.hasOwnProperty.call(t,n)},n.p="",n(n.s=326)}({0:function(t,n,r){var e=r(1),o=r(8),i=r(10),c=r(12),u=r(13),s=function(t,n,r){var f,a,p,l,v=t&s.F,h=t&s.G,d=t&s.S,y=t&s.P,m=t&s.B,x=h?e:d?e[n]||(e[n]={}):(e[n]||{}).prototype,_=h?o:o[n]||(o[n]={}),g=_.prototype||(_.prototype={});h&&(r=n);for(f in r)a=!v&&x&&void 0!==x[f],p=(a?x:r)[f],l=m&&a?u(p,e):y&&"function"==typeof p?u(Function.call,p):p,x&&c(x,f,p,t&s.U),_[f]!=p&&i(_,f,l),y&&g[f]!=p&&(g[f]=p)};e.core=o,s.F=1,s.G=2,s.S=4,s.P=8,s.B=16,s.W=32,s.U=64,s.R=128,t.exports=s},1:function(t,n){var r=t.exports="undefined"!=typeof window&&

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\shared-file.eeb97be84f[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):	1351
Entropy (8bit):	4.746120327391164
Encrypted:	false
SSDEEP:	24:jDGA057Rq0S0RdG9yZe9W9VJjR855jVXVA03VJjVa5gqVp5gKEfh7AqLZ5XZVAOe:j6A057RF97Gc/f9y5lVXVA0l9VaOWpOM
MD5:	30DBAF1AA2461B67BD0FBA1F018B7A8F
SHA1:	EB99C8D6124599E57C219DA1591D0F90DE9A68B6
SHA-256:	7491367269A0C97C9EF859DBB361062FAB032FCF2F2807683A05ACA2A91245A8
SHA-512:	B6AB176319DF944978E0DE2E7D83EF811E7F526197802C87D77CE9D96DB4456E3461CDCC8255E0F502E34BDE4283BC9F7961552A333C494E8EA033C1C823E6B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn01.boxcdn.net/enduser/shared-file.eeb97be84f.css
Preview:	.shared-file-recents-link{max-width:300px;color:#909090;font-weight:400}.shared-file-recents-link .shared-file-name{font-weight:400}.shared-file-recents-link:active,.shared-file-recents-link:focus,.shared-file-recents-link:hover{color:#4e4e4e;text-decoration:underline;cursor:pointer}.shared-file-chevron{margin:8px 10px 6px 6px;transition:all .3s}.shared-file-page .header-logo{flex:0 1 auto}.shared-file-info{display:flex;align-items:center;min-width:0}.shared-file-icon{flex:none}.shared-file-name{overflow:hidden;font-weight:700;white-space:nowrap;text-overflow:ellipsis}.shared-file-menu-container{display:none}.shared-file-menu-container .shared-file-menu-toggle{display:flex;align-items:center;min-width:0}.shared-file-menu-container .toggle-arrow{flex:none;width:7px;height:4px;margin-left:5px}.shared-file-hideable-actions{display:flex;align-items:center}.shared-file-hideable-actions .download-icon{padding:8px 10px}.shared-file-overflow-btn{width:34px;height:32px;padding:0}@media (max-wid

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\2_bc3d32a696895f78c19df6c717586a5d[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	1864
Entropy (8bit):	5.222032823730197
Encrypted:	false
SSDEEP:	48:yvswNIBLBpJawmMH44log6gw/MHm7pJroog6gwkMH9Xog6gwdMHdqdyqog7C:ykfXYx+odPcs9B
MD5:	BC3D32A696895F78C19DF6C717586A5D
SHA1:	9191CB156A30A3ED79C44C0A16C95159E8FF689D
SHA-256:	0E88B6FCBB8591EDFD28184FA70A04B6DD3AF8A14367C628EDD7CABA32E58C68
SHA-512:	8D4F38907F3423A86D90575772B292680F7970527D2090FC005F9B096CC81D3F279D59AD76EAFCA30C3D4BBAF2276BBAA753E2A46A149424CF6F1C319DED5A6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://aadcdn.msftauth.net/ests/2.1/content/images/backgrounds/2_bc3d32a696895f78c19df6c717586a5d.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="1920" height="1080" fill="none"><g opacity=".2" clip-path="url(#E)"><path d="M1466.4 1795.2c950.37 0 1720.8-627.52 1720.8-1401.6S2416.77-1008 1466.4-1008-254.4-380.482-254.4 393.6s770.428 1401.6 1720.8 1401.6z" fill="url(#A)"/><path d="M394.2 1815.6c746.58 0 1351.8-493.2 1351.8-1101.6S1140.78-387.6 394.2-387.6-957.6 105.603-957.6 714-352.38 1815.6 394.2 1815.6z" fill="url(#B)"/><path d="M1548.6 1885.2c631.92 0 1144.2-417.45 1144.2-932.4S2180.52 20.4 1548.6 20.4 404.4 437.85 404.4 952.8s512.276 932.4 1144.2 932.4z" fill="url(#C)"/><path d="M265.8 1215.6c690.246 0 1249.8-455.595 1249.8-1017.6S956.046-819.6 265.8-819.6-984-364.005-984 198-424.445 1215.6 265.8 1215.6z" fill="url(#D)"/></g><defs><radialGradient id="A" cx="0" cy="0" r="1" gradientUnits="userSpaceOnUse" gradientTransform="translate(1466.4 393.6) rotate(90) scale(1401.6 1720.8)"><stop stop-color="#107c10"/><stop offset="1" stop-color="#c4c4c4" stop-opacity="0"/></radialGradient><r

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\53_8b36337037cff88c3df203bb73d58e41[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 342 x 72, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	5139
Entropy (8bit):	7.865234009830226
Encrypted:	false
SSDEEP:	96:oX2DsRVNYc82nTGTirCPqKO1gDPFjDiwK3aM5yO/bUlVV6JKo5N9jIMw7RLW1ZHb:ofRgc82nTprQsgDNDP7QgVVoH9+kMK9
MD5:	8B36337037CFF88C3DF203BB73D58E41
SHA1:	1ADA36FA207B8B96B2A5F55078BFE2A97ACEAD0E
SHA-256:	E4E1E65871749D18AEA150643C07E0AAB2057DA057C6C57EC1C3C43580E1C898
SHA-512:	97D8CC97C4577631D8D58C0D9276EE55E4B80128080220F77E01E45385C20FE55D208122A8DFA5DADCB87543B1BC291B98DBBA44E8A2BA90D17C638C15D487
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://aadcdn.msftauth.net/ests/2.1/content/images/applogos/53_8b36337037cff88c3df203bb73d58e41.png
Preview:	.PNG.....IHDR...V...H.....tEXtSoftware.Adobe ImageReadyq.e<...%iTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c148 79.164036, 2019/08/13-01:06:57 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmp:CreatorTool="Adobe Photoshop 21.0 (Macintosh)" xmpMM:InstanceID="xmp.iid:DB120779422011EA9888910153D3A5E6" xmpMM:DocumentID="xmp.did:DB12077A422011EA9888910153D3A5E6"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:DB120777422011EA9888910153D3A5E6" stRef:documentID="xmp.did:DB120778422011EA9888910153D3A5E6"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>P.WI....IDATx..]]l.....(.5.K0P..0...E.qT..J X)F.(5X....J.}(m.R5.Q...RUEUPU~.....qp@.b.....L...k.m"0....."c.3

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\core.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with LF, NEL line terminators
Category:	downloaded
Size (bytes):	87635
Entropy (8bit):	5.293336083461073
Encrypted:	false
SSDEEP:	1536:k9NbTl2MRt0zxgAHAPHxC+OMH8obwNaWpbDlct:k99Tl2MjJ8cPW9lct
MD5:	8F402D83489BA25EF87CDFC67BF47932
SHA1:	EFBCAE4F111F6CECF56E1B88857F688EEECABAF1
SHA-256:	50DA66E885D183593100789E7376D6171310D22F64E798A1DDA6AD5940CF0967
SHA-512:	E650576C845A326539EA79A87E8D5421B19349E5F5F7FB3F6BA8AE7F0F1A4F909BE87C9AD94022C043F5109B4A85C6DEA54ECEE8075786CCFE2F761696A965D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn01.boxcdn.net/polyfills/core-js/2.5.3/core.min.js
Preview:	/**. * core-js 2.5.3. * https://github.com/zloirock/core-js. * License: http://rock.mit-license.org. * . 2017 Denis Pushkarev. */.!function(t,n,r){"use strict";!function(t){function __webpack_require__(r){if(n[r])return n[r].exports;var e=n[r]={i:r,l:!1,exports:{}};return t[r].call(e.exports,e,e.exports,__webpack_require__),e.l=!0,e.exports}var n={};__webpack_require__.m=t,__webpack_require__.c=n,__webpack_require__.d=function(t,n,r){__webpack_require__.o(t,n)||Object.defineProperty(t,n,{configurable:!1,enumerable:!0,get:r})},__webpack_require__.n=function(t){var n=t&&t.__esModule?function getDefault(){return t["default"]}:function getModuleExports(){return t};return __webpack_require__.d(n,"a",n),n},__webpack_require__.o=function(t,n){return Object.prototype.hasOwnProperty.call(t,n)},__webpack_require__.p="",__webpack_require__(__webpack_require__.s=129)}([function(t,n,e){var i=e(2),o=e(18),u=e(13),c=e(14),f=e(19),a="prototype",s=function(t,n,e){var l,h,p,v,g=t&s.F,y=t&s.G,d=t&s.P,_=

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\intersection-observer[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):	7260
Entropy (8bit):	5.079928008915343
Encrypted:	false
SSDEEP:	192:siG99SlhMUrFC6Y/g7LNqkMAhDGgXdyDLK22FrRbO2+t6vFmtteS4c5q:USP1Y/g7RxpVhXdyX2FrRZ+GeteS5l
MD5:	498AAC0CA5A2544927FAF2681402DE59
SHA1:	39F0C1FBF7452CC5568E5E9C499C898272C285CE
SHA-256:	542FADAE21CB6CA75B99B8FC0A0FA8E300F18F679FAD27046D23C74C275F59EE
SHA-512:	FC6EB201EFCC38E3BD26926B264D867656A6471D43EA14F2D662E630728AAD6F190DDE8E510CDDEB52E6F97C4D785D63416F5976C80907BAA6DD1B25262D915
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn01.boxcdn.net/polyfills/intersection-observer/0.5.0/intersection-observer.js
Preview:	!function(t){function e(r){if(n[r])return n[r].exports;var o=n[r]={i:r,l:!1,exports:{}};return t[r].call(o.exports,o,o.exports,e),o.l=!0,o.exports}var n={};e.m=t,e.c=n,e.d=function(t,n,r){e.o(t,n)||Object.defineProperty(t,n,{configurable:!1,enumerable:!0,get:r})},e.n=function(t){var n=t&&t.__esModule?function(){return t.default}:function(){return t};return e.d(n,"a",n),n},e.o=function(t,e){return Object.prototype.hasOwnProperty.call(t,e)},e.p="",e(e.s=318)}({318:function(t,e){!function(t,e){"use strict";function n(t){this.time=t.time,this.target=t.target,this.rootBounds=t.rootBounds,this.boundingClientRect=t.boundingClientRect,this.intersectionRect=t.intersectionRect||a(),this.isIntersecting=!!t.intersectionRect;var e=this.boundingClientRect,n=e.width*e.height,r=this.intersectionRect,o=r.width*r.height;this.intersectionRatio=n?o/n:this.isIntersecting?1:0}function r(t,e){var n=e||{};if("function"!=typeof t)throw new Error("callback must be a function");if(n.root&&1!=n.root.nodeType)thro

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\messagecenter~uploads-manager-enduser.e83b2dda31[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):	46540
Entropy (8bit):	5.2638289199792485
Encrypted:	false
SSDEEP:	768:vj13k4lZZZsGcXaKxdk2S/4N2S/J67EKB3ipef8QScD8gtEwQThwdOwaleOFDX2g:4xdk2S/4N2S/J67EKB3ipef8QScD8g1o
MD5:	0301C1A9C6BFCA3D5F81EF8A64E77C2E
SHA1:	3CD3BB4391C82A29191B5B0C9ABB4EE01AFCE8DA
SHA-256:	218F4E999ED4F2B19EEAC806BC5D64C8E71F63E7D3336A6FAECE22FB784214FD
SHA-512:	E15B0AB4A5E0A254726DD07335E525FFCA73573AB19177E4446CF5041681C9B097FCC12FAF653C8C6360270CABAFB15514310CDE5DA50D7D84ABE1EC32FBC9B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn01.boxcdn.net/enduser/messagecenter~uploads-manager-enduser.e83b2dda31.js
Preview:	(window.webpackJsonp=window.webpackJsonp||[]).push([["messagecenter~uploads-manager-enduser"],{"7G9T0A7Q2t":function(e,t,o){"use strict";var n=o("QbLZJtXF68"),r=o.n(n),i=o("Yz+Y0CAZeS"),l=o.n(i),a=o("iCc5sPGOWs"),s=o.n(a),c=o("V7oCdLSCTo"),d=o.n(c),u=o("FYw3c9QbSe"),h=o.n(u),f=o("mRg0wtBNeT"),S=o.n(f),p=o("q1tIBJhxTW"),m=o("m0AvLASv6a"),_=(o("17x9q+7QrQ"),function(e){function t(){var e,o,n,r;s()(this,t);for(var i=arguments.length,a=Array(i),c=0;c<i;c++)a[c]=arguments[c];return o=n=h()(this,(e=t.__proto__||l()(t)).call.apply(e,[this].concat(a))),n.state={height:n.props.defaultHeight||0,width:n.props.defaultWidth||0},n._onResize=function(){var e=n.props,t=e.disableHeight,o=e.disableWidth,r=e.onResize;if(n._parentNode){var i=n._parentNode.offsetHeight||0,l=n._parentNode.offsetWidth||0,a=window.getComputedStyle(n._parentNode)||{},s=parseInt(a.paddingLeft,10)||0,c=parseInt(a.paddingRight,10)||0,d=parseInt(a.paddingTop,10)||0,u=parseInt(a.paddingBottom,10)||0,h=i-d-u,f=l-s-c;(!t&&n.state.hei

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\microsoft_logo_ee5c8d9fb6248c938fd0dc19370e90bd[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	3651
Entropy (8bit):	4.094801914706141
Encrypted:	false
SSDEEP:	96:wO4DZ+Stb/jY+eo4hAryAes9mBYYQgWLDm9:wToSBjlevudl9nO
MD5:	EE5C8D9FB6248C938FD0DC19370E90BD
SHA1:	D01A22720918B781338B5BBF9202B241A5F99EE4
SHA-256:	04D29248EE3A13A074518C93A18D6EFC491BF1F298F9B87FC989A6AE4B9FAD7A
SHA-512:	C77215B729D0E60C97F075998E88775CD0F813B4D094DC2FDD13E5711D16F4E5993D4521D0FBD5BF7150B0DBE253D88B1B1FF60901F053113C5D7C1919852D5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://aadcdn.msftauth.net/ests/2.1/content/images/microsoft_logo_ee5c8d9fb6248c938fd0dc19370e90bd.svg

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\microsoft_logo_ee5c8d9fb6248c938fd0dc19370e90bd[1].svg	
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="108" height="24" viewBox="0 0 108 24"><title>assets</title><path d="M44.836,4.6V18.4h-2.4V7.583H42.4L38 .119,18.4H36.531L32.142,7.583h-.029V18.4H29.9V4.6h3.436L37.3,14.83h.058L41.545,4.6Zm2,1.049a1.268,1.268,0,0,1,.419-.967,1.413,1.413,0,0,1,1-.39,1.392, 1.392,0,0,1,1.02.4,1.3,1.3,0,0,1,.4.958,1.248,1.248,0,0,1-.414.953,1.428,1.428,0,0,1-1.01.385A1.4,1.4,0,0,1,47.25,6.6a1.261,1.261,0,0,1-.409-.948M49.41,18.4H47. 081V8.507H49.41Zm7.064-1.694a3.213,3.213,0,0,0,1.145-.241,4.811,4.811,0,0,0,1.155-.635V18a4.665,4.665,0,0,1-1.266.481,6.886,6.886,0,0,1-1.554.164,4.707,4.707,0, 0,1-4.918-4.908,5.641,5.641,0,0,1,1.4-3.932,5.055,5.055,0,0,1,3.955-1.545,5.414,5.414,0,0,1,1.324.168,4.431,4.431,0,0,1,1.063.39v2.233a4.763,4.763,0,0,0-1.1-.61 1,3.184,3.184,0,0,0-1.15-.217,2.919,2.919,0,0,0-2.223.9,3.37,3.37,0,0,0-.847,2.416,3.216,3.216,0,0,0,.813,2.338,2.936,2.936,0,0,0,2.209.837M65.4,8.343a2.952,2.9 52,0,0,1,.5.039,2.1,2.1,0,0,1,.375.1v2.358a2.04,2.04,0,0,0-.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\pdf.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	330993
Entropy (8bit):	5.424757612418792
Encrypted:	false
SSDEEP:	3072:nFgCairre0QtIRq+VUCTBE3cxB9Bptk4RLpNKXOz:nFgKrXQMVUCtEaB9BptRRLpNKXq
MD5:	9A9AC5F2FB76274116C651226A647C95
SHA1:	EEDC500FC742C9762BF5789AE470132B2011AF77
SHA-256:	6CF4C965636CFA49500C3A95FDEF2C5F4722FD0367ED26D70A19F1A13DFFE173
SHA-512:	13132DAB411AEB5C8204171B3B350FE9B372B3ABA057F6BC3EABCE2BB5218212DDDA1A2020D9B00A986162AE5D85B88F7B3E1AAA4E7F8F7C4F63329DE48C76 0A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn01.boxcdn.net/platform/preview/third-party/doc/2.16.0/pdf.min.js
Preview:	(function(c,d){"object"===typeof exports&&"object"===typeof module?module.exports=d():"function"===typeof define&&define.amd?define("pdfjs-dist/build/pdf",[],d) :"object"===typeof exports?exports["pdfjs-dist/build/pdf"]=d():c["pdfjs-dist/build/pdf"]=c.pdfjsLib=d()})(this,function(){return function(c){function d(l){if(a[l])return a[l].expor ts;var n=a[l]={i:l,l:!1,exports:{}};c[l].call(n.exports,n,n.exports,d);n.l=!0;return n.exports}var a={};d.m=c;d.c=a;d.d=function(a,c,h){d.o(a,c)||Object.defineProperty(a,.c,{enumer able:!0,get:h})};d.r=function(a){"undefined"!==typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(a,Symbol.toStringTag,{value:"Module"});Object.defineProp erty(a,"__esModule",{value:!0})};d.t=function(a,c){c&1&&(a=d(a));if(c&8||c&4&&"object"===typeof a&&a&&a.__esModule)return a;var h=Object.create(null);d.r(h);Obj ect.defineProperty(h,"default",{enumerable:!0,value:a});if(c&2&&"string"!=typeof a)for(var n in a)d.d(h,n,function(h){return a[h]}.bind(null,n));return h};d.n=f

