ID: 345225
Cookbook: browseurl.jbs
Time: 20:55:54
Date: 27/01/2021
Version: 31.0.0 Emerald

Table of Contents

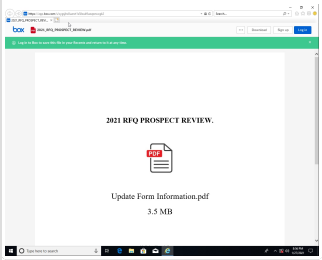
Analysis Report https://app.box.com/s/xygsjhx8uarct1s…

Overview

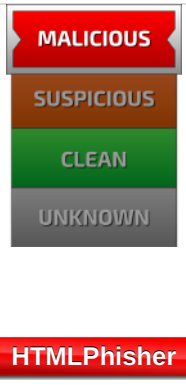
General Information

Sample URL:	http://https://app.box.com/s/xygsjhx8uarct1s5ilzuk9uozpewcgk2
Analysis ID:	345225

Most interesting Screenshot:



Detection



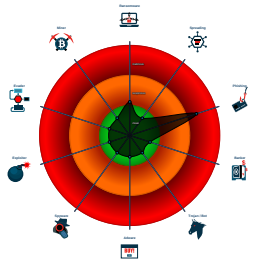
HTMLPhisher

Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for URL or domain
- Yara detected HtmlPhish_10
- Machine Learning detection for dropp…
- 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: 6836 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6880 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6836 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

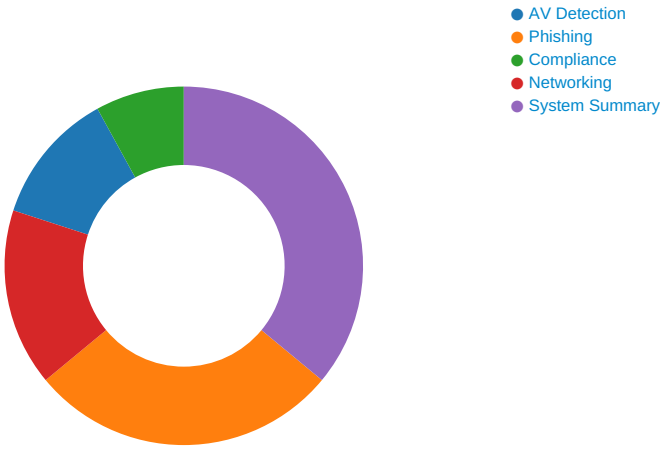
Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\Priv8[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

Antivirus detection for URL or domain

Machine Learning detection for dropped file

Phishing:

Yara detected HtmlPhish_10

Phishing site detected (based on logo template match)

Compliance:

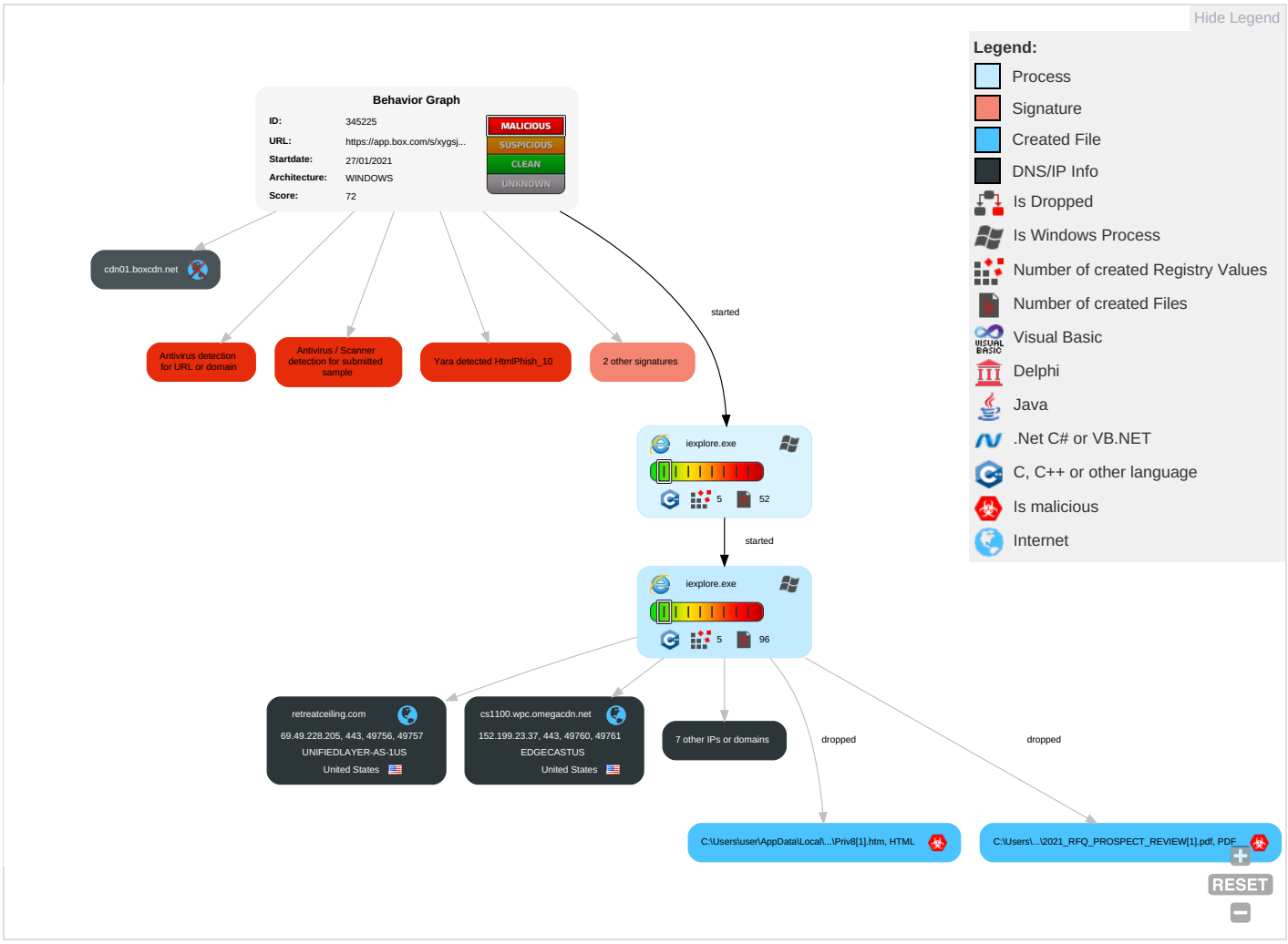
Uses new MSVCR Dlls

Uses secure TLS version for HTTPS connections

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	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