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\pdf_viewer.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	102404
Entropy (8bit):	5.401114766957238
Encrypted:	false
SSDEEP:	1536:jvbatbmMCjHJYfcgL5VMCaPx0g6T/xiZVBkAi0VV:qV6jWfzL5VMzPx0g6LMtpi07
MD5:	C1B5589ABBA40B2ED3D3AE6EB0F45373
SHA1:	D3F971D2C68F79F055E986F687F5F259DAED3226
SHA-256:	8FC790E9167754C61FFCD21E2382D2B6F55903C708239A5CDC7A15748F864B1B
SHA-512:	A10AD32428C2BF3A815C5F594C390812CA8FF9B7FAE49591CB9D2DBC7BDBEF70199808B69687A259F785DA80C9D49EE8E2FB300BE63B837ACBBA133D4DFD25 1B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn01.boxcdn.net/platform/preview/third-party/doc/2.16.0/pdf_viewer.min.js
Preview:	(function(q,f){"object"===typeof exports&&"object"===typeof module?module.exports=f():"function"===typeof define&&define.amd?define("pdfjs-dist/web/pdf_viewer", [],f):"object"===typeof exports?exports["pdfjs-dist/web/pdf_viewer"]=f():q["pdfjs-dist/web/pdf_viewer"]=q.pdfjsViewer=f()})(this,function(){return function(q){function f(h) {if(m[h])return m[h].exports;var k=m[h]={i:h,l:!1,exports:{}};q[h].call(k.exports,k,k.exports,f);k.l=!0;return k.exports}var m={};f.m=q;f.c=m;f.d=function(h,k,m){f.o(h,k)||Objec t.defineProperty(h,k,{enumerable:!0,get:m})};f.r=function(f){"undefined"!==typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(f,Symbol.toStringTag,{value: "Module"});Object.defineProperty(f,"__esModule",{value:!0})};f.t=function(h,k){k&1&&(h=f(h));if(k&8||k&4&&"object"===typeof h&&h&&h.__esModule)return h;var m=Ob ject.create(null);f.r(m);Object.defineProperty(m,"default",{enumerable:!0,value:h});if(k&2&&"string"!=typeof h)for(var n in h)f.d(m,n,function(f){return h[f]}.bind(null,n

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\picker_account_aad_9de70d1c5191d1852a0d5aac28b44a6c[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	756
Entropy (8bit):	4.879179443781471
Encrypted:	false
SSDEEP:	12:t4pb8WsQKvkBWSfYcW3ffBfYfomQO1a7aajR2F1hgWSnuCNSganii7v/NPujARqj:t4pb8WvKMTfY3ffBfYfomQO1eXjR2oug
MD5:	9DE70D1C5191D1852A0D5AAC28B44A6C
SHA1:	F4F64F5CBDBE6D1115C10A7F9CCB8828E6B67CAE
SHA-256:	5D3357BD875B7335ACE42E8EE3A64578E4253BED1A4E279109DE403EEDAE3A69
SHA-512:	CAC13FC2FE30E10772008F2AFF70FCA031EA9918E1F8C5C8B91CB9E79463383183406EFAADF89360DE3A08573FCDF2716C14DA6411E24B7E260B96AF84F0076
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\picker_account_aad_9de70d1c5191d1852a0d5aac28b44a6c[1].svg	
Reputation:	low
IE Cache URL:	http://https://aadcdn.msftauth.net/ests/2.1/content/images/picker_account_aad_9de70d1c5191d1852a0d5aac28b44a6c.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="48" height="48" viewBox="0 0 48 48"><title>assets</title><circle cx="24" cy="24" r="24" fill="#e6e6e6"/><path d="M34,35V14a2.938,2.938,0,0,0-3-3H27V8l2-1L27.948,5.638,24,8,20.07,5.648,19,7l2,1v3H17a2.938,2.938,0,0,0-3,3V35a2.938,2.938,0,0,0,3,3H31A2.938,2.938,0,0,0,34,35Zm-3,1H17a.979.979,0,0,1-1-1V14a.979.979,0,0,1,1-1h6V10h2v3h6a.979.979,0,0,1,1,1V35A.979.979,0,0,1,31,36Z" fill="#404040"/><path d="M26.766,25.42a4.432,4.432,0,1,0-5.533,0A6.237,6.237,0,0,0,17.765,31h1.653a4.582,4.582,0,1,1,9.165,0h1.653A6.237,6.237,0,0,0,26.766,25.42Zm-5.546-3.435A2.779,2.779,0,1,1,24,24.765,2.783,2.783,0,0,1,21.221,21.985Z" fill="#404040"/><rect x="21" y="14" width="6" height="2" rx="1" ry="1" fill="#404040"/></svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\picker_account_add_56e73414003cdb676008ff7857343074[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	222
Entropy (8bit):	5.004415423297573
Encrypted:	false
SSDEEP:	3:tIsqDmJS4RKb5zMc7XpCN+bJMacvRxyJAgR/QvfqhcDQKG2TcVER+HLZqWTboZUq:tI9mc4slztdbC/yXADQKDTcVEqLwDZsc
MD5:	56E73414003CDB676008FF7857343074
SHA1:	9ED7A58CD0E81E9689AC8C6D548A47D0185E0FDC
SHA-256:	749F85621D92A5B31B2A377A8C385A36D48A83327DAD9A8A8DA93CD831B8C9A2
SHA-512:	FAD0071AC2DFA23989BFBC7D3850415F3C340A74A54D3D8D797AFCCD6A301513BBC769DF4E5148605BE1E23A8750973EB80726F3CC959A2A457B0EC09AE14F7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://aadcdn.msftauth.net/ests/2.1/content/images/picker_account_add_56e73414003cdb676008ff7857343074.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="48" height="48" viewBox="0 0 48 48"><title>assets</title><circle cx="24" cy="24" r="24" fill="#e6e6e6"/><path d="M25,23H36v2H25V36H23V25H12V23H23V12h2Z" fill="#404040"/></svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\picker_more_7568a43cf440757c55d2e7f51557ae1f[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	899
Entropy (8bit):	3.8260330857236338
Encrypted:	false
SSDEEP:	24:t4CvnAVROLgCWbVHTVSRUyL3Fe09gCWbVHTVeUVh10UsSgCWbVHTVeUVh10Usb7:fncCWRH0JL3FECWRHQA10rCWRHQA10F
MD5:	7568A43CF440757C55D2E7F51557AE1F
SHA1:	55C22CA98B5CDCED134F6E24205C288845312A2D
SHA-256:	B7FCD37EAAFE3F08647ED072D5289EADFFF6C660A26CDEF31532B3FCFB4A0BB2
SHA-512:	F01DA2804594C3C78C0694FD6CC49B667663DA95AE7367EE3F0F5112B9957A3220389AAE4A5B750BCB3BC4F1092EA614266A4BFFD7E0FE16232E1CB57606E90
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://aadcdn.msftauth.net/ests/2.1/content/images/picker_more_7568a43cf440757c55d2e7f51557ae1f.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16" viewBox="0 0 16 16"><title>assets</title><path d="M9.143,1.143a1.107,1.107,0,0,1-.089.446,1.164,1.164,0,0,1-.607.607,1.161,1.161,0,0,1-.893,0,1.164,1.164,0,0,1-.607-.607,1.107,1.107,0,0,1-.089-.446A1.107,1.107,0,0,1,6.946.7,1.164,1.164,0,0,1,7.554.089a1.161,1.161,0,0,1,.893,0A1.164,1.164,0,0,1,9.054.7a1.107,1.107,0,0,1,.089.446M9.143,8a1.107,1.107,0,0,1-.089.446,1.164,1.164,0,0,1-.607.607,1.161,1.161,0,0,1-.893,0,1.164,1.164,0,0,1-.607-.607,1.161,1.161,0,0,1,0-.893,1.164,1.164,0,0,1,.607-.607,1.161,1.161,0,0,1,.893,0,1.164,1.164,0,0,1,.607.607A1.107,1.107,0,0,1,9.143,8m0,6.857a1.107,1.107,0,0,1-.089.446,1.164,1.164,0,0,1-.607.607,1.161,1.161,0,0,1-.893,0,1.164,1.164,0,0,1-.607-.607,1.161,1.161,0,0,1,0-.893,1.164,1.164,0,0,1,.607-.607,1.161,1.161,0,0,1,.893,0,1.164,1.164,0,0,1,.607.607A1.107,1.107,0,0,1,9.143,14.857Z"/></svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\preview-components.04034d91d5[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):	355729
Entropy (8bit):	5.492745127857912
Encrypted:	false
SSDEEP:	6144:/+SLOmw28TMELb78ipOv0HCIWcbFP5zWdWPOCh//S:/zxSYELRMXm5tDh//S
MD5:	EE0D104467B92AF33F74DFCD3B6BBC74
SHA1:	E7CFE1B099D6C66AC6FE87A83C2C0726AD3CEED1
SHA-256:	4887550D4631CD25C442D8064A66B3255F7879BC84D57E5FE5A8DFD8AF2FD70F
SHA-512:	7B8FCAECFA3F654B800239E495F88D592B727CF2DE2C0383917BDDCA90280F07F43F8EB795F252B2291E29896552BD31B5FB110ECC992B098BEC3E3762FB43E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn01.boxcdn.net/enduser/preview-components.04034d91d5.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\preview-components.04034d91d5[1].js	
Preview:	(window.webpackJsonp=window.webpackJsonp||[]).push([["preview-components"],{"+BZej3U4u/":function(e,t,n){"use strict";var r=n("q1tIBJhxTW"),o=n("vN+2IcUykn"),a=n.n(o),i=n("8Wpvjplx0g"),c=n("dtRsU6L1/l");function l(e){return(l="function"===typeof Symbol&&"symbol"===typeof Symbol.iterator?function(e){return typeof e}:function(e){return e&&"function"===typeof Symbol&&e.constructor===Symbol&&e!==Symbol.prototype?"symbol":typeof e})(e)}function s(e,t){if(null==e)return{};var n,r,o=function(e,t){if(null==e)return{};var n,r,o={},a=Object.keys(e);for(r=0;r<a.length;r++)n=a[r],t.indexOf(n)>=0||(o[n]=e[n]);return o}(e,t);if(Object.getOwnPropertySymbols){var a=Object.getOwnPropertySymbols(e);for(r=0;r<a.length;r++)n=a[r],t.indexOf(n)>=0||Object.prototype.propertyIsEnumerable.call(e,n)&&(o[n]=e[n])}return o}function u(e,t){var n=Object.keys(e);if(Object.getOwnPropertySymbols){var r=Object.getOwnPropertySymbols(e);t&&(r=r.filter((function(t){return Object.getOwnPropertyDescriptor(e,t).enumerable})))

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\preview-components.b6077e4fab[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):	20090
Entropy (8bit):	4.989082656749395
Encrypted:	false
SSDEEP:	384:jvVY2bm2cD2cI252TTc//T4/fnsWsgeWegnWngwWwhsQsGeQeGnQnGwQwrE07Sg8:jvTorMh6qMD2RhO6tFZU
MD5:	9AF8E1B956E70CCEBD85A9D3160A6DDA
SHA1:	30D31CFBA084F6A1F1DA1C8842730B22FF2CBD2E
SHA-256:	040E778FE44D8F018644A17C4DE15DDDB65ABC85F2C81DE51DC10165F8911FC9
SHA-512:	A012F3C0838F18BEF267E8D48CD65E3EF4A994E51B36FE99134C9723888E6D7F365E229534233945DD43B1A57792CDA529BD9931A37975E6CE456B969A7C60A8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn01.boxcdn.net/enduser/preview-components.b6077e4fab.css
Preview:	.error-mask{display:flex;flex-direction:column;align-items:center;padding:40px;overflow:hidden;border:1px dashed #909090;border-radius:3px}.error-mask .error-mask-sad-cloud{margin-bottom:20px}.error-mask h4{margin-top:-10px}.error-mask h4,.error-mask h5{width:100%;margin-bottom:0;color:#767676;text-align:center}.be .be-default-error{margin:8px}.bcpr .bcpr-notification{position:absolute;width:100%}.bcpr .bcpr-notification .notification>svg{display:none}.bcpr-FileInfo{display:flex;align-items:center}.bcpr-FileInfo-name{padding-left:5px;font-weight:700}.be-logo{padding-left:20px}.be-logo .be-logo-custom{max-width:80px;max-height:32px}.be-is-small .be-logo .be-logo-custom{max-width:75px}.be-logo .be-logo-placeholder{display:flex;align-items:center;justify-content:center;width:75px;height:32px;background-color:#e8e8e8;border:1px dashed}.be-is-small .be-logo .be-logo-placeholder{width:60px}.be-logo .be-logo-placeholder span{font-size:10px;text-transform:uppercase}.be-logo svg{display:block}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\preview[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):	699644
Entropy (8bit):	5.361811434311016
Encrypted:	false
SSDEEP:	6144:2KMZx0z5hFgHhdVZWjCAiAyO5ysvCMaRPvyc4v8plplMlpMGf9U:2P47wdYievCMaRPvG8plpKA
MD5:	212C1C6F38556CA9AC11E7B948EA455B
SHA1:	88C786BCE6A97557671E37503CE4FC56B5B06758
SHA-256:	DD637D4D06A59E696D64B95EFBA124EBAC48B2FC86F34CB333D436909C76AE80
SHA-512:	58F8580589803FE0D5EAAD3116904607693A82E829245A174662B6952797A64E30E15C7E39AE8CA77F2379819B859CD34BD3B6294A05037C3E2AD2004447D0E2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn01.boxcdn.net/platform/preview/2.61.0/en-US/preview.js
Preview:	/*!. * Box Content Preview. * . * Copyright 2019 Box, Inc. All rights reserved.. * . * This product includes software developed by Box, Inc. ("Box"). * (http://www.box.com). * . * ALL BOX SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESS OR IMPLIED. * WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF. * MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.. * IN NO EVENT SHALL BOX BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,. * SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT. * LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE,. * DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY. * THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT. * (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE. * OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.. * . * See the Box license for the specific language governing permissions. * and limitations under the licen

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\uploads-manager-enduser.47cb9896f5[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	96149
Entropy (8bit):	5.321706811661044
Encrypted:	false
SSDEEP:	1536:rQgaSb0h7ChdEF6QgNWCONl6CGKduS2z3Vh8MXBJ6P:eh7C4YQgNWCqoCpduSwVhvXBJ6P
MD5:	D305D69628296EB43A77FB0C8A6BD476
SHA1:	7EDF40E42CB0067CBC9A35716B6B1BE182C8BF41
SHA-256:	51E79C882120DA0B28E9FE45A485BD73F49828C2AE61A237732D012CB8372805
SHA-512:	C95D2A441E984FC10AA51B0C1E989E6D2D4041FA7DC0EDF4797C92987A3A7A69B0FB3D2EEA37D84AD709FB2DE6394CA1174CE225E2184429EF6E65B566D69AF4

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\uploads-manager-enduser.47cb9896f5[1].js</th></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Reputation:</td><td>low</td></tr>
<tr><td>IE Cache URL:</td><td>http://https://cdn01.boxcdn.net/enduser/uploads-manager-enduser.47cb9896f5.js</td></tr>
<tr><td>Preview:</td><td>/*! For license information please see uploads-manager-enduser.47cb9896f5.js.LICENSE.txt */.(window.webpackJsonp=window.webpackJsonp||[]).push([["uploads-manager-enduser"],{"/5QKqsbcTJ":function(e,t,n){"use strict";var r=n("q1tIBJhxTW"),o=n("DJuBjJIVWu");t.a=function(e){var t=e.className,n=void 0===t?"":t,a=e.color,i=void 0===a?"#000000":a,l=e.height,s=void 0===l?24:l,u=e.title,c=e.width,d=void 0===c?24:c;return r.createElement(o.default,{className:"icon-check ".concat(n),height:s,title:u,viewBox:"0 0 24 24",width:d},r.createElement("path",{d:"M0 0h24v24H0z",fill:"none"}),r.createElement("path",{className:"fill-color",d:"M9 16.17L4.83 12l-1.42 1.41L9 19 21 7l-1.41-1.41z",fill:i}))}},"2W6zXrfv2o":function(e,t,n){"use strict";var r=function(){};e.exports=r},"2rMqT+dBMw":function(e,t,n){var r;!function(){"use strict";var o=!("undefined"===typeof window||!window.document||!window.document.createElement),a={canUseDOM:o,canUseWorkers:"undefined"!==typeof Worker,canUseEventListeners:o&&!(!win</td></tr>
</table>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\Lato-woff[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	271824
Entropy (8bit):	6.004035154725513
Encrypted:	false
SSDEEP:	6144:7iSn14Pe5e8PMyBdu/gFU7Eu2bzHB1v1e/OHjl0Cl:eS18e5eqMy7RbT/v1QODl0Cl
MD5:	E1E5023A4D0B29824C8A6937ED303B03
SHA1:	93159BA90E4ACA126C45282D047E4E1D544AD100
SHA-256:	80745E4A131F2F16302232F53845BFA223915A3465369A40A9AA777D2C0A30BD
SHA-512:	09A87AA0383D5E78FAF21CD63E4EE6EB875AC39F52AAF0805224DDFE39B56E91ECEEA743B811C2C8473A0113BDA678C472EAD4FECA207004A37699D051EA68B6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn01.boxcdn.net/fonts/1.0.2/lato/Lato-woff.css
Preview:	@font-face {. font-family: 'Lato';. /* This is Base64 encoded from Lato-Regular.woff */. src: url('data:application/x-font-woff;charset=utf-8;base64,d09GRgABAAAAAdFcABMAAAADhOgAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABGRlRNAAABqAAAABwAAAAccNlcTUdERUYAAAHEAAAANwAAADgSeA2uR1BPUwAAAfwAANZ6AAGuYg7b1pNHU1VCAADYeAAAAywAAAtGQYaNc09TLzIAANukAAAAXwAAAGBp8+XGY21hcAAA3AQAAATZAAAGoHgSIT5jdnQgAADg4AAAAHIAAADqPzmz1GZwZ20AAOFUAAAFqAAAC5fkFNvwZ2FzcAAA5vwAAAAIAAAACAAAABBnbHlmAADnBAAAwI4AAWHYuL0/gWhlYWQAAaeUAAAAMQAAADYO+nFmaGhlYQABp8gAAAAhAAAAJBEGCeFobXR4AAGn7AAACQ4AABIS60ObMmxvY2EAAbD8AAAI5AAACR6IDi0mbWF4cAABueAAAAAgAAAAIAZMAeluYW1lAAG6AAAABQQAAA/ywsuuaHBvc3QAAb8EAAARqgAAJ+ABEAopcHJlcAAB0LAAAACiAAAAuW8KaTp3ZWJmAAHRVAAAAAYAAAAGYIZWjQAAAAEAAAAAzD2izwAAAADR6Kh5AAAAANKzEQR42mNgZGBg4ANiAwYQYGJgZWBkagLiZqY2BmamdhZvBkYWHxZfBiYWP5ZeBkYGFrAqBgBp7gRDAHjapL0JfE3X+v+/9t4h8zwPZkVJEVVTU1xUY1ZVVFTVRbVVVXXbolJVVVdDTTVXFVU1z5XEHMFBcCKVSCJizEkaJyGhqmr932ed0+a06t77/f1vX5/9WWedtdZeZ4e18R8c18R8c/xY0eJBq

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\T.B.%20Penick%20&%20Sons,%20Inc[1].pdf</th></tr>
<tr><td>Process:</td><td>C:\Program Files (x86)\Internet Explorer\iexplore.exe</td></tr>
<tr><td>File Type:</td><td>PDF document, version 1.6</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>131839</td></tr>
<tr><td>Entropy (8bit):</td><td>7.635069874483118</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>3072:OoScUhP4d9Xh/ZlteVefdDAIFLs6P8VL77wfU4V1Kl3Hii5:LUiltVXL58VLX0rOCi5</td></tr>
<tr><td>MD5:</td><td>568F17A6C29B787AB760F9D2745B8C2F</td></tr>
<tr><td>SHA1:</td><td>9B3C2A55DD842F437E10621D99F1F95C7E325390</td></tr>
<tr><td>SHA-256:</td><td>CC22F6D75DFBA78622F0CF5FD3178C2756BE9405F0557D54518281C5CD4E9D6D</td></tr>
<tr><td>SHA-512:</td><td>BD30F6D45901D66011F07153A57DA1A9380664CD75E54A24BC7C9AEFE39C08E18D422FCDBDE333B31AAB1E2F5B74D3F651512B1ACA1787A36CBC858A21E1EF02</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Reputation:</td><td>low</td></tr>
<tr><td>Preview:</td><td>%PDF-1.6.%......12 0 obj.<</Linearized 1/L 122083/O 14/E 117534/N 1/T 121782/H [519 189]>>.endobj.   .33 0 obj.<</DecodeParms<</Columns 5/Predictor 12>>/Filter/FlateDecode/ID[<5456EF336601E7B4FD1BC437B7D72182><CA58E4D1474E49C191B5D4358961A536>]/Index[12 49]/Info 11 0 R/Length 105/Prev 121783/Root 13 0 R/Size 61/Type/XRef/W[1 3 1]>>stream..h.bbd`.``b``.."....|...."%.."Q .U...... .C.........4.H.U`v!.......*..&?....7...?....0.$...t...........q.m.endstream.endobj.startxref.0.%%EOF.   .60 0 obj.<</Filter/FlateDecode/I 125/Length 103/S 38/V 103>>stream..h.b``.f``.e```<.........A.IL...."....V.?d`d9..........4FM.@F..#FVF1.....W..c<..5...8.... ..*.........endstream.endobj.13 0 obj.<</AcroForm 34 0 R/Metadata 2 0 R/Pages 10 0 R/Type/Catalog>>.endobj.14 0 obj.<</BleedBox[0 7.8299813 595.5 850.07996]/Contents 15 0 R/CropBox[0 7.8299813 595.5 850.07996]/MediaBox[0 7.8299813 595.5 850.07996]/Parent 10 0 R/Resources<</ExtGState<</GS0 35 0 R/GS1 36 0 R>>/Font<</C0_0</td></tr>
</table>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\app.3caae0bb80[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):	1359024
Entropy (8bit):	5.444597719854545
Encrypted:	false
SSDEEP:	24576:pKccx9Vdggwac+Yf/LVQRL70RcKgmFudvomN82M0arMo/PUObHBshTptG5jJWK9D:phcx9Vdggwac+uTVQRL70RcKgmFudvo7

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\app.3caae0bb80[1].js	
MD5:	51C67DB8B1D7AB44CC195AF49A7C66A2
SHA1:	CE6F64290EEB0619162D8A8BD635C67C2988E423
SHA-256:	D0C2B02F0D4852810D52265097EAF00D317667621CFC0B432F1E67C271E10F8C
SHA-512:	B844597C37EDCD8E771B76EFC04F388D3E8F815EF0E86FF233E7B1A81B108996DF44A9FBBB91FC6C5696BA22E06F54CEFD11F84634C2726E0993295550CB1FE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn01.boxcdn.net/enduser/app.3caae0bb80.js
Preview:	(window.webpackJsonp=window.webpackJsonp||[]).push([["app"],{"+4HFvFfEZ0":function(e,t,n){"use strict";var r=n("q1tIBJhxTW"),o=n("1En/ASmD05"),a=n("4Whi4X5bOd");function i(){return(i=Object.assign||function(e){for(var t=1;t<arguments.length;t++){var n=arguments[t];for(var r in n)Object.prototype.hasOwnProperty.call(n,r)&&(e[r]=n[r])}return e}).apply(this,arguments)}t.a=function(e){return r.createElement(a.a,i({width:16,height:16,viewBox:"0 0 16 16"},e),r.createElement("path",{fill:o.bdlGray50,fillRule:"evenodd",d:"M14.119 3.176a.5.5 0 01.815.574l-.053.074-5.055 5.95a.502.502 0 01-.597.127l-.083-.05-3.553-2.649-3.703 4.611a.501.501 0 01-.628.127l-.075-.05a.501.501 0 01-.127-.628l.05-.075L5.116 6.2a.5.5 0 01.614-.134l.074.046 3.563 2.656 4.752-5.592z"}))}},"+5Szpi0raq":function(e,t,n){"use strict";var r=n("q1tIBJhxTW"),o=n("1En/ASmD05"),a=n("4Whi4X5bOd");function i(){return(i=Object.assign||function(e){for(var t=1;t<arguments.length;t++){var n=arguments[t];for(var r in n)Object.prototype

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\app.8f4ad58129[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):	155223
Entropy (8bit):	5.017204621947009
Encrypted:	false
SSDEEP:	3072:4dyg6zSqfO6QAQlkkBh39AiDQyUyoTwTrhmvdhU4pSs/MY:4dyg6zSqfO6QAQlkkBh39AiDQyUyoTwA
MD5:	45FE981ECE793E20C3AF7AE4E8B36FDD
SHA1:	416B54B82BF359DA73F4A13FA809C49776689D14
SHA-256:	81AA096AE4F9AD6DEB38A8151DD22A118B5D5175926233B85F297EAE83217938
SHA-512:	F64ACE5A4E7943718D15506C5C123276D59788699E9B2F9494ABD3740694DAE6289487F547980C223C130C279E42C85CD463E41003FC3F82E58C7C2A835066DC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn01.boxcdn.net/enduser/app.8f4ad58129.css
Preview:	.flyout-overlay{font-family:Lato,Helvetica Neue,Helvetica,Arial,sans-serif;-webkit-font-smoothing:antialiased;-moz-osx-font-smoothing:grayscale;text-rendering:optimizeLegibility;font-weight:400;font-size:13px;color:#222;line-height:20px;letter-spacing:.3px;z-index:190;box-sizing:border-box}.flyout-overlay>div:not(.should-outline-focus):focus{outline:none}.flyout-overlay .overlay{padding:15px;border-radius:4px}.flyout-overlay.dropdown-menu-element-attached-center .overlay,.flyout-overlay.flyout-overlay-target-attached-left .overlay,.flyout-overlay.flyout-overlay-target-attached-right .overlay{animation:fade-in .15s cubic-bezier(0,0,.6,1)}.scroll-container{position:relative;display:flex;flex-grow:1;height:100%;overflow:hidden}.scroll-container .scroll-wrap-container{flex-grow:1;overflow-y:auto}.scroll-container .scroll-wrap-container:after,.scroll-container .scroll-wrap-container:before{position:absolute;display:block;width:100%;height:30px;border-radius:inherit;opacity:0;transition:opac

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\content-sidebar.d7d089246d[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):	49949
Entropy (8bit):	5.38788940473956
Encrypted:	false
SSDEEP:	768:fs/VCjHEsHlmIG67fBf/37FDvuMtvvzeKQ2rsr5HusUGp:7VJ/37FzumvwlHl
MD5:	EFB99E97F0787C9BEAA050A8547E3457
SHA1:	3527F4862B6FAE2A6B8F3D282A5C3F958C899995
SHA-256:	18300F5956B71A7612403F8C3F3B8F2B39D23793BCC6EED9A0E44DC287643F62
SHA-512:	D29F493B73F6685797F5FE0910BCD35757CFE1D0FA5924254EE9AB940103C6FE6C7D29205C9CC876913E2DC64A21C25415C88AF29C993A8171AA4AA360EB5E7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn01.boxcdn.net/enduser/content-sidebar.d7d089246d.js
Preview:	(window.webpackJsonp=window.webpackJsonp||[]).push([["content-sidebar"],{"+HTToFDsKF":function(e,t,n){"use strict";n.r(t);n("ls82xohDAq");var r=n("q1tIBJhxTW"),a=n.n(r),i=n("vN+2IcUykn"),o=n.n(i),c=n("56YHLNIoDA"),s=n.n(c),l=n("Jdck50bD+l"),u=n("9v9/QOdyjq"),d=n("NR/qkXUXgp"),f=n("TSYQbtd+U2"),p=n.n(f),b=n("mwIZSSbMl2"),h=n.n(b),y=n("mNz5hShaC3"),m=n.n(y),v=n("Ty5D64ufpF"),g=n("UroeuGWH9k"),S=n("03vecjQMf5"),O=n("JRPeW/Ew/U"),E=n("Amu/syeQX8"),I=n("mxNUbu5+54"),w=n("DJuBjJlVWu"),A=function(e){var t=e.className,n=void 0===t?"":t,a=e.color,i=void 0===a?"#999":a,o=e.height,c=void 0===o?24:o,s=e.title,l=e.width,u=void 0===l?24:l;return r.createElement(w.default,{className:"icon-doc-info ".concat(n),height:c,title:s,viewBox:"0 0 24 24",width:u},r.createElement("path",{className:"fill-color",d:"M19.41 7.41l-4.82-4.82A2 2 0 0 0 13.17 2H6a2 2 0 0 0-2 2v16a2 2 0 0 0 2 2h12a2 2 0 0 0 2-2V8.83a2 2 0 0 0-.59-1.42zM13 16a1 1 0 0 1-2 0v-4a1 1 0 0 1 2 0zm-1-6a1 1 0 1 1 1-1 1 1 0 0 1-1 1z",fill:i}))},

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\ellipsis_635a63d500a92a0b8497cdc58d0f66b1[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	900
Entropy (8bit):	3.8081778439799248
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\ellipsis_635a63d500a92a0b8497cdc58d0f66b1[1].svg	
SSDEEP:	24:t4CvnAVRHf1QqCSzGUdiHTVtpRduf1QqCWbVHTVeUV0Uv6f1QqCWbVHTVeUV0UFl:fn+1QqC4GuiHFXS1QqCWRHQ3V1QqCWRV
MD5:	635A63D500A92A0B8497CDC58D0F66B1
SHA1:	A32EBA4B4D139E8DA52C5801A13C1EE222B2B882
SHA-256:	61D7CCC5D2C41BF86BE6CEFB0063405067849BA64E9F219F60596EF09A54A942
SHA-512:	EFFE15E105FC5FA853E76917B533AAE6C75EBA9A256049FB5EAB88BBF319D63A4CE4AE3743A09D6A5F474B01649D6EDC5C8BCCC61B8CA9EA9E5C39E7AE724C16
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://aadcdn.msftauth.net/ests/2.1/content/images/ellipsis_635a63d500a92a0b8497cdc58d0f66b1.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16" viewBox="0 0 16 16"><title>assets</title><path d="M1.143,6.857a1.107,1.107,0,0,1,.446.089,1.164,1.164,0,0,1,.607.607,1.161,1.161,0,0,1,0,.893,1.164,1.164,0,0,1-.607.607,1.107,1.107,0,0,1-.446.089A1.107,1.107,0,0,1,.7,9.054a1.164,1.164,0,0,1-.607-.607,1.161,1.161,0,0,1,0-.893A1.164,1.164,0,0,1,.7,6.946a1.107,1.107,0,0,1,.446-.089M8,6.857a1.107,1.107,0,0,1,.446.089,1.164,1.164,0,0,1,.607.607,1.161,1.161,0,0,1,0,.893,1.164,1.164,0,0,1-.607.607,1.161,1.161,0,0,1,0-.893,1.164,1.164,0,0,1,.607-.607A1.107,1.107,0,0,1,8,6.857m6.857,0a1.107,1.107,0,0,1,.446.089,1.164,1.164,0,0,1,.607.607,1.161,1.161,0,0,1,0,.893,1.164,1.164,0,0,1-.607.607,1.161,1.161,0,0,1-.893,0,1.164,1.164,0,0,1-.607-.607A1.107,1.107,0,0,1,14.857,6.857Z"/></svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\ellipsis_grey_2b5d393db04a5e6e1f739cb266e65b4c[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	915
Entropy (8bit):	3.8525277758130154
Encrypted:	false
SSDEEP:	24:t4CvnAVRfFArf1QqCSzGUdiHTVtpRduf1QqCWbVHTVeUVx:fn1r1QqC4GuiHFXS1QqCWRHQ3V1QqCWz
MD5:	2B5D393DB04A5E6E1F739CB266E65B4C
SHA1:	6A435DF5CAC3D58CCAD655FE022CCF3DD4B9B721
SHA-256:	16C3F6531D0FA5B4D16E82ABF066233B2A9F284C068C663699313C09F5E8D6E6
SHA-512:	3A692635EE8EBD7B15930E78D9E7E808E48C7ED3ED79003B8CA6F9290FA0E2B0FA3573409001489C00FB41D5710E75D17C3C4D65D26F9665849FB7406562A406
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://aadcdn.msftauth.net/ests/2.1/content/images/ellipsis_grey_2b5d393db04a5e6e1f739cb266e65b4c.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16" viewBox="0 0 16 16"><title>assets</title><path fill="#777777" d="M1.143,6.857a1.107,1.107,0,0,1,.446.089,1.164,1.164,0,0,1,.607.607,1.161,1.161,0,0,1,0,.893,1.164,1.164,0,0,1-.607.607,1.107,1.107,0,0,1-.446.089A1.107,1.107,0,0,1,.7,9.054a1.164,1.164,0,0,1-.607-.607,1.161,1.161,0,0,1,0-.893A1.164,1.164,0,0,1,.7,6.946a1.107,1.107,0,0,1,.446-.089M8,6.857a1.107,1.107,0,0,1,.446.089,1.164,1.164,0,0,1,.607.607,1.161,1.161,0,0,1,0,.893,1.164,1.164,0,0,1-.607.607,1.161,1.161,0,0,1,0-.893,1.164,1.164,0,0,1,.607-.607A1.107,1.107,0,0,1,8,6.857m6.857,0a1.107,1.107,0,0,1,.446.089,1.164,1.164,0,0,1,.607.607,1.161,1.161,0,0,1,0,.893,1.164,1.164,0,0,1-.607.607,1.161,1.161,0,0,1-.893,0,1.164,1.164,0,0,1-.607-.607A1.107,1.107,0,0,1,14.857,6.857Z"/></svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\eqit09n816yvtnxs1iqirsq7ectaev7m[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):	9244
Entropy (8bit):	5.281191603287551
Encrypted:	false
SSDEEP:	192:G8eHxkAYOA7lkZkrjyBuDoPql3+z6GUBfo1eM7cn2cjj6QDB7Ey4fVCrHk:G8gxkAVApkZkrjyBuDoP+3+z6GUHnvjs
MD5:	830FDA616B6A9595BC7BCE62C2FBBD72
SHA1:	0250C5829E230C095174AE0392E4AC26B81D68A4
SHA-256:	76BC7CFD639BAC685F9C599837074D44F77E827985AA0B3F5488A3B08119DDF8
SHA-512:	A93E6740C7FD39557491E1A765B126C03741471F030E89F6D7BC01744E5C41F0FF3208C947D7819033461BE9A4930FADD30C21CBE938EF585E6770DC99E45562
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE html><html lang="en-US" data-resin-client="web"><head><meta http-equiv="X-UA-Compatible" content="IE=edge"><meta name="viewport" content="width=device-width, initial-scale=1.0"><meta name="robots" content="noindex, nofollow"><title>Box</title> <link rel="stylesheet" href="https://cdn01.boxcdn.net/fonts/1.0.2/lato/Lato-woff.css"> <link rel="stylesheet" href="https://cdn01.boxcdn.net/enduser/app.8f4ad58129.css"> <link rel="apple-touch-icon" sizes="57x57" href="https://cdn01.boxcdn.net/_assets/img/favicons/apple-touch-icon-57x57-fLlEpj.png">.<link rel="apple-touch-icon" sizes="60x60" href="https://cdn01.boxcdn.net/_assets/img/favicons/apple-touch-icon-60x60-Uv0qzu.png">.<link rel="apple-touch-icon" sizes="72x72" href="https://cdn01.boxcdn.net/_assets/img/favicons/apple-touch-icon-72x72-7aVqne.png">.<link rel="apple-touch-icon" sizes="76x76" href="https://cdn01.boxcdn.net/_assets/img/favicons/apple-touch-icon-76x76-ZVGnRV.png">.<link rel="apple-touch-icon" sizes="114x114" href=