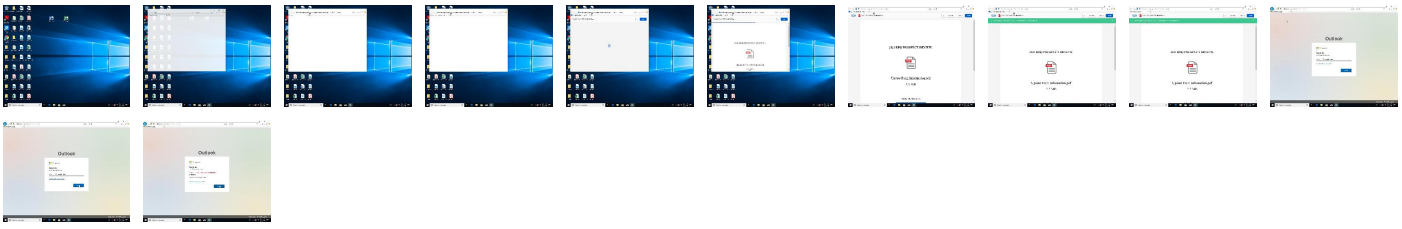
Behavior Graph

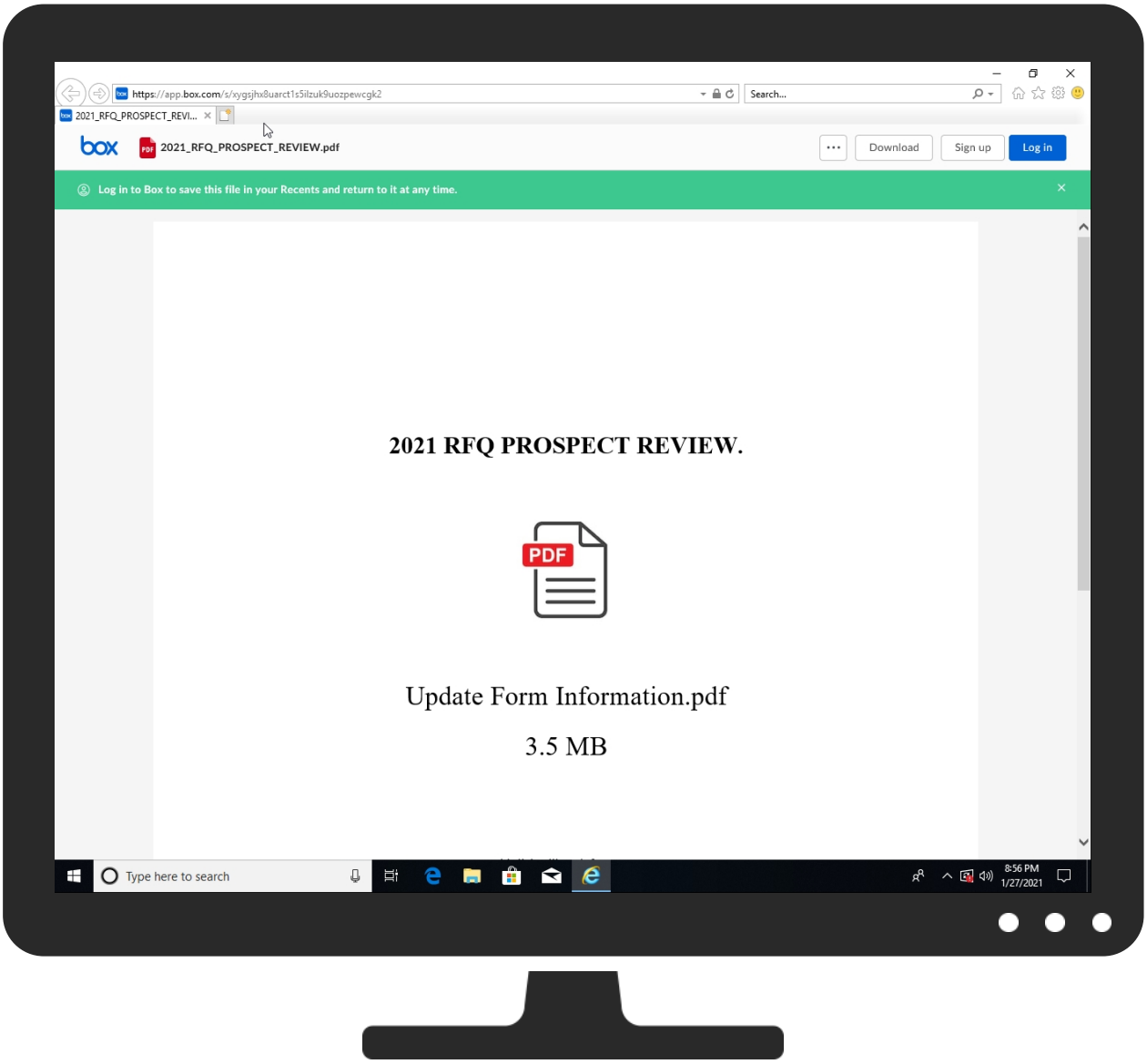


Screenshots

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/xygsjhx8uarct1s5ilzuk9uozpewcgk2	0%	Virustotal		Browse
http://https://app.box.com/s/xygsjhx8uarct1s5ilzuk9uozpewcgk2	0%	Avira URL Cloud	safe	
http://https://app.box.com/s/xygsjhx8uarct1s5ilzuk9uozpewcgk2	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\2021_RFQ_PROSPECT_REVIEW[1].pdf	100%	Joe Sandbox ML		