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\lang-en-AU~lang-en-CA~lang-en-GB~lang-en-US~lang-en-x-pseudo.57dba5f597[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):	18553
Entropy (8bit):	4.767569802615062

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\lang-en-AU~lang-en-CA~lang-en-GB~lang-en-US~lang-en-x-pseudo.57dba5f597[1].js	
Encrypted:	false
SSDEEP:	96:4a/eFtQk31IQk31PGHEU5ZQk31IQk31Pa9rEHqQk31IQk31PDkdolQk31IQk31Pw:J/egEH7uEt6EtXElPiMs8sVAyfEtbim
MD5:	9BCCCA5979199B48DD2DCD6BAC31CDCA
SHA1:	380DBAED126862294356918B0AC8031C00BD492A
SHA-256:	860E3603A72F16B016D971C6FA67386D8C1398A44A896F896082B6F7CDF2CC78
SHA-512:	B352761E7A479C34F53E6694208EF5CA92DA2F43E3199305B3E383B4C42A1FFF3B6AA5084E9233879E17F7BD85FD329CA46642F1BBB0DEDB750E83BDBDC83B27
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn01.boxcdn.net/enduser/lang-en-AU~lang-en-CA~lang-en-GB~lang-en-US~lang-en-x-pseudo.57dba5f597.js
Preview:	(window.webpackJsonp=window.webpackJsonp||[]).push([["lang-en-AU~lang-en-CA~lang-en-GB~lang-en-US~lang-en-x-pseudo"],{PTt16PTTsL:function(e,a,t){e.exports=function(){"use strict";return[{locale:"en",pluralRuleFunction:function(e,a){var t=String(e).split("."),o=!t[1],n=Number(t[0])==e,r=n&&t[0].slice(-1),i=n&&t[0].slice(-2);return a?1==r&&11!=i?"one":2==r&&12!=i?"two":3==r&&13!=i?"few":"other":1==e&&o?"one":"other"},fields:{year:{displayName:"year",relative:{0:"this year",1:"next year","-1":"last year"},relativeTime:{future:{one:"in {0} year",other:"in {0} years"},past:{one:"{0} year ago",other:"{0} years ago"}}},"year-short":{displayName:"yr.",relative:{0:"this yr.",1:"next yr.","-1":"last yr."},relativeTime:{future:{one:"in {0} yr.",other:"in {0} yr."},past:{one:"{0} yr. ago",other:"{0} yr. ago"}}},month:{displayName:"month",relative:{0:"this month",1:"next month","-1":"last month"},relativeTime:{future:{one:"in {0} month",other:"in {0} months"},past:{one:"{0} month ago",other:"{0} mo

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\lang-en-US.e38312dc59[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):	514623
Entropy (8bit):	4.8633386077970435
Encrypted:	false
SSDEEP:	12288:2yV20X7edTsKge2YSYgoST7bF4TjdFjsjejQjecDuScSai:2yV20X7ed/cD1cSai
MD5:	06B461355C5F9FC1BA6AB27AF0AAC102
SHA1:	F6FFFBF4F0E19A7B455D7D8ABA6E5B495F98D1FC
SHA-256:	79330BEAB86C8B84AD9C6559A89C9D51C0F03E0D8A983CCBD82F338B0F37D538
SHA-512:	9294AFE9929A2AA6EE97CCC28127F571549939CB14D05D64DBC64ED5D5642CA7D9DDB7842B91BA63813EB4475B43F9A5CB3DD66FF0047AC85388433FED65EC8B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn01.boxcdn.net/enduser/lang-en-US.e38312dc59.js
Preview:	(window.webpackJsonp=window.webpackJsonp||[]).push([["lang-en-US"],{RGqkULYfOR:function(e,o,a){"use strict";a.r(o);var t=a("PTt16PTTsL"),r=a.n(t),n=a("pBVgBhjduU");function i(e,o){var a=Object.keys(e);if(Object.getOwnPropertySymbols){var t=Object.getOwnPropertySymbols(e);o&&(t=t.filter((function(o){return Object.getOwnPropertyDescriptor(e,o).enumerable})),a.push.apply(a,t)}return a}function s(e,o,a){return o in e?Object.defineProperty(e,o,{value:a,enumerable:!0,configurable:!0,writable:!0}):e[o]=a,e}a.d(o,"language",(function(){return l})),a.d(o,"locale",(function(){return d})),a.d(o,"messages",(function(){return u})),a.d(o,"reactIntlLocaleData",(function(){return r.a})),a.d(o,"boxCldrData",(function(){return n.a}));var l="en-US",d="en",u=function(e){for(var o=1;o<arguments.length;o++){var a=null!=arguments[o]?arguments[o]:{};o%2?i(Object(a),!0).forEach((function(o){s(e,o,a[o])})):Object.getOwnPropertyDescriptors?Object.defineProperties(e,Object.getOwnPropertyDescriptors(a)):i(Object(

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\pdf.worker.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	770438
Entropy (8bit):	5.63651891023521
Encrypted:	false
SSDEEP:	12288:/B8HgJ+hAaAZ9KBbYRhv1vxjvkcZjuMl68DXX:/B8AsqaA7KBE31vxwEuMl68Dn
MD5:	8F43F3A32DF23400F995137BD39B3E96
SHA1:	9F368C68F4788C9565EDEA054541683CB6791E3F
SHA-256:	1DFAD8C9B4B4981418A528C29A316683E17C222C0D27348264627C57580D2F37
SHA-512:	6000022D4694690E17324F449F090B49000BC7D043C81D6291DE595D98DB3D1FBA060A673A104DF12F71C05D1576861E39272FA14CF525AF172DF4EF58011AD0
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn01.boxcdn.net/platform/preview/third-party/doc/2.16.0/pdf.worker.min.js
Preview:	(function(q,g){"object"===typeof exports&&"object"===typeof module?module.exports=g():"function"===typeof define&&define.amd?define("pdfjs-dist/build/pdf.worker",[],g):"object"===typeof exports?exports["pdfjs-dist/build/pdf.worker"]=g():q["pdfjs-dist/build/pdf.worker"]=q.pdfjsWorker=g()})(this,function(){return function(q){function g(a){if(c[a])return c[a].exports;var w=c[a]={i:a,l:!1,exports:{}};q[a].call(w.exports,w,w.exports,g);w.l=!0;return w.exports}var c={};g.m=q;g.c=c;g.d=function(a,c,b){g.o(a,c)||Object.defineProperty(a,c,{enumerable:!0,get:b})};g.r=function(a){"undefined"!==typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(a,Symbol.toStringTag,{value:"Module"});Object.defineProperty(a,"__esModule",{value:!0})};g.t=function(a,c){c&1&&(a=g(a));if(c&8||c&4&&"object"===typeof a&&a&&a.__esModule)return a;var b=Object.create(null);g.r(b);Object.defineProperty(b,"default",{enumerable:!0,value:a});if(c&2&&"string"!=typeof a)for(var l in a)g.d(b,l,function(b){return a[b]}.bind(

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\runtime.1abde09726[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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\runtime.1abde09726[1].js	
Size (bytes):	46300
Entropy (8bit):	4.916444243499991
Encrypted:	false
SSDEEP:	768:iewMOjRzRUGVKxdta9Cvxt6z/q8n+UORrlAwYsCF20qHGnOjRzRUGVKxdta9CvxH:yROxsz/qjZ5zzCFV9QROxsz/qw+jgFqV
MD5:	60291C6FCEFADC4DF56EFF9D738D49A4
SHA1:	6DFD6824B919109045F9387BCCD51FDDE7E76E20
SHA-256:	84B96A9F444D283601BE884F5F7E1CBCF4817323A12F29FD78EABE4731EE622E
SHA-512:	8605C862EC9A850AF637BF06AF96E30D806A08F2BBAE6F17427B964C973A7AEC9DA1FF2856D1E69BB67C417B789FDDF803CEA3AEB13F43BC1BACDF0E3BB3F9C6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn01.boxcdn.net/enduser/runtime.1abde09726.js
Preview:	!function(e){function a(a){for(var t,l,d=a[0],i=a[1],r=a[2],c=0,f=[];c<d.length;c++)l=d[c],Object.prototype.hasOwnProperty.call(n,l)&&n[l]&&f.push(n[l][0]),n[l]=0;for(t in i)Object.prototype.hasOwnProperty.call(i,t)&&(e[t]=i[t]);for(m&&m(a);f.length;)f.shift()();return s.push.apply(s,r||[]),o()}function o(){for(var e,a=0;a<s.length;a++){for(var o=s[a],t=!0,l=1;l<o.length;l++){var i=o[l];0!==n[i]&&(t=!1)}t&&(s.splice(a--,1),e=d(d.s=o[0]))}return e}var t={},l={runtime:0},n={runtime:0},s=[];function d(a){if(t[a])return t[a].exports;var o=t[a]={i:a,l:!1,exports:{}};return e[a].call(o.exports,o,o.exports,d),o.l=!0,o.exports}d.e=function(e){var a=[];l[e]?a.push(l[e]):0!==l[e]&&{"access-stats-export-modal~activity-sidebar~as-account~as-diagnostics~as-integrations~as-notification~5f5ce412":1,"access-stats-export-modal~classification-modal-v2~file-request-and-setting-modal~file-request-builde~0e8c2ec7":1,"access-stats-export-modal~activity-sidebar~edit-tags-modal~keywordless-search~multi-share-

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\vendors~app.ad1b5c324e[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	747750
Entropy (8bit):	5.45219030923825
Encrypted:	false
SSDEEP:	6144:q8A8sZzoh+GzlUKvBUZ2Zkm9z5JpgvdjnVUi40E9Pg38hLdp5xnXcIbdS+ydTzST:ZTsZalUeZkm9Malj9hLdPZvup2dF
MD5:	482A2EAB5A48A63B469D4C4FB1D2313E
SHA1:	B1D1253F8497F642E3477D0EEBCDE25B40F81529
SHA-256:	5BFEBE33BD3194DFCBCC63ADC0E4CDC5D2B5A9B2A70AFFE9322DBDE24F1EED1D
SHA-512:	F7B433D5671DE6418BACBCA18E1DB2755F6A00C2845149FB0B3BEFFEFBB6EF3D2C6DAEA24BE5646FBD8391E2C7515D3B033BD4F431D505D67D67E2005F4D0I2B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn01.boxcdn.net/enduser/vendors~app.ad1b5c324e.js
Preview:	/*! For license information please see vendors~app.ad1b5c324e.js.LICENSE.txt */.(window.webpackJsonp=window.webpackJsonp||[]).push([["vendors~app"],{"+5jU5LlWGD":function(e,t,n){var r=n("HMbdZSjBQ4");e.exports=function(e,t){var n=Number(t);return r(e,-n)}},"+6+2nNgl5l":function(e,t,n){var r=n("yNUOxrtTnd");e.exports=function(e){var t=r(e);return t.setMinutes(0,0,0),t}},"+6XX5+lld6":function(e,t,n){var r=n("y1pIOgaOIe");e.exports=function(e){return r(this.__data__,e)>-1}},"+K+bU4dw7B":function(e,t,n){var r=n("JHRd0Wtpo2");e.exports=function(e){var t=new e.constructor(e.byteLength);return new r(t).set(new r(e)),t}},"+QkaJiEUcy":function(e,t,n){var r=n("fmRcAGUJsu"),o=n("t2Dn8l5vat"),i=n("cq/+ZHEllX"),a=n("T1AVtgJeLR"),u=n("GoyQGQ25b1"),s=n("mTTRHTH0TC"),c=n("itsjJeh/nX");e.exports=function e(t,n,l,f,p){t!==n&&i(n,(function(i,s){if(p||(p=new r),u(i))a(t,n,s,l,e,f,p);else{var d=f?f(c(t,s),i,s+"",t,n,p):void 0;void 0===d&&(d=i),o(t,s,d)}}),s)}},"+c4WVrHK/K":function(e,t,n){var r=n("711d4qXG

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\VAHFWDJC\arrow_left_a9cc2824ef3517b6c4160dcf8ff7d410[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	513
Entropy (8bit):	4.720499940334011
Encrypted:	false
SSDEEP:	12:t4BdU/uRqv6DLfBHKFWJCDLfBSU1pRXIFl+MJ4bADc:t4TU/uRff0EcfIU1XXU+t2c
MD5:	A9CC2824EF3517B6C4160DCF8FF7D410
SHA1:	8DB9AEBAD84CA6E4225BFDD2458FF3821CC4F064
SHA-256:	34F9DB946E89F031A80DFCA7B16B2B686469C9886441261AE70A44DA1DFA2D58
SHA-512:	AA3DDAB0A1CFF9533F9A668ABA4FB5E3D75ED9F8AFF8A1CAA4C29F9126D85FF4529E82712C0119D2E81035D1CE1CC491FF9473384D211317D4D00E0E234AD9F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://aadcdn.msftauth.net/ests/2.1/content/images/arrow_left_a9cc2824ef3517b6c4160dcf8ff7d410.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="24" height="24" viewBox="0 0 24 24"><title>assets</title><path d="M18,11.578v.844H7.617l3.921,3.928-.594.594L6,12l4.944-4.944.594.594L7.617,11.578Z" fill="#404040"/><path d="M10.944,7.056l.594.594L7.617,11.578H18v.844H7.617l3.921,3.928-.594.594L6,12l4.944-4.944m0-.141-.071.07L5.929,11.929,5.858,12l.071.071,4.944,4.944.071.07.071-.07.594-.595.071-.07-.071-.071L7.858,12.522H18.1V11.478H7.858l3.751-3.757.071-.071-.071-.07-.594-.595-.071-.07Z" fill="#404040"/></svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\VAHFWDJC\content-sidebar.a7013a9589[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\VAHFWDJC\content-sidebar.a7013a9589[1].css	
Category:	downloaded
Size (bytes):	5630
Entropy (8bit):	5.020963614043702
Encrypted:	false
SSDEEP:	96:jcbFo3CeCC+i8DpMKfi5KCZe+jox8hm8wTy8E5fuG:IhDejSpMKfi0ClSUbL
MD5:	159F5E7E94AF878664C6490270CD2998
SHA1:	EFB4B60AF7A7BB6E543339B4016A60BDC78C7D41
SHA-256:	6E5D870B3EE59E9DAD6A378F1E264C193830BD895FAF1145383E709714A82D76
SHA-512:	C746CF7D3F795CEFAB5EBA4CAC86633563D9C8FF78BE867EB52721D8B55AC927662C5DB71EE80A82D3CB2DE0710329261BEBF1871BFC8EFFA82F462AC8DE5AC3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn01.boxcdn.net/enduser/content-sidebar.a7013a9589.css
Preview:	.bdl-BackButton,.bdl-BackButton:focus,.bdl-BackButton:hover{display:flex}.bcs .bcs-NavButton{position:relative;display:flex;align-items:center;justify-content:center;width:59px;height:60px;background-color:transparent}.bcs .bcs-NavButton:before{position:absolute;top:0;bottom:0;left:-1px;display:block;width:3px;content:"";pointer-events:none}.bcs .bcs-NavButton.bcs-is-selected:before{background-color:#0061d5}.bcs .bcs-NavButton.bcs-is-selected svg .fill-color{fill:#0061d5}.bcs .bcs-NavButton:hover{background-color:#f4f4f4}.bcs .bcs-NavButton:hover:not(.bcs-is-selected) svg .fill-color{fill:#4e4e4e}.bdl-SidebarToggleButton{margin:0 3px;padding:4px;border-radius:4px}.bdl-SidebarToggleButton path{fill:#909090}.bdl-SidebarToggleButton:not(.bdl-is-disabled):hover,.bdl-SidebarToggleButton:not(.is-disabled):hover{background-color:#f4f4f4}.bdl-SidebarToggleButton:not(.bdl-is-disabled):focus,.bdl-SidebarToggleButton:not(.is-disabled):focus{border-color:#96a0a6;box-shadow:0 1px 2px rgba(0,0,0,.1)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\VAHFWDJC\exif.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	10914
Entropy (8bit):	5.5397855270447085
Encrypted:	false
SSDEEP:	192:5p8x/dTa2Cuzp6HWcTz1AVrEgrzMer6Z6L57kpJq/RQ:+/c2Cuzp6HWwhA1xb5eJqJQ
MD5:	0DB669C9033252050E919900AD0BEFA0
SHA1:	23EDB95E1E737E0F23EE6C7CEF07D634236A52E3
SHA-256:	ADD547634768E8CE49D67775D02F958597EFD5E6DF2D1077EF4DFC8C0878B688
SHA-512:	C1BF384AEBA143964831F2F3A7A28566C635C253BC2A4A12C56C56EFC01847F6D39E774B136B8A9062652F9F7929673023C5B3AE13799E40F6754DE7860B294D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn01.boxcdn.net/platform/preview/third-party/doc/2.16.0/exif.min.js
Preview:	(function(){function v(a,c){c||a.match(/^data\:([^\;]+)\;base64,/mi);a=a.replace(/^data\:([^\;]+)\;base64,/gmi,"");for(var b=atob(a),g=b.length,d=new ArrayBuffer(g),e=new Uint8Array(d),h=0;h<g;h++)e[h]=b.charCodeAt(h);return d}function w(a,c){var b=new XMLHttpRequest;b.open("GET",a,!0);b.responseType="blob";b.onload=function(a){200!=this.status&&0!==this.status||c(this.response)};b.send()}function x(a,c){function b(b){var e=t(b);a:{var d=new DataView(b);if(255!=d.getUint8(0)||216!=d.getUint8(1))b=.!1;else{for(var g=2,h=b.byteLength;g<h;){var k=d,f=g;if(56===k.getUint8(f)&&66===k.getUint8(f+1)&&73===k.getUint8(f+2)&&77===k.getUint8(f+3)&&4===k.getUint8(f+4)&&4===k.getUint8(f+5)){k=d.getUint8(g+7);0!==k%2&&(k+=1);0===k&&(k=4);var h=g+8+k,g=d.getUint16(g+6+k),l,d=h;b=new DataView(b);h={};for(k=d;k<d+g;)28===b.getUint8(k)&&2===b.getUint8(k+1)&&(l=b.getUint8(k+2),l in u&&(f=b.getInt16(k+3),l=u[l],f=q(b,k+5,f),h.hasOwnProperty(l)?h[l]instanceof Array?h[l].push(f):h[l]=[h[l],f]:h[l]=f)),k++;b

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\VAHFWDJC\favicon-32x32-VwW37b[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 32 x 32, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	1157
Entropy (8bit):	7.424718197664869
Encrypted:	false
SSDEEP:	24:hMkjvNSTHDyCbibxDx4fZ9qMfhkbOTKBN:hdjvA3bc9ENhkbb
MD5:	86AEDF25C0B3AE1224D92E32D80FFEF8
SHA1:	D75B54256BC48B27E6D7DF1C2A6F4635DE2FE5EE
SHA-256:	D1A4A65AC84A381199843B9722E6470470C8093885CF2A6481C2FF0DEF618C64
SHA-512:	13C4E0AF14577A4858D6E85D93E399186FD5F4AD4A836FA014D89C79673FF7E53EE9B06DE271374C70B3B15F72250075CB8F20E690AAAEE93C6698ABF7D6898
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn01.boxcdn.net/_assets/img/favicons/favicon-32x32-VwW37b.png
Preview:	.PNG........IHDR... ... .D.......gAMA......a.....sRGB........ cHRM..z&.............u0...`..:....p..Q<....PLTE....a..a..a..a..a..a..a..a..a..a..a..a..a..a..a..a..a..a..a..a..a..a..a..a..a..a..a..a..a..a..a..`.._.H..w...i....../~......2..._.1~..d..n..`..m..f..c..a...................!u..^."u...........g...j......q.E....G......................F......................g.,{.......U.....A...h..r.............. u..h.:.....e............b...]..j.......q.....}.....n.G...........b...d..v..r.. t....+{.i..z..\........*z.......h..&x.@.......$w.c.....y........a...n.D.........t........a..p...j..%w.f...E...e..h.V.......=..Q..e../}...?...b..p.Y....tRNS... 78.-.....)..*...6...&..W.w....IDAT8.c```dbfa..X........\.X.../.##.#;..N .. .!....10..S .. *.O..(.+7>...)...@V^AQ...%e.9..T..5d!f..bW.....#+#...."...T&.o.W`hdlbjfnaiemckg....,....&.w..........{@`Pp..{hXxDd..BAtLl\\|BbRrJjZ.QFfVv.{.....y..r...E..2.Q%..e.....Y..22:N.Z22..U.5...u.p_h.7X.Y6F.75.....v..N....].=.}...#.b&N..<e

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\VAHFWDJC\jquery-3.1.1.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\VAHFWDJC\loading[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 30 x 30
Category:	downloaded
Size (bytes):	851
Entropy (8bit):	5.9990571488582125
Encrypted:	false
SSDEEP:	12:3yV3DYBupPHJa3DUDYsHEDKBDfEDYOecS3Y4DuBDzEDYSecS3Y4DyBDYs/ln:3yGiPETNIL9XYv9bYgAln
MD5:	2E4AAFDC48FD2295ADE1A275F1BAE547
SHA1:	D35E3EB9261AEF6827067E9D8D0C8C7B796E0AFB
SHA-256:	B3A3C601451C06183AF82CBF2270C4D80F3D5D680EA9960ED0816B506FBB8C33
SHA-512:	8D0A2A583E165AD727F172F2FAD7C3879B5E214D2248628DF464184D1C51C694705D6BA2FD5E92478A1BDEC88E8AE26711213946B2D20470A15C54821AFBB17E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn01.boxcdn.net/platform/preview/2.61.0/en-US/loading.gif
Preview:	GIF89a.....<..a.....!..NETSCAPE2.0.....!..ImageMagick.gamma=0.45455.!.....,.....V.....Zeo.\..u\..be.....~c}.....M.2..../.L..D..:..p;....>..o9..:.....#..!..ImageMagick.gamma=0.45455.!.....,.....!..ImageMagick.gamma=0.45455.!.....,.....V..!..ImageMagick.gamma=0.45455.!.....,.....!..ImageMagick.gamma=0.45455.!.....,.....F.....X...Ek. O{y.....X...,m..q.....?3..:.iJ.p..5s..J\6.....(..!..ImageMagick.gamma=0.45455.!.....,.....V..!..ImageMagick.gamma=0.45455.!.....,.....!..ImageMagick.gamma=0.45455.!.....,.....F.....X...Ek. O{y.....X...,m..q.....?3..:.iJ.p..5s..J\6.....(..!..ImageMagick.gamma=0.45455.!.....,.....V..!..ImageMagick.gamma=0.45455.!.....,.....;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\VAHFWDJC\messagecenter~preview-components~uploads-manager-enduser.4c14b7f15f[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	258193
Entropy (8bit):	5.3294936427684565
Encrypted:	false
SSDEEP:	3072:ze3JHdzVr1YHZvk8H2RDyUlBgxIhVfwYgONQqwQfbk03rzRGtwMNBw6iJGU0QIMA:zeugSiGrgXwS8q2
MD5:	B162BA9687FA94BF290F0F5F14A0ADC9
SHA1:	DBEECDD021104BFEDA7F96F9623961184EB2AAEE
SHA-256:	B39D4AC30BEE183D42B704ED262F19E8EA2F9A375CA17F37D0EF8ADCC2E70CB3
SHA-512:	5BD681A2FBB3CAA119A86062D7967BE0D96320BDE9EB94E46E2DA6F8948A29F1F1194295C0E30267B9453E10FD3A105333E217F79F3E448C47DB496CEFC04F9E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn01.boxcdn.net/enduser/messagecenter~preview-components~uploads-manager-enduser.4c14b7f15f.js
Preview:	/*! For license information please see messagecenter~preview-components~uploads-manager-enduser.4c14b7f15f.js.LICENSE.txt */.(window.webpackJsonp=window.webpackJsonp||[]).push([["messagecenter~preview-components~uploads-manager-enduser"],{"03vecjQMf5":function(e,t,r){"use strict";var n=r("BSXSWhc9DH");function o(e,t){for(var r=0;r<t.length;r++){var n=t[r];n.enumerable=n.enumerable||!1,n.configurable=!0,"value"in n&&(n.writable=!0),Object.defineProperty(e,n.key,n)}}var i=function(){function e(){!function(e,t){if(!(e instanceof t))throw new TypeError("Cannot call a class as a function")}(this,e),this.memoryStore=new n.a;try{this.localStorage=window.localStorage,this.isLocalStorageAvailable=this.canUseLocalStorage()}catch(e){this.isLocalStorageAvailable=!1}}var t,r,i;return t=e,(r=[{key:"buildKey",value:function(e){return"".concat("localStore","/").concat("0","/").concat(e)}},{key:"canUseLocalStorage",value:function(){if(!this.localStorage)return!1;try{return this.localStorage.setItem(thi

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\VAHFWDJC\preview-components~shared-file.ff88431f84[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	192
Entropy (8bit):	4.777419992372014
Encrypted:	false
SSDEEP:	3:1t7EqFxF5MWTL3CEmElEWXanQ6LXsEWXanQ6LXnEDTfjKBF4UARpyEQ+EWXanQ6i:zEqFbS/6EzXsEzXzBF7ARI+EzTi
MD5:	0628C102A3DA83FE10C4AC340F055329
SHA1:	F290C0DC982CA76807C00EEAE59B3335983BBDC4
SHA-256:	B23D25ACC423D13F6DE5278961700C672B481E93EC189A8179BF27AE43824279
SHA-512:	C6A43F897F882A6DAC9585E2C66A1F3BF68012BE1E8870F5E9295B17877AC46751D23ADC9DC02828B837EDDFD28E74D46B6CDD3AE916CF25C72BA7D3AAF898 35
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn01.boxcdn.net/enduser/preview-components~shared-file.ff88431f84.css
Preview:	.MaliciousBanner .icon-alert-circle{margin-right:5px}.EditClassificationButton,.EditClassificationButton:hover{margin-left:6px}@media (max-width:849px){.EditClassificationButton{display:none}}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\VAHFWDJC\preview[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	56511
Entropy (8bit):	5.018999718758012
Encrypted:	false
SSDEEP:	768:SSI0/galv136bUEci7fZ3Mki45g4vcqK7KOdUyUM:Be36gEZZQ4RK7KOdIM
MD5:	5996ADF4A309F66807EB3CB098B02CF7
SHA1:	086DE88D2106957CE92C7D79B70258C1DA88E159
SHA-256:	C94D9E6F0F8679CE72F9D52CCAB973E75CC7A23AE9C8EAF0F1FA25BF7D86C75A
SHA-512:	E53B0C79531A720971AC210168203E1C71A581D4521A8065ABF65FC1B113EDF0051FC151EC12A9D68B7DC2EC93E2293AABB4F2322A704EF02C45A2A28DDEB85 D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn01.boxcdn.net/platform/preview/2.61.0/en-US/preview.css
Preview:	/*!. * Box Content Preview. * . * Copyright 2019 Box, Inc. All rights reserved.. * . * This product includes software developed by Box, Inc. ("Box"). * (http://www.box.com). * . * ALL BOX SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESS OR IMPLIED. * WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF. * MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.. * IN NO EVENT SHALL BOX BE LIABLE FOR ANY DIRECT, I NDIRECT, INCIDENTAL,. * SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT. * LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE,. * DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY. * THEORY OF LIABILITY, W HETHER IN CONTRACT, STRICT LIABILITY, OR TORT. * (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE. * OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.. * . * See the Box license for the specific language governing permissions. * and limitations under the licen

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\VAHFWDJC\shared-file.9493eefcb7[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):	13621
Entropy (8bit):	5.2740190584271796
Encrypted:	false
SSDEEP:	192:QQnwXvKIoruPBcZJymwC49/4TfiFSr5fkro0O9QwyY5F7rftc7FocuVy6:Qks8ueZJ0FtAiFYIpO9Qwvtc7Fej
MD5:	491D7AE9477AE2C9DD45C64E0C5A2B24
SHA1:	44D9D151D9ED85C7D851BB8134B8E147E5576D8C
SHA-256:	B36869FDBB9DE2E6265C817512B9AF78ACA20BC17BDB078D36931BD47C2F40FA
SHA-512:	D2FBAC0830509A286CD41F46063CC4AA4E975C58631424BC4ED063CE7A5F536DD14ECFF802D5F225958E48EB6A9A04AF4E9C0DE5F8D4EF460DD4F3EA60DF10 57
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn01.boxcdn.net/enduser/shared-file.9493eefcb7.js
Preview:	(window.webpackJsonp=window.webpackJsonp||[]).push([["shared-file"],{"8bPKGyOoiP":function(e,t,n){},"9Nyd+vSxbR":function(e,t,n){},eNYSbZFTnr:function(e,t,n){"use strict";var r=n("mv074FmJXE");n.d(t,"a",(function(){return r.a}))},ge6f43AXgi:function(e,t,n){"use strict";n.r(t);var r,a=n("e7SQulcBac"),o=n("8Uoiwx9NYF"),i=n("ctmAoT7YrD"),l=n("jyz5Lsk3MC"),s=n("Iqkazkw3SQ"),c=Object(s.b)("sharedFilePage/GET",(function(e){return Object(l.c)("/app-api/enduserapp/item/".concat(e),{format:"sharedFilePreview"},{exclusiveGroup:i.g})}),{navigation:!0});function u(e,t){var n=Object.keys(e);if(Object.getOwnPropertySymbols){var r=Object.getOwnPropertySymbols(e);t&&(r=r.filter((function(t){return Object.getOwnPropertyDescriptor(e,t).enumerable}))),n.push.apply(n,r)}return n}function d(e){for(var t=1;t<arguments.length;t++){var n=null!=arguments[t]?arguments[t]:{};t%2?u(Object(n),!0).forEach((function(t){f(e,t,n[t])})):Object.getOwnPropertyDescriptors?Object.defineProperties(e,Object.getOwnPropertyDes

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\VAHFWDJC\uploads-manager-enduser.41330e25db[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):	9240
Entropy (8bit):	4.950505849395374
Encrypted:	false
SSDEEP:	192:zhU05Wfn+YW3DZ87/8v8UT8S81/b80d8Fuflf0FfGI0bIUX0fXmvHpY6bXeGX9CZ:z6nauXA
MD5:	2736E5D199EFCFE06501B7F72B3F5DD2
SHA1:	B9B553FBB2DFE567111B7D51CF682EB72D9EB9C6
SHA-256:	6557DF16669DDFB8E5BF239CC8004991B14835680900133108570O2CD051B85A
SHA-512:	7F175FB31672C46A14A8C666E835D85D8CD06C7AD41B07B833DB8FD56C8F6C7AFB02B47979C5E007E6BE189FC7C411D85C2C66E4911369F901CF4CF73850A2F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn01.boxcdn.net/enduser/uploads-manager-enduser.41330e25db.css
Preview:	.bcu-item-label{max-width:300px;overflow:hidden;white-space:nowrap;text-overflow:ellipsis}.bcu-item-icon-name{display:flex;width:100%;height:50px;cursor:default}.bcu-item-icon{flex:0 0 50px;align-items:center}.bcu-item-icon,.bcu-item-name{display:flex;justify-content:center}.bcu-item-name{flex:1;flex-direction:column;align-items:flex-start;overflow:hidden;line-height:15px;text-align:left}.bcu-icon-badge .badges .bottom-right-badge{bottom:-4px;left:calc(100% - 16px)}.bcu-progress-container{z-index:201;width:100%;height:2px;margin-right:40px;background:#e8e8e8;transition:opacity .4s}.bcu-progress-container .bcu-progress{top:0;left:0;max-width:100%;height:2px;background:#0061d5;box-shadow:0 1px 5px 0 #e4f4ff;transition:width .1s}.bcu-item-progress{display:flex;align-items:center}.bcu-progress-label{min-width:35px}.bcu-item-action{width:24px;height:24px}.bcu-item-action .crawler{display:flex;align-items:center;justify-content:center;height:100%}.bcu-item-action button{display:flex}.bcu-ite

C:\Users\user\AppData\Local\Temp\datB0DC.tmp	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 119132, version 1.0
Category:	dropped
Size (bytes):	119132
Entropy (8bit):	**7.991532245734968**
Encrypted:	**true**
SSDEEP:	3072:pECjkMzGFzkgGdoAiZzixFwotRAE9urcBQbtF0roFS:pECjVzIGYZ4Fpx9urUQbtFeoFS
MD5:	3E4A4FC6317C4C2CF35D7C77EC1789C3
SHA1:	40EA0D8678B92988824193587F707E3AEDC4591F
SHA-256:	607EC0A4A29F6A4607F6E0A3CF486E50322DDF66F1F1870150CB69A7061E978D
SHA-512:	F7D639520F4C3A3539AD7506EC1CEBED8107C2A264316FE0E98A15132ACCFE6212A22391F4A7203B6D8304B3222B603F0137BA9ACAC7478F217363EEF4556DE
Malicious:	false
Reputation:	low
Preview:	wOFF.....\.....FFTM.....p.\MGDEF.....7...8.x..GPOS.....z...b...GSUB...x...,...FA..sOS/2....._...`i...cmap.....x.!>cvt .....r....?9..fpgm...T..... ..gasp.....glyf.....a..?.head.....1...6..qfhhea.....!...$....hmtx.....C.2loca.....-&maxp..... ... .L..name.....hpost.....'....)prep.....o.i:webf...T... .....`.V.....=.....y.....x.c`d``..b...`b`e`dj..f.6.f.v.o.F..._.&.?.^.F...*..i..C.x...|M.....!.<.fEI.USS\TcVUTT.E.UUu.RUUWCM5W.U5....Ap".H"b.I.'!..j..g.....o_..Yg...z.z....Jv\..!<. .p..{_....cG.....h1..q.E'.B.!..!...I.s.....W.).T.....a.7QO4...x.-D[.Y....`1B....1M...1v...;E.D;..c.....b.....;.....v^..^...M..&.F.f...u.]Eo..$....7.Vi...&W9]..au}F].T....[>.t.....+..F j.X.^U...jzu}.._W...OS.....M.;.].k.fQ..../.K.h.f..\.vr..... ..#]G..s..:.u.k..\.E..]W..s...u..!.c..\3]s\.\.....r.....-.-..[...n....w.....n...p.....nS..