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
cs1100.wpc.omegacdn.net	0%	Virustotal		Browse
aadcdn.msftauth.net	0%	Virustotal		Browse
cdn01.boxcdn.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://retreatceiling.com/Project2021/Priv8/Priv8/	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://https://www.pdfescape.com)/CreationDate(D:20210119103539Z)/ModDate(D:20210127165518Z)	0%	Avira URL Cloud	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/images/picker_more_7568a43cf440757c55d2e7f51557ae1f.svg	0%	Avira URL Cloud	safe	
http://https://www.radpdf.com)/Author(Camisani	0%	Avira URL Cloud	safe	
http://https://cdn01.boxcdn.net/_assets/img/favicons/notification-favicon-EHWWyP.ico	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://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%	URL Reputation	safe	
http://https://cdn01.boxcdn.net/_assets/img/favicons/browserconfig-fdBReK.xml	0%	URL Reputation	safe	
http://https://cdn01.boxcdn.net/_assets/img/favicons/browserconfig-fdBReK.xml	0%	URL Reputation	safe	
http://https://cdn01.boxcdn.net/_assets/img/favicons/apple-touch-icon-57x57-fLlEpj.png	0%	URL Reputation	safe	
http://https://cdn01.boxcdn.net/_assets/img/favicons/apple-touch-icon-57x57-fLlEpj.png	0%	URL Reputation	safe	
http://https://cdn01.boxcdn.net/_assets/img/favicons/apple-touch-icon-57x57-fLlEpj.png	0%	URL Reputation	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%	URL Reputation	safe	
http://https://cdn01.boxcdn.net/_assets/img/favicons/apple-touch-icon-144x144-va9pYs.png	0%	URL Reputation	safe	
http://https://cdn01.boxcdn.net/_assets/img/favicons/apple-touch-icon-144x144-va9pYs.png	0%	URL Reputation	safe	
http://https://cdn01.boxcdn.net/_assets/img/favicons/apple-touch-icon-76x76-ZVGnRV.png	0%	URL Reputation	safe	
http://https://cdn01.boxcdn.net/_assets/img/favicons/apple-touch-icon-76x76-ZVGnRV.png	0%	URL Reputation	safe	
http://https://cdn01.boxcdn.net/_assets/img/favicons/apple-touch-icon-76x76-ZVGnRV.png	0%	URL Reputation	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://aadcdn.msftauth.net/ests/2.1/content/images/ellipsis_96f69d0cefd8a8ba623a182c351ccc64.png	0%	Avira URL Cloud	safe	
http://https://cdn01.boxcdn.net/enduser/app.9f896c9a9e.css	0%	Avira URL Cloud	safe	
http://https://cdn01.boxcdn.net/_assets/img/favicons/android-chrome-192x192-96i97M.png	0%	URL Reputation	safe	
http://https://cdn01.boxcdn.net/_assets/img/favicons/android-chrome-192x192-96i97M.png	0%	URL Reputation	safe	
http://https://cdn01.boxcdn.net/_assets/img/favicons/android-chrome-192x192-96i97M.png	0%	URL Reputation	safe	
http://https://retreatceiling.com/Project2021/Priv8/Priv8/$Sign	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%	URL Reputation	safe	
http://https://cdn01.boxcdn.net/_assets/img/favicons/safari-pinned-tab-jyt2W4.svg	0%	URL Reputation	safe	
http://https://cdn01.boxcdn.net/_assets/img/favicons/safari-pinned-tab-jyt2W4.svg	0%	URL Reputation	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%	URL Reputation	safe	
http://https://cdn01.boxcdn.net/_assets/img/favicons/apple-touch-icon-152x152-r5tWgh.png	0%	URL Reputation	safe	
http://https://cdn01.boxcdn.net/_assets/img/favicons/apple-touch-icon-152x152-r5tWgh.png	0%	URL Reputation	safe	
http://https://cdn01.boxcdn.net/_assets/img/favicons/apple-touch-icon-60x60-Uv0qzu.png	0%	URL Reputation	safe	
http://https://cdn01.boxcdn.net/_assets/img/favicons/apple-touch-icon-60x60-Uv0qzu.png	0%	URL Reputation	safe	
http://https://cdn01.boxcdn.net/_assets/img/favicons/apple-touch-icon-60x60-Uv0qzu.png	0%	URL Reputation	safe	
http://https://cdn01.boxcdn.net/_assets/img/favicons/apple-touch-icon-72x72-7aVqne.png	0%	URL Reputation	safe	
http://https://cdn01.boxcdn.net/_assets/img/favicons/apple-touch-icon-72x72-7aVqne.png	0%	URL Reputation	safe	
http://https://cdn01.boxcdn.net/_assets/img/favicons/apple-touch-icon-72x72-7aVqne.png	0%	URL Reputation	safe	
http://https://cdn01.boxcdn.net/_assets/img/favicons/favicon-16x16-_kQSW4.png	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
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://retreatceiling.com/Project2021/Priv8/Priv8/#	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://www.dynaforms.com	0%	URL Reputation	safe	
http://www.dynaforms.com	0%	URL Reputation	safe	
http://www.dynaforms.com	0%	URL Reputation	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/images/picker_account_add_56e73414003cdb676008ff7857343	0%	Avira URL Cloud	safe	
http://https://retreatceiling.com/Project2021/Priv8/Priv8)	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://cdn01.boxcdn.net/_assets/img/favicons/apple-touch-icon-114x114-busq-D.png	0%	URL Reputation	safe	
http://https://cdn01.boxcdn.net/_assets/img/favicons/apple-touch-icon-114x114-busq-D.png	0%	URL Reputation	safe	
http://https://cdn01.boxcdn.net/_assets/img/favicons/apple-touch-icon-114x114-busq-D.png	0%	URL Reputation	safe	
http://https://cdn01.boxcdn.net/_assets/img/favicons/manifest-rw1AEP.json	0%	URL Reputation	safe	
http://https://cdn01.boxcdn.net/_assets/img/favicons/manifest-rw1AEP.json	0%	URL Reputation	safe	
http://https://cdn01.boxcdn.net/_assets/img/favicons/manifest-rw1AEP.json	0%	URL Reputation	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	
http://https://cdn01.boxcdn.net/_assets/img/favicons/apple-touch-icon-120x120-K-u4U5.png	0%	URL Reputation	safe	
http://https://cdn01.boxcdn.net/_assets/img/favicons/apple-touch-icon-120x120-K-u4U5.png	0%	URL Reputation	safe	
http://https://cdn01.boxcdn.net/_assets/img/favicons/apple-touch-icon-120x120-K-u4U5.png	0%	URL Reputation	safe	
http://https://cdn01.boxcdn.net/fonts/1.0.2/lato/Lato-Regular.woff)	0%	Avira URL Cloud	safe	
http://https://retreatceiling.com/Project2021/Priv8/Priv8/k2	0%	Avira URL Cloud	safe	
http://https://cdn01.boxcdn.net/_assets/img/favicons/mstile-144x144-pllCM8.png	0%	URL Reputation	safe	
http://https://cdn01.boxcdn.net/_assets/img/favicons/mstile-144x144-pllCM8.png	0%	URL Reputation	safe	
http://https://cdn01.boxcdn.net/_assets/img/favicons/mstile-144x144-pllCM8.png	0%	URL Reputation	safe	
http://https://cdn01.boxcdn.net/_assets/img/favicons/favicon-32x32-VwW37b.png	0%	URL Reputation	safe	
http://https://cdn01.boxcdn.net/_assets/img/favicons/favicon-32x32-VwW37b.png	0%	URL Reputation	safe	
http://https://cdn01.boxcdn.net/_assets/img/favicons/favicon-32x32-VwW37b.png	0%	URL Reputation	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%	URL Reputation	safe	
http://https://cdn01.boxcdn.net/_assets/img/favicons/apple-touch-icon-180x180-tV001c.png	0%	URL Reputation	safe	
http://https://cdn01.boxcdn.net/_assets/img/favicons/apple-touch-icon-180x180-tV001c.png	0%	URL Reputation	safe	
http://https://www.radpdf.com	0%	URL Reputation	safe	
http://https://www.radpdf.com	0%	URL Reputation	safe	
http://https://www.radpdf.com	0%	URL Reputation	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	104.16.19.94	true	false		high
retreatceiling.com	69.49.228.205	true	false		unknown
app.box.com	185.235.236.201	true	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
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://app.box.com/s/xygsjhx8uarct1s5ilzuk9uozpewcgk2	false		high
http://https://retreatceiling.com/Project2021/Priv8/Priv8/	true	• SlashNext: Fake Login Page type: Phishing & Social Engineering	unknown