C:\Users\user\AppData\Local\Temp\datB11C.tmp	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format (Version 2), TrueType, length 84396, version 2.983
Category:	dropped
Size (bytes):	84396
Entropy (8bit):	**7.996116383259223**
Encrypted:	**true**
SSDEEP:	1536:lhWk7aeOTww2X4owbcnRqvjFkw8cyW/fTJnh2r667bZ3fTyG/q+TBpMLB:lHdOk9ojj2a//rFoeutTyG/ZBC
MD5:	8A54EA1AEB67D07C751BD5F03068317B
SHA1:	CFBEE4F2FD7F359A2A60648BB6797CAC1FD4DA3E
SHA-256:	4230A20B841519BDBE4B0C154BAD414E017CF80B3918127D45C4F907EEA07280
SHA-512:	A3CA9E052DBB81A20C71DDD24962CE57E842134A8B30842328410DF3FCF76EED4367C3A5A1148DD11092CF0CF3E29B57040CF79D40AC6450D8234F27204D47E
Malicious:	false
Reputation:	low
Preview:	wOF2.....l.....m...l;.....?FFTM..8...>..F.`.. ..j.....|.6.$..$..(.. ..Z.....9?webf.[/0..B%.^..m.m..[..F...&...v....!.....i.V]\.l....b.a..96....H.....J...../....3.H...X.g.** .j.....v.!p4.-.l....P..i..1vTS..}..&A.Z..FT}?([..j..[.....c.*.@...LmwV...B.A.9$!.....z..'..C.1.....$!...uu....>.....4....R&..}9.h-.T../..Iz.....W>.....7..u...z~...V...~2....b.>....{~e[..HP:qT.L.o..P .hF..B...U.w.+E..o..dV>.....,.U^L..... .....Y.pN.....{1T...V.....|.&.?/Q...|4.I.k.... .v..T...;....7B..]..|..R_.].|..D.:b.....%.....D.*./.!.@.....;p.%.g...w..(|...[.9.....T...y.,... .N.i.. L..AVe.>..B.e.H.O!?.@/..ku.f.....w...Xg..YR.gD....i=...\.$Y.iG.....F...CN.(|.A.{\..K5x....>i!....".....N..0.R.y...G.A..jt.Lg.ML.`.....3Y{=.m$..x....%..|f.wvU..\...R.x....._...tl.NH._.Y .....2....r.).J.....R..DLo.zG.U.xj.4..~..7G=!.....*.X&.(.a.-.....$..;._qL.,.d..i..XJ5.P.-{.....J.$o@b...l.h....r..5..i..Jx@..T..I.Nt/."7.z.K>2...\

C:\Users\user\AppData\Local\Temp\datD57D.tmp	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	OpenType font data
Category:	dropped
Size (bytes):	1120

C:\Users\user\AppData\Local\Temp\datD57D.tmp	
Entropy (8bit):	3.2457346287152515
Encrypted:	false
SSDEEP:	12:+5H921oNY0p9b1IfSly/VAAc5EK/HU1qsG1bhCEo8+R5+ddmq0/gNV11Mp1VySia:+Z9fuUx1IfSljAP3G6M3B8PBiAo/K
MD5:	1D484FAB22DCBDC5524F6CE660A11548
SHA1:	C232F6E7EBDECD1C69280043B72892971F42A927
SHA-256:	FF1770728D19AFB5774E0DF68FCB04D6571F7D3B8F0C200210050277A7B3D491
SHA-512:	F580FDBA03C7E0828C1D38D569FB66AF5D4DDCF6A5B1BEFD687EA4E91C531DB4E6EE91D51BB1624E49115C6393D9D84A076C57F730BC3E47DA451EF3C62C053
Malicious:	false
Reputation:	low
Preview:	OTTO.....0CFF ..u.....FFTMe.6p.....GDEF.....8....OS/2V.c.... ...`cmap.....4...Bhead..E.....6hhea.d.....$hmtx.....X....maxp..P.....nameX.t~.....post...3...x... ... .Q..._.<.....<.....!.....!...Z.....P.....1.....PfEd..... .8.Z.!..... . ...X.X.....<..... ....2.....X...!.....|..... .!XXXlt16106036813770XXXXXXXX

C:\Users\user\AppData\Local\Temp\datD5BD.tmp	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	OpenType font data
Category:	dropped
Size (bytes):	1120
Entropy (8bit):	3.244475780916843
Encrypted:	false
SSDEEP:	12:+5Q921oNY0p9b1IfSly/VAAc5EK/HU1qsG1bhCEo8+R5+ddmq0/gNV11Mp1VJefd:+29fuUx1IfSljAP3G6M3B8PJAo/K
MD5:	0F30F84958B059F2A63FA5A09FCF57AF
SHA1:	C714485CF7B404ABD029CCE348604A0D5857DA7F
SHA-256:	2CFC1D29FD4D862D7C51F7F370C8185B4000F990CC0C39222BAA4D7FF1149053
SHA-512:	9188D4E38719C6C6D9AAED71B7B90E8845029ABC38E73540BD32D28D922708D473C2D4BAF3E2CE554E3F196A7A4A77B092C44911DE2AC0270C387B1FE76CD15
Malicious:	false
Reputation:	low
Preview:	OTTO.....0CFF ..v.....FFTMe.6p.....GDEF.....8....OS/2V.c.... ...`cmap.....4...Bhead..E.....6hhea.d.....$hmtx.....X....maxp..P.....nameX.t~.....post...3...x... ... .Q..._.<.....<.....!.....!...Z.....P.....1.....PfEd..... .8.Z.!..... . ...X.X.....<..... ....2.....X...!.....|..... .!XXXlt16106036814321XXXXXXXX

C:\Users\user\AppData\Local\Temp\datD669.tmp	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	OpenType font data
Category:	dropped
Size (bytes):	1120
Entropy (8bit):	3.2416675246420876
Encrypted:	false
SSDEEP:	12:+5rT921oNY0p9b1IfSly/VAAc5EK/HU1qsG1bhCEo8+R5+ddmq0/gNV11Mp1VWe1:+Z9fuUx1IfSljAP3G6M3B8PWAo/K
MD5:	EC5E2BDD4F7321F86AB1EC6AE73E9F8E
SHA1:	8D187A125F70AE5B4626C59A9D18694F788DB032
SHA-256:	22D11BDAEE4DB6C83381FCC5AFACB578561091ECE9BEFDEF0DD53344A73A308F
SHA-512:	0110B9A5DA8161EA80B51A4BD4E7A4F265393F9EC35C0C724D26F85A299008D7A28B5F4C787A26C65610EED4DA1D49F8411C41A7263873B7C3FCED5AF1381A6
Malicious:	false
Reputation:	low
Preview:	OTTO.....0CFF ..w.....FFTMe.6p.....GDEF.....8....OS/2V.c.... ...`cmap.....4...Bhead..E.....6hhea.d.....$hmtx.....X....maxp..P.....nameX.t~.....post...3...x... ... .Q..._.<.....<.....!.....!...Z.....P.....1.....PfEd..... .8.Z.!..... . ...X.X.....<..... ....2.....X...!.....|..... .!XXXlt16106036816142XXXXXXXX

C:\Users\user\AppData\Local\Temp\datD6C8.tmp	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	OpenType font data
Category:	dropped
Size (bytes):	1120
Entropy (8bit):	3.241140658154782
Encrypted:	false
SSDEEP:	12:+5ir921oNY0p9b1IfSly/VAAc5EK/HU1qsG1bhCEo8+R5+ddmq0/gNV11Mp1V6oa:+Er9fuUx1IfSljAP3G6M3B8PnAo/K
MD5:	128D020DAB462EA658834BD7FB3A11F0

C:\Users\user\AppData\Local\Temp\datD6C8.tmp	
SHA1:	3E845BB03AB40F562A0D4F4C0DB9C6E72A389D00
SHA-256:	8B8B068732EAF052EAFE23700A7BD60D636CB5D2CE0D76C918EC4C6F05EE2A81
SHA-512:	2E89498296973EE365E95F7734C67993F752DB4ABCD0035FEE3F7A979292FED7EFB23C3F3FB2821507866BB6D6190DCB1E98B8BB3F80BF61CFE41DDCCD1F241B
Malicious:	false
Reputation:	low
Preview:	OTTO.....0CFF ..x.....FFTMe.6p.....GDEF.....8....OS/2V.c.... ...`cmap.....4...Bhead..E.....6hhea.d.....$hmtx.....X....maxp..P.....nameX.t~.....post...3...x... ... .Q..._.<.....<.....!.....!...Z.....P.....1.....PfEd..... .8.Z.!..... . ...X.X.....<..... ....2.....X...!.....|..... .!XXXlt16106036816703XXXXXXXX

C:\Users\user\AppData\Local\Temp\datDB4D.tmp	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	OpenType font data
Category:	dropped
Size (bytes):	1120
Entropy (8bit):	3.2475203430009656
Encrypted:	false
SSDEEP:	12:+5Jr921oNY0p9b1IfSly/VAAc5EK/HU1qsG1bhCEo8+R5+ddmq0/gNV11Mp1V/9R:+n9fuUx1IfSljAP3G6M3B8P/oAo/K
MD5:	688D3F4D02515B4D8D3C28F1BB5DA9A9
SHA1:	05FDEA155CD804D683AA906E985AE0BEE0432121
SHA-256:	40A06BECF70B2128431CDA6EDC8AE7D19D55E2A44548BBE9C99009BE06A171E7
SHA-512:	1824FA34099F7D9718C8795C510EEFBBC0886333DC6FFC0D188280CE5F2571F12D13DF9902FF10FE6915076533F4C9E18BB1005378609593D9528D7F0C12396B
Malicious:	false
Reputation:	low
Preview:	OTTO.....0CFF ..z.....FFTMe.6p.....GDEF.....8....OS/2V.c.... ...`cmap.....4...Bhead..E.....6hhea.d.....$hmtx.....X....maxp..P.....nameX.t~.....post...3...x... ... .Q..._.<.....<.....!.....!...Z.....P.....1.....PfEd..... .8.Z.!..... . ...X.X.....<..... ....2.....X...!.....|..... .!XXXlt16106036828714XXXXXXXX

C:\Users\user\AppData\Local\Temp\datDBAC.tmp	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	TrueType Font data, 13 tables, 1st "OS/2", 20 names, Macintosh, Original licenceOpenSans-RegularUnknownuniqueIDOpenSans-RegularVersion 0.11UnknownUnknownUnknow
Category:	dropped
Size (bytes):	11776
Entropy (8bit):	4.775123392084225
Encrypted:	false
SSDEEP:	192:IdMfvHMIC6+gACms4hUalhsEM8CSURjXkru3YEL:7HHMIzmSwh5BotXkru3Yg
MD5:	46BB280807C177145F9B587B18566B4F
SHA1:	A709A7DE17FA84B0ADCDB5172B4492F4DB03B84E
SHA-256:	FB7B842A0CDD459E6995360F779433347D160CB57B2730FD3FF2CBFC4EC3BFCC
SHA-512:	BEA516675EBE168CE22E52C253865182BF597C3BDCFABFF39F084A67B5390A9A98930D76012457B4F5E2D4A3A98E46E38A9F6358E094F650C08FB15B06D0745F
Malicious:	false
Reputation:	low
Preview:	.....POS/2}.~.....`cmap.....<...Tcvt .M.....fpgm~a.....4....glyf1W|.....<head..cp...$...6hhea...g...\...$hmtx\T.o.....^locaBk@..."....2maxp.1....*.... name..&W..*4....post.....,.... prepC.....,.....3.....3.....f.....1ASC.@.....X .....H..... .....H.....%.).0.8.D.G.H.I.L.P.Q.R.S.U.W.....N.... .u.....H..... .....@G[ZYXUTSRQPONMLKJIHGFEDCBA@?>=<;:9876510/.-,('&%$#"!... ....., ..`E..% .Fa#E#aH-, E.hD-,E#F`. a .F`..&#HH-,E#F#a. ` .&a. a..&#HH-,E#F`.@a .f`..&#HH-,E#F#a.@` .&a.@a..&#HH-,.. <.<-, E# ..D# ..ZQX# ..D#Y ..QX# .MD#Y ..&QX# ..D#Y!!-, E.hD ..` E.Fvh.E`D-,....C#Ce.-,....C#C.-,..(#p..(>..(#p..(E:.....-, E..%Ead.PQXED.!!Y-,I..#D-, E..C`D-,...C..Ce.-, i.@a... .,.....b`+.d#da\X..aY-,..E.. ...+.)#D.)z..-,Ee.,#DE.+#D-,KRXED.!!Y-,K

C:\Users\user\AppData\Local\Temp\datDBCC.tmp	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	OpenType font data
Category:	dropped
Size (bytes):	2480
Entropy (8bit):	6.289148570221438
Encrypted:	false
SSDEEP:	48:YDaJdw1uhebZvJx1AAQJtWEUBYUFC3ILXsXZkD:TJ2rZvJwAMMCWHsJk
MD5:	FF656FE36DB1BB7388ABFE4CAEECE694
SHA1:	BBC7B8EBD5148DB0AB7FE85F3F3564455A058B96
SHA-256:	ECB6725783F6676220D7F7F387C68A72C034F534E3E26D84380650C5DED376D9
SHA-512:	734F6A04C34CD949CD9C11AAF46FC4494ED373674EB449D2D5763DC97B859A6833D8C900762759583F86E5A6EFEB305F05F062251D3FBB32190387523715A5B6

C:\Users\user\AppData\Local\Temp\datDBCC.tmp	
Malicious:	false
Reputation:	low
Preview:	OTTO.....CFF ..G.....OS/2.:+....,...`cmap...<.....,head.'O.....6hhea...-.....$hmtx.b.....,maxp..P....@....name./v!...H...Fpost..... .....AUFRIW+MinionPro-Regular. ...A.....q.....l.%....Q.$.....AdobeIdentityCopyright 1990, 1991, 1992, 1994, 1997, 1998, 2000, 2002, 2004 Adobe Systems Incorporated. All rights reserved. Minion is either a registered trademark or a trademark of Adobe Systems Incorporated in the United States and/or other countries./FSType 8 def MinionPro-Regular.....P.R.....w...2.....G.....$.....P...P..8....>...>.....>...>.....>...>.....>...>.... ..%.....n....5..%.6..5..p.....h.Z...M-.....$.....n...\. 2$..45. .OBj.....1|.....[.....-..f...;.H.T.$.!.I.K.+...l.\.-...>.wg.....g.T'....!$...P.O.....B.....w....{...,.(....f~N{\..t....M....q.....'..1. .}..{.:J.....I....VD8.V.m.....T.....Z.....ige{c.E=.....

C:\Users\user\AppData\Local\Temp\datDBDD.tmp	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	TrueType Font data, 13 tables, 1st "OS/2", 20 names, Macintosh, Original licenceOpenSans-LightUnknownuniqueIDOpenSans-LightVersion 0.11UnknownUnknownUnknown
Category:	dropped
Size (bytes):	6544
Entropy (8bit):	6.21147302373066
Encrypted:	false
SSDEEP:	192:5+XWvHMIC6+gACms4hUalH72Q5s14Ew7Idr+RS:oAHMIzmSwve+Ebrp
MD5:	7C04F6E1105B1E608EDAC9D6E07C3069
SHA1:	3CE867A0E94539E438CD8743433A26385E9AF16C
SHA-256:	8C478590761204B281EA8871AC003CCBB4152130955F8E424C19D22F1CD778BD
SHA-512:	E2B848307897514664691293EE3D0A33854D2555C5EAC31E8C4418FD64A97A29BBC91C2F3087B30C54B024465655055B6625CD89B8E5E874818F9439E6D3E07
Malicious:	false
Reputation:	low
Preview:	...........POS/2}9{.....`cmap.....<...Rcvt .....fpgm~a.....<....glyf0.).....head..F.....6hhea.....$hmtxF..l...@...vloca1./.....maxp.....x... name.6.a.....post.....4... prep..]...T...:.....,.....3.....3.....f.....1ASC.@.....X .....?..... .....F.....]...).-.D.F.G.H.I.K.L.O.Q.R.U.V.W.X.\.....N.....u..... ?.....Z.^.W.R.^.a.[.Y.`.R.V...R.R.p..@G[ZYXUTSRQPONMLKJIHGFEDCBA@?>=<;:9876510/.-,('&% $#"!....., ..`E..% .Fa#E#aH-, E.hD-,E#F`. a .F`..&#HH-,E#F#a. ` .&a. a..&#HH-,E#F`.@a .f`..&#HH-,E#F#a.@` .&a.@a..&#HH-,.. <.<-, E# ..D# ..ZQX# ..D#Y ..QX# .MD#Y ..&QX# ..D#Y!-, E.hD ..` E.Fvh.E`D-,....C#Ce.-,....C#C.-,..(#p..(>..(#p..(E:.....-, E..%Ead.PQXED.!!Y-,I..#D-, E..C`D-,...C..Ce.-, i.@a... .,.....b`+.d#da\X..aY-,..E..... +.)#D.)z..-,Ee.,#DE.+#D-,KRXE

C:\Users\user\AppData\Local\Temp\datDBFD.tmp	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	TrueType Font data, 13 tables, 1st "OS/2", 20 names, Macintosh, Original licenceOpenSans-BoldUnknownuniqueIDOpenSans-BoldVersion 0.11UnknownUnknownUnknown
Category:	dropped
Size (bytes):	5476
Entropy (8bit):	6.009557126893462
Encrypted:	false
SSDEEP:	96:MxE/oIaTLuA0MMICqQy+gCnpCZyrs4hU6xla9D/AdfHbPXU3crD1K:McUTvHMIC6+gACkrs4hUalieMiDc
MD5:	3FBB4D3BF2AF971A8A15B891EB81318F
SHA1:	384D8045D9848AD949609C476BFE1A72B297E32D
SHA-256:	A797B01B0EFAF43867B227E8CA83E5C7D28C26D854341A630EDF19ABFC6B941A
SHA-512:	0CEDB0AD5AC0B081CC227DDA66772C42BD3D17402ED8EA8BB5A08C39CE10B0BE225F29ECA1789F03A5BF9034F6CE16BFCD2D8753DEAE975D8151190631E16EB
Malicious:	false
Reputation:	low
Preview:	...........POS/2~.....`cmap.x....<...@cvt .-.....|....fpgm.s.u...(....glyf_..l.....head.El.... ...6hhea.).....X...$hmtx4].K...|...nloca!. c.....maxp..... name..$.....post.....L... prep...k...l.....3.....3.....f.....1ASC. .....X .....^..... .....4.....[.'.).3.D.G.O.Q.R.Z.....u.....^...{..... .....V.....+.....T..@G[ZYXUTSRQPONMLKJIHGFEDCBA@?>=<;:9876510/.-,('&%$#"!....., ..`E..% .Fa#E#aH-, E.hD-,E#F`. a .F`..&#HH-,E#F#a. ` .&a. a..&#HH-,E#F`.@a .f`..&#HH-,E#F#a.@` .&a.@a..&#HH-,.. <.<-, E# ..D# ..ZQX# ..D#Y ..QX# .MD#Y ..&QX# ..D#Y!-, E.hD ..` E.Fvh.E`D-,....C#Ce.-,....C#C.-,..(#p..(>..(#p..(E:.....-, E..%Ead.PQXED.!!Y-,I..#D-, E..C`D-,...C..Ce.-, i.@a... .,.....b`+.d#da\X..aY-,..E.....+.)#D.)z..-,Ee.,#DE.+#D-,KRXED.!!Y-,KQXED.!!Y-,..

C:\Users\user\AppData\Local\Temp\datE100.tmp	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	OpenType font data
Category:	dropped
Size (bytes):	3296
Entropy (8bit):	6.732725932253368
Encrypted:	false
SSDEEP:	96:/T2qvV7KqltXu3iSoXoJnQOu56LlgtRGTwxXYr:/T2qN7Kodu3iSNQ5qQWwhY
MD5:	0253F91F8BAD3DFB6BB945944829C1A3
SHA1:	D91BFCDD77C43B77DF6114FD6861CF52BE44AC20
SHA-256:	6A0BF1DE617FEF62E9A311707988404732D12F07DC03312EE28EE3285223147C
SHA-512:	2E6A72C3E4C72D18FCD3C7E0B95A26D01BD3E157FD55962AFC87B212BC0FFC1D5A13419B13355AA281A4BCC82B39E1887FEA8167AF76CB599573332E1C57CB4
Malicious:	false

C:\Users\user\AppData\Local\Temp\datE100.tmp	
Reputation:	low
Preview:	OTTO........CFF ..C........OS/2.],....T...`cmap...C.......,head.'O........6hhea...4.......$hmtx.M.....<...Hmaxp..P.........name...........4post........... ....AUFRIW+MinionPro-Bold....A ....^.%....f.$...............AdobeIdentityCopyright 1990, 1991, 1992, 1994, 1997, 1998, 2000, 2002, 2004 Adobe Systems Incorporated. All rights reserved. Minion is either a registered trademark or a trademark of Adobe Systems Incorporated in the United States and/or other countries./FSType 8 defMinionPro-Bold ..............Q.T...P.n...?...#.....V...;.....S...........$......P...P..8....>...>.........>...>.........>...>.........>...>........z}...Qv....[.....X..%...A....p.>...i...}w^{k{ozqE.R.n...............E.'....(8= 2P._.d....2MXg7.5.'........g.i.~.~..t...;...\.M.K...............O.}...YWNscqu.G.p.........].....HI.......A._.@.lq[p^.............5.jmvlu........mi.anmNr..h.......I.Y....,...(..........k.`bkk_^.l....,........h.. .....6."...)...%......

C:\Users\user\AppData\Local\Temp\~DF8555B65C2B7E7125.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.48248318527915796
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lozR+9lozRu9lWzRPF2icFQoXQBiro:kBqoIjVOJC1
MD5:	ACE47988F48C885DF6575DE831EBB643
SHA1:	FE14851371D724EF77DE214F276D34234BB30E7A
SHA-256:	DFE997F837C3F439F1451D614BC2A02B9AF63C9CD75150CACC8DA69F1DD9714D
SHA-512:	9E4AE0870C91E719EE31C41AA1AC50EDEF569C227BFAC7A16BFD1FF7F6F7CB8583B3E78E624FB0F371E37D35A1DE83E69B91CE842FDC2B1A17A67322564717 0
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(................... ....*%..H..M..{y..+.0...(................... ....

C:\Users\user\AppData\Local\Temp\~DF957A63CC4223DA9F.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.2883653032372121
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laAQ:kBqoxxJhHWSVSEab
MD5:	E90A5E9A94E193FC6CB5B52CA833ADD9
SHA1:	D85DAAC5BB4FE040A6549D50D739596418E0E92D
SHA-256:	A234F1EFD8F0DE144819415460FC735E3FCC50AD3AD0D4FAB4357B69DF5E21C9
SHA-512:	68CA04691F68A4CBF6EA3F0FC14F98EEEBF08B9BDEFDDF2D42DE583518D7D7FEEB4AE3A37D5ABACF2EACB357587EA149A494287F0BD3D941F2E4B2FF1D0B 21AC
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(................... ....*%..H..M..{y..+.0...(................... ....

C:\Users\user\AppData\Local\Temp\~DFF6C89A18730061FE.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	62985
Entropy (8bit):	1.0996864017481822
Encrypted:	false
SSDEEP:	384:kBqoxKAuqR+uoCLYZ1G1gDsg2BPqbhWf6:98MY
MD5:	49ED3DBDEBF06B96C9B5D15736B7A249
SHA1:	94F90E36F238E9EF0FB5E299E99AC8AB32A29D03
SHA-256:	9796C4D91F11B500BBD26C230DE6E731791CABCF113D8E31AA9369FCA8A946C6
SHA-512:	2F4FE5BA8D6D99D1F4FCEFEEB7118EB1CC0071FB2BD8EDA7FD2883BFC46B7CD368825D750D064CF960CE89E2A9F72174B8B0390D165AFFECD7609250811A1I 67
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\~DFF6C89A18730061FE.TMP

Preview:	..............................*%..H..M..{y..+.0...(.................... ....*%..H..M..{y..+.0...(.................... ....

Static File Info

No static file info

Network Behavior

Network Port Distribution

Total Packets: 96

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 21:54:31.532516003 CET	49715	443	192.168.2.7	185.235.236.201
Jan 13, 2021 21:54:31.540534973 CET	49716	443	192.168.2.7	185.235.236.201
Jan 13, 2021 21:54:31.578242064 CET	443	49715	185.235.236.201	192.168.2.7
Jan 13, 2021 21:54:31.578375101 CET	49715	443	192.168.2.7	185.235.236.201
Jan 13, 2021 21:54:31.585973024 CET	443	49716	185.235.236.201	192.168.2.7
Jan 13, 2021 21:54:31.586071014 CET	49716	443	192.168.2.7	185.235.236.201
Jan 13, 2021 21:54:31.587007999 CET	49715	443	192.168.2.7	185.235.236.201
Jan 13, 2021 21:54:31.587600946 CET	49716	443	192.168.2.7	185.235.236.201
Jan 13, 2021 21:54:31.632525921 CET	443	49715	185.235.236.201	192.168.2.7
Jan 13, 2021 21:54:31.632795095 CET	443	49716	185.235.236.201	192.168.2.7
Jan 13, 2021 21:54:31.633369923 CET	443	49715	185.235.236.201	192.168.2.7
Jan 13, 2021 21:54:31.633405924 CET	443	49715	185.235.236.201	192.168.2.7
Jan 13, 2021 21:54:31.633420944 CET	443	49715	185.235.236.201	192.168.2.7
Jan 13, 2021 21:54:31.633474112 CET	49715	443	192.168.2.7	185.235.236.201
Jan 13, 2021 21:54:31.633511066 CET	49715	443	192.168.2.7	185.235.236.201
Jan 13, 2021 21:54:31.633773088 CET	443	49716	185.235.236.201	192.168.2.7
Jan 13, 2021 21:54:31.633791924 CET	443	49716	185.235.236.201	192.168.2.7
Jan 13, 2021 21:54:31.633805990 CET	443	49716	185.235.236.201	192.168.2.7
Jan 13, 2021 21:54:31.633846045 CET	49716	443	192.168.2.7	185.235.236.201
Jan 13, 2021 21:54:31.633877993 CET	49716	443	192.168.2.7	185.235.236.201
Jan 13, 2021 21:54:31.667464018 CET	49716	443	192.168.2.7	185.235.236.201
Jan 13, 2021 21:54:31.667510033 CET	49715	443	192.168.2.7	185.235.236.201
Jan 13, 2021 21:54:31.674616098 CET	49716	443	192.168.2.7	185.235.236.201
Jan 13, 2021 21:54:31.713100910 CET	443	49716	185.235.236.201	192.168.2.7
Jan 13, 2021 21:54:31.713200092 CET	49716	443	192.168.2.7	185.235.236.201

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 21:54:31.713249922 CET	443	49715	185.235.236.201	192.168.2.7
Jan 13, 2021 21:54:31.713316917 CET	49715	443	192.168.2.7	185.235.236.201
Jan 13, 2021 21:54:31.758547068 CET	443	49716	185.235.236.201	192.168.2.7
Jan 13, 2021 21:54:32.010397911 CET	443	49716	185.235.236.201	192.168.2.7
Jan 13, 2021 21:54:32.010432005 CET	443	49716	185.235.236.201	192.168.2.7
Jan 13, 2021 21:54:32.010552883 CET	49716	443	192.168.2.7	185.235.236.201
Jan 13, 2021 21:54:32.014543056 CET	49716	443	192.168.2.7	185.235.236.201
Jan 13, 2021 21:54:32.128570080 CET	443	49716	185.235.236.201	192.168.2.7
Jan 13, 2021 21:54:32.128595114 CET	443	49716	185.235.236.201	192.168.2.7
Jan 13, 2021 21:54:32.128649950 CET	49716	443	192.168.2.7	185.235.236.201
Jan 13, 2021 21:54:32.128683090 CET	49716	443	192.168.2.7	185.235.236.201
Jan 13, 2021 21:54:32.179122925 CET	443	49716	185.235.236.201	192.168.2.7
Jan 13, 2021 21:54:32.179141045 CET	443	49716	185.235.236.201	192.168.2.7
Jan 13, 2021 21:54:32.179224968 CET	49716	443	192.168.2.7	185.235.236.201
Jan 13, 2021 21:54:34.008429050 CET	49716	443	192.168.2.7	185.235.236.201
Jan 13, 2021 21:54:34.093278885 CET	443	49716	185.235.236.201	192.168.2.7
Jan 13, 2021 21:54:34.740958929 CET	443	49716	185.235.236.201	192.168.2.7
Jan 13, 2021 21:54:34.740995884 CET	443	49716	185.235.236.201	192.168.2.7
Jan 13, 2021 21:54:34.741061926 CET	49716	443	192.168.2.7	185.235.236.201
Jan 13, 2021 21:54:34.741091967 CET	49716	443	192.168.2.7	185.235.236.201
Jan 13, 2021 21:54:37.250329018 CET	49716	443	192.168.2.7	185.235.236.201
Jan 13, 2021 21:54:37.295749903 CET	443	49716	185.235.236.201	192.168.2.7
Jan 13, 2021 21:54:37.309091091 CET	49716	443	192.168.2.7	185.235.236.201
Jan 13, 2021 21:54:37.310475111 CET	49715	443	192.168.2.7	185.235.236.201
Jan 13, 2021 21:54:37.354521036 CET	443	49716	185.235.236.201	192.168.2.7
Jan 13, 2021 21:54:37.356090069 CET	443	49715	185.235.236.201	192.168.2.7
Jan 13, 2021 21:54:37.533370018 CET	443	49715	185.235.236.201	192.168.2.7
Jan 13, 2021 21:54:37.533539057 CET	49715	443	192.168.2.7	185.235.236.201
Jan 13, 2021 21:54:37.565794945 CET	443	49716	185.235.236.201	192.168.2.7
Jan 13, 2021 21:54:37.565835953 CET	443	49716	185.235.236.201	192.168.2.7
Jan 13, 2021 21:54:37.565962076 CET	49716	443	192.168.2.7	185.235.236.201
Jan 13, 2021 21:54:37.657439947 CET	49724	443	192.168.2.7	185.235.236.197
Jan 13, 2021 21:54:37.657951117 CET	49725	443	192.168.2.7	185.235.236.197
Jan 13, 2021 21:54:37.702824116 CET	443	49724	185.235.236.197	192.168.2.7
Jan 13, 2021 21:54:37.702939034 CET	49724	443	192.168.2.7	185.235.236.197
Jan 13, 2021 21:54:37.703459024 CET	443	49725	185.235.236.197	192.168.2.7
Jan 13, 2021 21:54:37.703522921 CET	49725	443	192.168.2.7	185.235.236.197
Jan 13, 2021 21:54:37.703763008 CET	49724	443	192.168.2.7	185.235.236.197
Jan 13, 2021 21:54:37.704246044 CET	49725	443	192.168.2.7	185.235.236.197
Jan 13, 2021 21:54:37.749064922 CET	443	49724	185.235.236.197	192.168.2.7
Jan 13, 2021 21:54:37.749691010 CET	443	49725	185.235.236.197	192.168.2.7
Jan 13, 2021 21:54:37.750561953 CET	443	49724	185.235.236.197	192.168.2.7
Jan 13, 2021 21:54:37.750579119 CET	443	49724	185.235.236.197	192.168.2.7
Jan 13, 2021 21:54:37.750595093 CET	443	49724	185.235.236.197	192.168.2.7
Jan 13, 2021 21:54:37.750638008 CET	49724	443	192.168.2.7	185.235.236.197
Jan 13, 2021 21:54:37.750644922 CET	443	49725	185.235.236.197	192.168.2.7
Jan 13, 2021 21:54:37.750662088 CET	49724	443	192.168.2.7	185.235.236.197
Jan 13, 2021 21:54:37.750665903 CET	443	49725	185.235.236.197	192.168.2.7
Jan 13, 2021 21:54:37.750679970 CET	443	49725	185.235.236.197	192.168.2.7
Jan 13, 2021 21:54:37.750710011 CET	49725	443	192.168.2.7	185.235.236.197
Jan 13, 2021 21:54:37.750725031 CET	49725	443	192.168.2.7	185.235.236.197
Jan 13, 2021 21:54:37.758105040 CET	49725	443	192.168.2.7	185.235.236.197
Jan 13, 2021 21:54:37.758131027 CET	49724	443	192.168.2.7	185.235.236.197
Jan 13, 2021 21:54:37.758577108 CET	49725	443	192.168.2.7	185.235.236.197
Jan 13, 2021 21:54:37.803649902 CET	443	49724	185.235.236.197	192.168.2.7
Jan 13, 2021 21:54:37.803770065 CET	49724	443	192.168.2.7	185.235.236.197
Jan 13, 2021 21:54:37.803816080 CET	443	49725	185.235.236.197	192.168.2.7
Jan 13, 2021 21:54:37.803880930 CET	49725	443	192.168.2.7	185.235.236.197
Jan 13, 2021 21:54:37.843813896 CET	443	49725	185.235.236.197	192.168.2.7
Jan 13, 2021 21:54:37.946600914 CET	443	49725	185.235.236.197	192.168.2.7
Jan 13, 2021 21:54:37.946718931 CET	49725	443	192.168.2.7	185.235.236.197
Jan 13, 2021 21:54:37.950887918 CET	49725	443	192.168.2.7	185.235.236.197
Jan 13, 2021 21:54:37.996620893 CET	443	49725	185.235.236.197	192.168.2.7
Jan 13, 2021 21:54:37.996646881 CET	443	49725	185.235.236.197	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 21:54:38.405431032 CET	443	49725	185.235.236.197	192.168.2.7
Jan 13, 2021 21:54:38.405456066 CET	443	49725	185.235.236.197	192.168.2.7
Jan 13, 2021 21:54:38.405514002 CET	49725	443	192.168.2.7	185.235.236.197
Jan 13, 2021 21:54:38.405554056 CET	49725	443	192.168.2.7	185.235.236.197
Jan 13, 2021 21:54:40.348809004 CET	49727	443	192.168.2.7	185.235.236.200
Jan 13, 2021 21:54:40.349045038 CET	49728	443	192.168.2.7	185.235.236.200
Jan 13, 2021 21:54:40.394280910 CET	443	49727	185.235.236.200	192.168.2.7
Jan 13, 2021 21:54:40.394428968 CET	443	49728	185.235.236.200	192.168.2.7
Jan 13, 2021 21:54:40.394489050 CET	49728	443	192.168.2.7	185.235.236.200
Jan 13, 2021 21:54:40.395777941 CET	49728	443	192.168.2.7	185.235.236.200
Jan 13, 2021 21:54:40.396322012 CET	49727	443	192.168.2.7	185.235.236.200