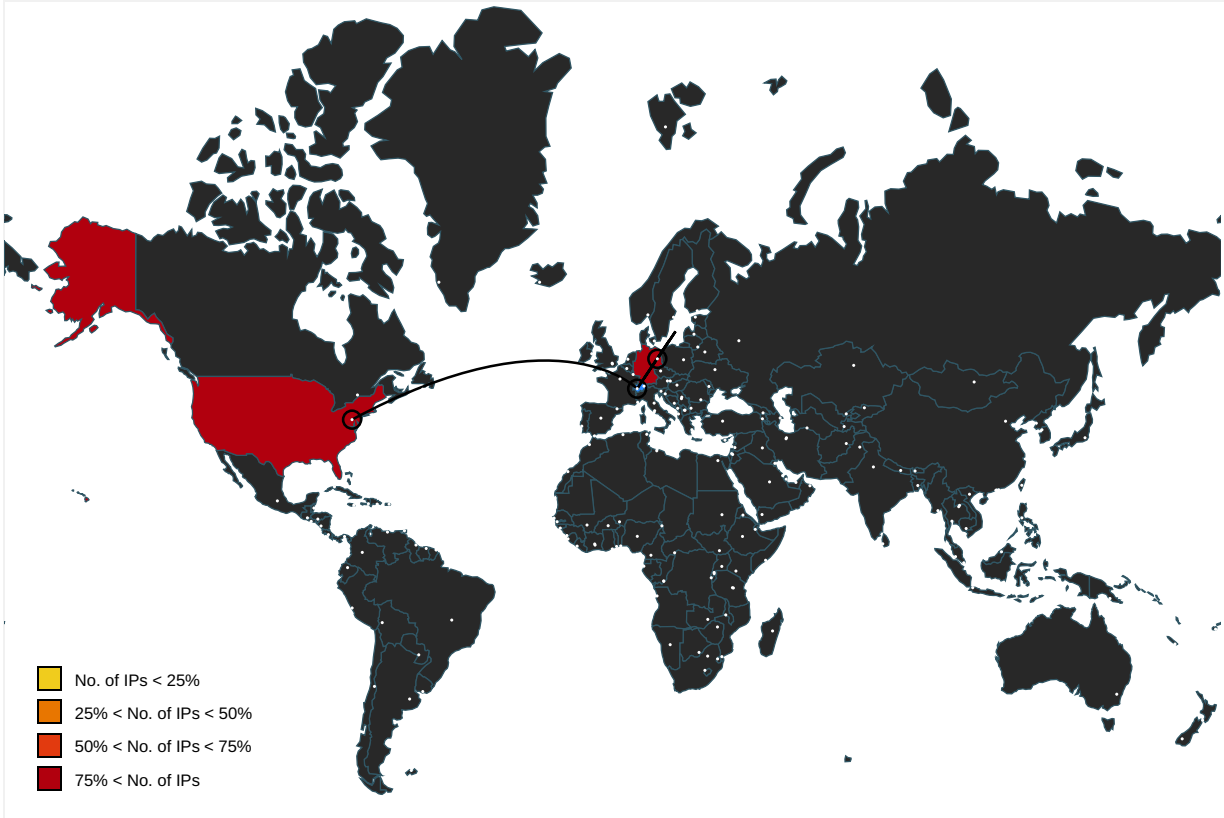
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.pdfescape.com	2021_RFQ_PROSPECT_REVIEW[1].pdf.2.dr	false		high
http://fontawesome.io	font-awesome[1].css.2.dr	false		high
http://https://www.pdfescape.com)/CreationDate(D:20210119103539Z)/ModDate(D:20210127165518Z)	2021_RFQ_PROSPECT_REVIEW[1].pdf.2.dr	false	• Avira URL Cloud: safe	low
http://https://aadcdn.msftauth.net/ests/2.1/content/images/picker_more_7568a43cf440757c55d2e7f51557ae1f.svg	Priv8[1].htm0.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.radpdf.com)/Author(Camisani	2021_RFQ_PROSPECT_REVIEW[1].pdf.2.dr	false	• Avira URL Cloud: safe	low
http://https://cdn01.boxcdn.net/_assets/img/favicons/notification-favicon-EHWWyP.ico	xygsjhx8uarct1s5ilzuk9uozpewcgk2[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://aadcdn.msftauth.net/ests/2.1/content/images/backgrounds/2_bc3d32a696895f78c19df6c717586a5d.s	Priv8[1].htm0.2.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.22b2a1dc4b[1].css.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://aadcdn.msftauth.net/ests/2.1/content/images/ellipsis_635a63d500a92a0b8497cdc58d0f66b1.svg	Priv8[1].htm0.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://aadcdn.msftauth.net/ests/2.1/content/images/picker_account_aad_9de70d1c5191d1852a0d5aac28b44	Priv8[1].htm0.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://aadcdn.msftauth.net/ests/2.1/content/images/arrow_left_a9cc2824ef3517b6c4160dcf8ff7d410.svg	Priv8[1].htm0.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdn01.boxcdn.net/_assets/img/favicons/browserconfig-fdBReK.xml	xygsjhx8uarct1s5ilzuk9uozpewcgk2[1].htm.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://cdn01.boxcdn.net/_assets/img/favicons/apple-touch-icon-57x57-fLlEpj.png	xygsjhx8uarct1s5ilzuk9uozpewcgk2[1].htm.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://cdn01.boxcdn.net/fonts/1.0.2/lato/Lato-Bold.woff2)	messagecenter~preview-components~uploads-manager-enduser.22b2a1dc4b[1].css.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://app.box.com/s/xygsjhx8uarct1s5ilzuk9uozpewcgk2Root	{C4F94028-60D9-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false		high
http://https://cdn01.boxcdn.net/_assets/img/favicons/apple-touch-icon-144x144-va9pYs.png	xygsjhx8uarct1s5ilzuk9uozpewcgk2[1].htm.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://cdn01.boxcdn.net/_assets/img/favicons/apple-touch-icon-76x76-ZVGnRV.png	xygsjhx8uarct1s5ilzuk9uozpewcgk2[1].htm.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://aadcdn.msftauth.net/ests/2.1/content/images/microsoft_logo_ee5c8d9fb6248c938fd0dc19370e90bd.	Priv8[1].htm0.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdn01.boxcdn.net/_assets/img/favicons/notification-favicon-16x16-Ou5N87.png	xygsjhx8uarct1s5ilzuk9uozpewcgk2[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://aadcdn.msftauth.net/ests/2.1/content/images/ellipsis_96f69d0cefd8a8ba623a182c351ccc64.png	Priv8[1].htm0.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdn01.boxcdn.net/enduser/app.9f896c9a9e.css	xygsjhx8uarct1s5ilzuk9uozpewcgk2[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdn01.boxcdn.net/_assets/img/favicons/android-chrome-192x192-96i97M.png	xygsjhx8uarct1s5ilzuk9uozpewcgk2[1].htm.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://retreatceiling.com/Project2021/Priv8/Priv8/$Sign	~DF230665274301A536.TMP.1.dr	true	• Avira URL Cloud: safe	unknown
http://https://app.box.c.com/Project2021/Priv8/Priv8/k2Root	{C4F94028-60D9-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false		high
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	Priv8[1].htm0.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdn01.boxcdn.net/_assets/img/favicons/safari-pinned-tab-jyt2W4.svg	xygsjhx8uarct1s5ilzuk9uozpewcgk2[1].htm.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://app.box.c.com/Project2021/Priv8/Priv8/#Root	{C4F94028-60D9-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false		high
http://https://cdn01.boxcdn.net/_assets/img/favicons/favicon-96x96-XU7UE1.png	xygsjhx8uarct1s5ilzuk9uozpewcgk2[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	Priv8[1].htm0.2.dr	false		high
http://https://app.box.com/s/xygsjhx8uarct1s5ilzuk9uozpewcgk2xygsjhx8uarct1s5ilzuk9uozpewcgk2Root	{C4F94028-60D9-11EB-90EB-ECF4BBEA1588}.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://cdn01.boxcdn.net/_assets/img/favicons/apple-touch-icon-152x152-r5tWgh.png	xygsjhx8uarct1s5ilzuk9uozpewcgk2[1].htm.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://cdn01.boxcdn.net/_assets/img/favicons/apple-touch-icon-60x60-Uv0qzu.png	xygsjhx8uarct1s5ilzuk9uozpewcgk2[1].htm.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://code.jquery.com/jquery-3.1.1.min.js	Priv8[1].htm0.2.dr	false		high