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 21:54:25.676650047 CET	54329	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:54:25.724584103 CET	53	54329	8.8.8.8	192.168.2.7
Jan 13, 2021 21:54:26.504887104 CET	58052	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:54:26.552870989 CET	53	58052	8.8.8.8	192.168.2.7
Jan 13, 2021 21:54:27.456772089 CET	54008	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:54:27.504637003 CET	53	54008	8.8.8.8	192.168.2.7
Jan 13, 2021 21:54:28.362469912 CET	59451	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:54:28.410332918 CET	53	59451	8.8.8.8	192.168.2.7
Jan 13, 2021 21:54:29.978077888 CET	52914	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:54:30.025906086 CET	53	52914	8.8.8.8	192.168.2.7
Jan 13, 2021 21:54:30.325284004 CET	64569	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:54:30.384568930 CET	53	64569	8.8.8.8	192.168.2.7
Jan 13, 2021 21:54:31.448714018 CET	52816	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:54:31.517805099 CET	53	52816	8.8.8.8	192.168.2.7
Jan 13, 2021 21:54:32.068841934 CET	50781	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:54:32.127919912 CET	53	50781	8.8.8.8	192.168.2.7
Jan 13, 2021 21:54:36.315941095 CET	54230	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:54:36.372370958 CET	53	54230	8.8.8.8	192.168.2.7
Jan 13, 2021 21:54:37.587527990 CET	54911	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:54:37.650433064 CET	49958	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:54:37.655072927 CET	53	54911	8.8.8.8	192.168.2.7
Jan 13, 2021 21:54:37.698333025 CET	53	49958	8.8.8.8	192.168.2.7
Jan 13, 2021 21:54:40.288410902 CET	50860	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:54:40.346477032 CET	53	50860	8.8.8.8	192.168.2.7
Jan 13, 2021 21:54:40.503601074 CET	50452	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:54:40.554389000 CET	53	50452	8.8.8.8	192.168.2.7
Jan 13, 2021 21:54:42.946566105 CET	59730	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:54:42.997251034 CET	53	59730	8.8.8.8	192.168.2.7
Jan 13, 2021 21:54:50.350574017 CET	59310	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:54:50.408438921 CET	53	59310	8.8.8.8	192.168.2.7
Jan 13, 2021 21:54:50.882656097 CET	51919	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:54:50.941672087 CET	53	51919	8.8.8.8	192.168.2.7
Jan 13, 2021 21:54:51.157852888 CET	64296	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:54:51.217111111 CET	53	64296	8.8.8.8	192.168.2.7
Jan 13, 2021 21:54:51.723078012 CET	56680	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:54:51.770989895 CET	53	56680	8.8.8.8	192.168.2.7
Jan 13, 2021 21:54:52.705688953 CET	58820	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:54:52.756361961 CET	53	58820	8.8.8.8	192.168.2.7
Jan 13, 2021 21:54:54.733489990 CET	60983	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:54:54.781517982 CET	53	60983	8.8.8.8	192.168.2.7
Jan 13, 2021 21:54:54.950824022 CET	49247	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:54:55.167629957 CET	53	49247	8.8.8.8	192.168.2.7
Jan 13, 2021 21:54:56.114928007 CET	52286	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:54:56.162833929 CET	53	52286	8.8.8.8	192.168.2.7
Jan 13, 2021 21:54:56.348973036 CET	56064	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:54:56.399971008 CET	53	56064	8.8.8.8	192.168.2.7
Jan 13, 2021 21:54:56.485903025 CET	63744	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:54:56.542682886 CET	53	63744	8.8.8.8	192.168.2.7
Jan 13, 2021 21:54:56.665409088 CET	61457	53	192.168.2.7	8.8.8.8

Copyright null 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 21:54:56.716202974 CET	53	61457	8.8.8.8	192.168.2.7
Jan 13, 2021 21:54:57.524045944 CET	58367	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:54:57.571928024 CET	53	58367	8.8.8.8	192.168.2.7
Jan 13, 2021 21:55:00.344216108 CET	60599	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:55:00.392049074 CET	53	60599	8.8.8.8	192.168.2.7
Jan 13, 2021 21:55:01.011658907 CET	59571	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:55:01.068286896 CET	53	59571	8.8.8.8	192.168.2.7
Jan 13, 2021 21:55:01.344687939 CET	60599	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:55:01.392580986 CET	53	60599	8.8.8.8	192.168.2.7
Jan 13, 2021 21:55:02.016978979 CET	59571	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:55:02.065083981 CET	53	59571	8.8.8.8	192.168.2.7
Jan 13, 2021 21:55:02.362363100 CET	60599	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:55:02.418446064 CET	53	60599	8.8.8.8	192.168.2.7
Jan 13, 2021 21:55:02.854703903 CET	52689	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:55:02.921499014 CET	53	52689	8.8.8.8	192.168.2.7
Jan 13, 2021 21:55:03.032315969 CET	59571	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:55:03.080209017 CET	53	59571	8.8.8.8	192.168.2.7
Jan 13, 2021 21:55:04.376132965 CET	60599	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:55:04.423965931 CET	53	60599	8.8.8.8	192.168.2.7
Jan 13, 2021 21:55:05.048110962 CET	59571	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:55:05.096009016 CET	53	59571	8.8.8.8	192.168.2.7
Jan 13, 2021 21:55:08.376619101 CET	60599	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:55:08.424896002 CET	53	60599	8.8.8.8	192.168.2.7
Jan 13, 2021 21:55:09.048597097 CET	59571	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:55:09.104763985 CET	53	59571	8.8.8.8	192.168.2.7
Jan 13, 2021 21:55:14.017033100 CET	50290	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:55:14.065198898 CET	53	50290	8.8.8.8	192.168.2.7
Jan 13, 2021 21:55:14.168950081 CET	60427	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:55:14.216995955 CET	53	60427	8.8.8.8	192.168.2.7
Jan 13, 2021 21:55:15.693655014 CET	56209	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:55:15.752923965 CET	53	56209	8.8.8.8	192.168.2.7
Jan 13, 2021 21:55:19.182723045 CET	59582	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:55:19.230617046 CET	53	59582	8.8.8.8	192.168.2.7
Jan 13, 2021 21:55:24.739811897 CET	60949	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:55:24.797482967 CET	53	60949	8.8.8.8	192.168.2.7
Jan 13, 2021 21:55:32.770812035 CET	58542	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:55:32.829925060 CET	53	58542	8.8.8.8	192.168.2.7
Jan 13, 2021 21:55:33.414207935 CET	59179	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:55:33.470340967 CET	53	59179	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 13, 2021 21:54:31.448714018 CET	192.168.2.7	8.8.8.8	0x26ee	Standard query (0)	app.box.com	A (IP address)	IN (0x0001)
Jan 13, 2021 21:54:32.068841934 CET	192.168.2.7	8.8.8.8	0x148d	Standard query (0)	cdn01.boxcdn.net	A (IP address)	IN (0x0001)
Jan 13, 2021 21:54:37.587527990 CET	192.168.2.7	8.8.8.8	0x1e15	Standard query (0)	api.box.com	A (IP address)	IN (0x0001)
Jan 13, 2021 21:54:40.288410902 CET	192.168.2.7	8.8.8.8	0xc8e6	Standard query (0)	public.box cloud.com	A (IP address)	IN (0x0001)
Jan 13, 2021 21:54:51.157852888 CET	192.168.2.7	8.8.8.8	0xc4cc	Standard query (0)	cdn01.boxcdn.net	A (IP address)	IN (0x0001)
Jan 13, 2021 21:54:54.950824022 CET	192.168.2.7	8.8.8.8	0x8c60	Standard query (0)	costa-rica-infos.com	A (IP address)	IN (0x0001)
Jan 13, 2021 21:54:56.114928007 CET	192.168.2.7	8.8.8.8	0x8dea	Standard query (0)	cdnjs.clou dflare.com	A (IP address)	IN (0x0001)
Jan 13, 2021 21:54:56.485903025 CET	192.168.2.7	8.8.8.8	0x533a	Standard query (0)	aadcdn.msf tauth.net	A (IP address)	IN (0x0001)
Jan 13, 2021 21:54:56.665409088 CET	192.168.2.7	8.8.8.8	0x3cd5	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)

DNS Answers

Copyright null 2021

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 13, 2021 21:54:31.517805099 CET	8.8.8.8	192.168.2.7	0x26ee	No error (0)	app.box.com		185.235.236.201	A (IP address)	IN (0x0001)
Jan 13, 2021 21:54:32.127919912 CET	8.8.8.8	192.168.2.7	0x148d	No error (0)	cdn01.boxcdn.net	cdn01.boxcdn.net.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 21:54:37.655072927 CET	8.8.8.8	192.168.2.7	0x1e15	No error (0)	api.box.com		185.235.236.197	A (IP address)	IN (0x0001)
Jan 13, 2021 21:54:40.346477032 CET	8.8.8.8	192.168.2.7	0xc8e6	No error (0)	public.boxcloud.com		185.235.236.200	A (IP address)	IN (0x0001)
Jan 13, 2021 21:54:51.217111111 CET	8.8.8.8	192.168.2.7	0xc4cc	No error (0)	cdn01.boxcdn.net	cdn01.boxcdn.net.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 21:54:55.167629957 CET	8.8.8.8	192.168.2.7	0x8c60	No error (0)	costa-rica-infos.com		162.219.248.247	A (IP address)	IN (0x0001)
Jan 13, 2021 21:54:56.162833929 CET	8.8.8.8	192.168.2.7	0x8dea	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Jan 13, 2021 21:54:56.162833929 CET	8.8.8.8	192.168.2.7	0x8dea	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Jan 13, 2021 21:54:56.542682886 CET	8.8.8.8	192.168.2.7	0x533a	No error (0)	aadcdn.msftauth.net	aadcdnoriginneu.azureedge.net		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 21:54:56.542682886 CET	8.8.8.8	192.168.2.7	0x533a	No error (0)	cs1100.wpc.omegacdn.net		152.199.23.37	A (IP address)	IN (0x0001)
Jan 13, 2021 21:54:56.716202974 CET	8.8.8.8	192.168.2.7	0x3cd5	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 13, 2021 21:54:31.633420944 CET	185.235.236.201	443	192.168.2.7	49715	CN=app.box.com, O="Box, Inc.", L=Redwood City, ST=California, C=US CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Jun 23 02:00:00 CEST 2020	Sat Jul 23 14:00:00 CEST 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=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:45 CET 2017	Sat Nov 06 13:23:45 CET 2027		
Jan 13, 2021 21:54:31.633805990 CET	185.235.236.201	443	192.168.2.7	49716	CN=app.box.com, O="Box, Inc.", L=Redwood City, ST=California, C=US CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Jun 23 02:00:00 CEST 2020	Sat Jul 23 14:00:00 CEST 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=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:45 CET 2017	Sat Nov 06 13:23:45 CET 2027		
Jan 13, 2021 21:54:37.750595093 CET	185.235.236.197	443	192.168.2.7	49724	CN=*.box.com, O="Box, Inc.", L=Redwood City, ST=California, C=US CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Nov 18 01:00:00 CET 2020	Thu Nov 18 00:59:59 CET 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=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:45 CET 2017	Sat Nov 06 13:23:45 CET 2027		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:45 CET 2017	Sat Nov 06 13:23:45 CET 2027		
Jan 13, 2021 21:54:37.750679970 CET	185.235.236.197	443	192.168.2.7	49725	CN=*.box.com, O="Box, Inc.", L=Redwood City, ST=California, C=US CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Nov 18 01:00:00 CET 2020 Mon Nov 06 13:23:45 CET 2017	Thu Nov 18 00:59:59 CET 2021 Sat Nov 06 13:23:45 CET 2027	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=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:45 CET 2017	Sat Nov 06 13:23:45 CET 2027		
Jan 13, 2021 21:54:40.442269087 CET	185.235.236.200	443	192.168.2.7	49728	CN=*.boxcloud.com, O="Box, Inc.", L=Redwood City, ST=California, C=US CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Feb 07 01:00:00 CET 2018 Mon Nov 06 13:23:45 CET 2017	Fri Feb 19 13:00:00 CET 2021 Sat Nov 06 13:23:45 CET 2027	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=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:45 CET 2017	Sat Nov 06 13:23:45 CET 2027		
Jan 13, 2021 21:54:40.442779064 CET	185.235.236.200	443	192.168.2.7	49727	CN=*.boxcloud.com, O="Box, Inc.", L=Redwood City, ST=California, C=US CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Feb 07 01:00:00 CET 2018 Mon Nov 06 13:23:45 CET 2017	Fri Feb 19 13:00:00 CET 2021 Sat Nov 06 13:23:45 CET 2027	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=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:45 CET 2017	Sat Nov 06 13:23:45 CET 2027		
Jan 13, 2021 21:54:55.563993931 CET	162.219.248.247	443	192.168.2.7	49740	CN=costa-rica-infos.com CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Sun Jan 03 01:00:00 CET 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Sun Apr 04 01:59:59 CEST 2021 Sun May 18 01:59:59 CEST 2025 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="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 13, 2021 21:54:55.564081907 CET	162.219.248.247	443	192.168.2.7	49739	CN=costa-rica-infos.com CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Sun Jan 03 01:00:00 CET 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Sun Apr 04 01:59:59 CEST 2021 Sun May 18 01:59:59 CEST 2025 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="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
Jan 13, 2021 21:54:56.249530077 CET	104.16.18.94	443	192.168.2.7	49742	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		
Jan 13, 2021 21:54:56.253432989 CET	104.16.18.94	443	192.168.2.7	49741	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		
Jan 13, 2021 21:54:56.732206106 CET	152.199.23.37	443	192.168.2.7	49744	CN=aadcdn.msftauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Jul 09 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013 Fri Nov 10 01:00:00 CET 2006	Fri Jul 09 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023 Mon Nov 10 01:00:00 CET 2031	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 SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 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
Jan 13, 2021 21:54:56.733073950 CET	152.199.23.37	443	192.168.2.7	49745	CN=aadcdn.msftauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Jul 09 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013 Fri Nov 10 01:00:00 CET 2006	Fri Jul 09 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023 Mon Nov 10 01:00:00 CET 2031	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 SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
Jan 13, 2021 21:54:56.733692884 CET	152.199.23.37	443	192.168.2.7	49746	CN=aadcdn.msftauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Jul 09 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013 Fri Nov 10 01:00:00 CET 2006	Fri Jul 09 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023 Mon Nov 10 01:00:00 CET 2031	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 SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
Jan 13, 2021 21:54:56.735327959 CET	152.199.23.37	443	192.168.2.7	49747	CN=aadcdn.msftauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Jul 09 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013 Fri Nov 10 01:00:00 CET 2006	Fri Jul 09 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023 Mon Nov 10 01:00:00 CET 2031	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 SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 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
Jan 13, 2021 21:54:56.741228104 CET	152.199.23.37	443	192.168.2.7	49749	CN=aadcdn.msftauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Jul 09 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013 Fri Nov 10 01:00:00 CET 2006	Fri Jul 09 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023 Mon Nov 10 01:00:00 CET 2031	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 SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
Jan 13, 2021 21:54:56.745568991 CET	152.199.23.37	443	192.168.2.7	49748	CN=aadcdn.msftauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Jul 09 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013 Fri Nov 10 01:00:00 CET 2006	Fri Jul 09 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023 Mon Nov 10 01:00:00 CET 2031	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 SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		

Code Manipulations

Statistics

Behavior

● iexplore.exe
● iexplore.exe

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 5696 Parent PID: 792

General

Start time:	21:54:29
Start date:	13/01/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff729180000
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: 5612 Parent PID: 5696

General

Start time:	21:54:30
Start date:	13/01/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5696 CREDAT:17410 /prefetch:2
Imagebase:	0xcc0000
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