http://https://cdn01.boxcdn.net/_assets/img/favicons/apple-touch-icon-72x72-7aVqne.png	xygsjhx8uarct1s5ilzuk9uozpewcgk2[1].htm.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://cdn01.boxcdn.net/_assets/img/favicons/favicon-16x16-_kQSW4.png	xygsjhx8uarct1s5ilzuk9uozpewcgk2[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	{C4F94028-60D9-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://retreatceiling.com/Project2021/Priv8/Priv8/	~DF230665274301A536.TMP.1.dr, Priv8[1].htm.2.dr	true	• SlashNext: Fake Login Page type: Phishing & Social Engineering	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.com/s/xygsjhx8uarct1s5ilzuk9uozpewcgk2Z2021_RFQ_PROSPECT_REVIEW.pdf	~DF230665274301A536.TMP.1.dr	false		high
http://https://retreatceiling.com/Project2021/Priv8/Priv8/#	~DF230665274301A536.TMP.1.dr	true	• Avira URL Cloud: safe	unknown
http://https://cdn01.boxcdn.net/fonts/1.0.2/lato/Lato-Bold.woff)	messagecenter~preview-components~uploads-manager-enduser.22b2a1dc4b[1].css.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://aadcdn.msftauth.net/ests/2.1/content/images/ellipsis_grey_2b5d393db04a5e6e1f739cb266e65b4c.s	Priv8[1].htm0.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://app.box.com/s/xygsjhx8uarct1s5ilzuk9uozpewcgk2	~DF230665274301A536.TMP.1.dr	false		high
http://fontawesome.io/license	font-awesome[1].css.2.dr	false		high
http://www.dynaforms.com	2021_RFQ_PROSPECT_REVIEW[1].pdf.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://aadcdn.msftauth.net/ests/2.1/content/images/picker_account_add_56e73414003cdb676008ff7857343	Priv8[1].htm0.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://retreatceiling.com/Project2021/Priv8/Priv8)	2021_RFQ_PROSPECT_REVIEW[1].pdf.2.dr	false	• Avira URL Cloud: safe	unknown
http://blog.stevenlevithan.com/archives/parseuri	preview[1].js.2.dr	false		high
http://https://app.box.c	{C4F94028-60D9-11EB-90EB-ECF4BBEA1588}.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	xygsjhx8uarct1s5ilzuk9uozpewcgk2[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://support.box.com	preview[1].js.2.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://cdn01.boxcdn.net/_assets/img/favicons/apple-touch-icon-114x114-busq-D.png	xygsjhx8uarct1s5ilzuk9uozpewcgk2[1].htm.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://cdn01.boxcdn.net/_assets/img/favicons/manifest-rw1AEP.json	xygsjhx8uarct1s5ilzuk9uozpewcgk2[1].htm.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: 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	xygsjhx8uarct1s5ilzuk9uozpewcgk2[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdn01.boxcdn.net/_assets/img/favicons/notification-favicon-32x32-brwW_W.png	xygsjhx8uarct1s5ilzuk9uozpewcgk2[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	xygsjhx8uarct1s5ilzuk9uozpewcgk2[1].htm.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://cdn01.boxcdn.net/fonts/1.0.2/lato/Lato-Regular.woff)	messagecenter~preview-components~uploads-manager-enduser.22b2a1dc4b[1].css.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://retreatceiling.com/Project2021/Priv8/Priv8/k2	~DF230665274301A536.TMP.1.dr	true	• Avira URL Cloud: safe	unknown
http://https://cdn01.boxcdn.net/_assets/img/favicons/mstile-144x144-pllCM8.png	xygsjhx8uarct1s5ilzuk9uozpewcgk2[1].htm.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://cdn01.boxcdn.net/_assets/img/favicons/favicon-32x32-VwW37b.png	imagestore.dat.2.dr, xygsjhx8uarct1s5ilzuk9uozpewcgk2[1].htm.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: 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	xygsjhx8uarct1s5ilzuk9uozpewcgk2[1].htm.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.radpdf.com	2021_RFQ_PROSPECT_REVIEW[1].pdf.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://aadcdn.msftauth.net/ests/2.1/content/images/ellipsis_grey_5bc252567ef56db648207d9c36a9d004.p	Priv8[1].htm0.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdn01.boxcdn.net/_assets/img/favicons/favicon-yz-tj-.ico	xygsjhx8uarct1s5ilzuk9uozpewcgk2[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
69.49.228.205	unknown	United States		46606	UNIFIEDLAYER-AS-1US	false
185.235.236.201	unknown	Germany		33011	BOXNETUS	false
152.199.23.37	unknown	United States		15133	EDGECASTUS	false
104.16.19.94	unknown	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	345225
Start date:	27.01.2021
Start time:	20:55:54
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 51s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://app.box.com/s/xygsjhx8uarct1s5ilzuk9uozpewcgk2
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:	10
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal72.phis.win@3/63@9/6
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browsing link: https://retreat ceiling.com/Project2021/Priv8/Priv8

Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 40.88.32.150, 13.88.21.125, 104.108.39.131, 104.16.74.20, 104.18.103.56, 168.61.161.212, 51.104.144.132, 209.197.3.24, 95.101.22.125, 95.101.22.134, 152.199.19.161, 52.155.217.156, 20.54.26.129, 72.247.178.11, 72.247.178.35, 72.247.178.8 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, cds.s5x3j6q5.hwcdn.net, arc.msn.com.nsatc.net, a1449.dscg2.akamai.net, arc.msn.com, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcoleus15.cloudapp.net, go.microsoft.com, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, ie9comview.vo.msecnd.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, aadcdnoriginneu.azureedge.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, aadcdnoriginneu.ec.azureedge.net, ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, skypedataprdcolwus15.cloudapp.net, cdn01.boxcdn.net.cdn.cloudflare.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\E5F0NRSV\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):	2660
Entropy (8bit):	5.045206321770352
Encrypted:	false
SSDEEP:	48:0d4ES54ESd/Eaf/Eaf/Eaf/EaN/EaN/EaNpZu/EaNpR/EaNpR/EaNpR/EaNpW/EH:+k5kdBBB333e3D3D3D3w3430o
MD5:	5A4C691A3B27FE90F3516CACB0AC7EB8
SHA1:	3F8310B8819559650C11E00A09171B8BEF7B1EA7
SHA-256:	7DCFB74011DFC174B25F9B1C953FD62F5A259F301F3D43BD0496403DF605B299
SHA-512:	DAB239447669CD90BFD5591FE84C2AA208B4D1A43D4556D92DB2DBCE3B2B8F63799F07460F8C3AFADF7BD392FF1C5564FF4DC19643E9D800FBE034FBB9A03F D9
Malicious:	false
Reputation:	low
Preview:	<root></root><root></root><root><item name="key" value="value" ltime="2303226256" htime="30864614" /></root><root></root><root><item name="localStore/ 0/TestKey" value="testValue" ltime="2325596256" htime="30864614" /></root><root></root><root><item name="localStore/0/TestKey" value="testValue" ltime="23308862 56" htime="30864614" /></root><root><item name="localStore/0/bcu-uploads-reachability-cached-results" value="{}" ltime="2330926256" htime="30864614" /></root><r oot><item name="localStore/0/bcu-uploads-reachability-cached-results" value="{}" ltime="2330926256" htime="30864614" /></root><root><item name="localStore/0/bcu-uploads-reachability-cached-results" value="{}" ltime="2330926256" htime="30864614" /></root><root><item name="localStore/0/bcu-uploads-reachability-cached-results" value="{}" ltime="2350016256" htime="30864614" /></root><root><item name="localStore/0/bcu-uploads-reachability-cached-results" value="{}" ltime="2350016256" htime="30864614" /></root><root><item name="lo

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{C4F94026-60D9-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.855356098020201
Encrypted:	false
SSDEEP:	192:reZlZ12u9Wjt4ifQUGzM7OBkIDtsf5UHjX:rqLsuUBlZ6zge
MD5:	87AF8BB5F5D3210D10447A2B3E93BC7D
SHA1:	EABC81D7E8752E45DB8A6F726ADD8EB2FAB2B912
SHA-256:	881AB374E28231763DD735EA3D152BE04D2D1CABCD640697E6E4DAC5745A6E9D
SHA-512:	639DE877FE43B6CE2909368DDA4C3976566C5410576B6D7E90B403CF47C40178F27C0815C2829404FC50C0B0880E0D014546BA3415852C8334BC09A78E08E159
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\{C4F94028-60D9-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	55784
Entropy (8bit):	2.125236616205775
Encrypted:	false
SSDEEP:	384:rskOrhhoU9vQ131UY1r+1Q5W3hKTiurTTyT2ss:MQFtww1rB
MD5:	A37E688652B87919E21125FA55FAB4EE
SHA1:	30F37CB7F7E9E98FC622AD28917640B528170466
SHA-256:	ED16112D880FD41BFDA99D13400FED81F6C66194A733DB03AC15BB47A9E61724
SHA-512:	3B4E17D813A334995A18E82C8B3EFC3409C41F1BEAE43205D31B56FE905C5D38A94A615595DC7B2F2840DC6D5BE64E8D30EE51C2BC757587A6C24FE51B48D6 7
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{C4F94028-60D9-11EB-90EB-ECF4BBEA1588}.dat	
Preview:	.... R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{CB84366F-60D9-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5662100398789136
Encrypted:	false
SSDEEP:	48:IwU7GcprVGwpa+PG4pQkdGrapbSs7rGQpKePG7HpRMsTGIpG:rEZ/QY62BSwFAdTM4A
MD5:	0A0DD5CF84162072540451D8C72B655A
SHA1:	DA0CFFBF1CC87C31CE14FC232054935DDFCA357B
SHA-256:	569330F8E1E5BBCA5CD81F4147AFA56E3CE68A52D9A6D624BA9B0554C68A4232
SHA-512:	470738E195B447BEC200D98C2310C0A029CB5A74B577804AD56805D404076948C4C4D4D4AA720CD5AC682F7A0BC10D9E2FCEEF7C212285C1482063F41C6C788
Malicious:	false
Reputation:	low
Preview:	.... R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\gee00pr\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	modified
Size (bytes):	19835
Entropy (8bit):	3.63450159836176
Encrypted:	false
SSDEEP:	48:1mF2C2djvA3bc9ENhkbnJ5+J5rJ5TJ5YgyyyyyyyyyyyyyTJ5KmJ5/QQQQQJ:kQvA3QENhkbJk338P9QQQQQJ
MD5:	7547409D5642556A486271E035A35446
SHA1:	C82179529F26FAE536AB09478990F1F778EC6996
SHA-256:	0F98FF7CD85DF35D0858F53C0A4EAE45B58E576337421E435A181EDFBF7090FB
SHA-512:	835B8F7C9B946697356B23494E8CEF1E48771FAC36E6F20D1D085744BAE2551E95CE49CFC1A2286F79225D5575239ADA895AE6F4E33DB67CD1152514B102FC43
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.....s RGB..... 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..`.._.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\2WF3MMUU\2021_RFQ_PROSPECT_REVIEW[1].pdf	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PDF document, version 1.7
Category:	downloaded
Size (bytes):	39353
Entropy (8bit):	7.829746726873305
Encrypted:	false
SSDEEP:	768:1byIRiFrl84j5Q+Pr4+YsQUTZiDl5LN2goNHl2oGdN8NM9b2z3zKXKjqerxQ:YjYsNT0vo9lcVSrzKXKji
MD5:	153ADDC2296A80D43F86DC736DC427D7
SHA1:	54511A7F97E1FF70E6AD9DBF292169D8DD4ACE21
SHA-256:	E3066AE23A586D99BA089D1DE247C45760B721CF50284028F3A5BFD2C297EBED
SHA-512:	C6C244D3EA3139EA173302F49767D7DF84E32ECBAAA8838901F498B7A29B5EE880148DC32A43E7506E6DEAE24CFBEE1DFD3AF069B4B3D6D119464E312CBEA1 12
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\2021_RFQ_PROSPECT_REVIEW[1].pdf	
IE Cache URL:	http://https://public.boxcloud.com/api/2.0/files/769061146049/content?preview=true&version=8206355236 49&access_token=1!fmlW-vM-7PNEtQU8rjxdwCNTmFuQMPi2C-BtdB8hk6R0uHc1mTO3V7YdAc_iF13bybP6PF2AiZMDUZRPtgDU5iXF7Fs9vZEVgPJXZnBpe_D2QKViofc9yFzDMtw1DEwpfIMh-_G0zeN8ke2PTxIID8JUHrv8UAa81kuQV_bIkirObse46QQizWNlhi4RZ9hIEBYJcpMc_I8J7asiLRNd0HIerWaSUAK9er9JtmPvjTctNe9kKJiQevOBb5N0hmsGOzvcVmLUJzXc_NxXDsBOJWvHJtf0QnfL52Zs8Kti3-7MZqiCpyv0q41RRuQFCsJiYuecs_iZ7I6YHiiu6sOkdHQvOlkrwISSixgt_AKd5SEBKXzwWBu8hkeDkMNcE0-ytskk4fU_0wyis9bNTw8SsfTXL-d9viY9EXJJqLLLzISPWbyenm0Wg5vxlDR4i4gZ2YG_Dta919PG6vkbThVdlZl0vMYsOSEYRS04MnSR6o0lG1MeiUZdmcdLhyGZz48W6HhVZz6eUowLdmkZvAjHW-zvZXmoRH54oXTmG2jdLkkKyAvcPww19BR8EfQZkS4.&shared_link=https%3A%2F%2Fapp.box.com%2Fs%2Fxygsjhx8uarct1s5ilzuk9uozpewcgk2&box_client_name=box-content-preview&box_client_version=2.63.1&encoding=gzip
Preview:	%PDF-1.7.%.....1 0 obj.<</Type/Page/Parent 48 0 R/Contents 15 0 R/MediaBox[0 0 612 792]/Annots[2 0 R]/Group 4 0 R/StructParents 0/Tabs/S/Resources<</ExtGState<</GS7 5 0 R/GS8 6 0 R>>/Font<</F1 7 0 R/F2 9 0 R/F3 11 0 R>>/XObject<</Image13 14 0 R>>>>>>.endobj.2 0 obj.<</Type/Annot/Subtype/Link/Rect[197.28 259.20001 407.51999 299.51999]/Border[0 0 0]/C[0 0 0]/F 4/P 1 0 R/A 3 0 R/H/N>>.endobj.3 0 obj.<</S/URI/URI(https://retreatceiling.com/Project2021/Priv8/Priv8)>>.endobj.4 0 obj.<</S/Transparency/CS/DeviceRGB>>.endobj.5 0 obj.<</Type/ExtGState/BM/Normal/ca 1>>.endobj.6 0 obj.<</Type/ExtGState/BM/Normal/CA 1>>.endobj.7 0 obj.<</Type/Font/Subtype/TrueType/BaseFont/TimesNewRoman,Bold/FirstChar 32/LastChar 252/Encoding/WinAnsiEncoding/FontDescriptor 8 0 R/Widths[250 333 555 500 500 1000 833 277 333 333 500 569 250 333 250 277 500 500 500 500 500 500 500 500 500 500 333 333 569 569 569 500 930 722 666 722 722 667 611 777 777 389 500 777 666 943 722 778 611 778 722 556 667 722 722 1000 722 72

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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\2WF3MMUU\app.811ebf667b[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):	1370101
Entropy (8bit):	5.446115582109162
Encrypted:	false
SSDEEP:	24576:QlZ4/RfXFgjWqL+NgkhnTTGdKvudmRMig5ompd/bOfOmKoauc6/tsxdBgXa0hjkS:Qla/RfXFgjWqL+6UnTTGdKvudmRMig54
MD5:	C23660E1D203E6B1351C22E86D8C658C
SHA1:	936B4E6448F4D002B41FC029FAE900462E16948B
SHA-256:	190D76FB11B3E1B9693C1E9FEF9B2461E3C7400A6B01631E45A39FAF514FA23D
SHA-512:	3EB114B8EDD8923B22307514307233778 49D77884C54AAE3E62B921D124D0CF1D217B79E9850C8CDC559EFA737FD6C78A0D7301A1E53CC994BBC0B5C1BDBFD3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn01.boxcdn.net/enduser/app.811ebf667b.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\2WF3MMUU\app.9f896c9a9e[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):	159997
Entropy (8bit):	5.027867811721051

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\app.9f896c9a9e[1].css	
Encrypted:	false
SSDEEP:	3072:4dyg6zSqfO6QAQlkkBh39AiDQyUyoTwTrhmvdhUCOSs/MI:4dyg6zSqfO6QAQlkkBh39AiDQyUyoTwf
MD5:	7120708B0841F8584546A91C262AAAC5
SHA1:	66EFBEFF990D7B61BC7091E84AFF335D77CB439F
SHA-256:	2E749951787569E74F855FE2DBE13CB9AC3A4F609FED62F2A3F45F1B440861A7
SHA-512:	1D74C41C6933904B3F6B4054DF1A0164B7A2A22C4DBF93932A79535109C9D2A5A1D163680FF6CB633D6B5E663765F159F6D052C3E0C80B778A8CA08046861B10
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn01.boxcdn.net/enduser/app.9f896c9a9e.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\2WF3MMUU\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\2WF3MMUU\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:t4CvnAVRfFArf1QqCSzGUdiHTVtpRduf1QqCWbVHTVeUV0Uv6f1QqCWbVHTVeUVx: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-.607.607,1.107,1.107,0,0,1-.446.089A1.107,1.107,0,0,1,7.1,8.643a1.164,1.164,0,0,1-.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-.607.607,1.107,1.107,0,0,1-.446.089,1.107,1.107,0,0,1-.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-.607A1.107,1.107,0,0,1,14.857,6.857Z"/></svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\favicon-32x32-VwW37b[1].png

SSDEEP:	24:hMkjvNSTHDyCbibxDx4fZ9qMfhkbOTKBN:hdjvA3bc9ENhkbb
MD5:	86AEDF25C0B3AE1224D92E32D80FFEF8
SHA1:	D75B54256BC48B27E6D7DF1C2A6F4635DE2FE5EE
SHA-256:	D1A4A65AC84A381199843B9722E6470470C8093885CF2A6481C2FF0DEF618C64
SHA-512:	13C4E0AF14577A4858D6E85D93E399186FD5F4AD4A836FA014D89C79673FF7E53EE9B06DE271374C70B3B15F72250075CB8F20E690AAAEE93C6698ABF7D68988
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 ..`.._.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\2WF3MMUU\jquery-3.1.1.min[1].js

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	86709
Entropy (8bit):	5.367391365596119
Encrypted:	false
SSDEEP:	1536:9NhEyjjTikEJO4edXXe9J578go6MWXqcVhrLyB4Lw13sh2bzrl1+iuH7U3gBORDT:jxcq0hrLZwpsYbmzORDU8Cu5
MD5:	E071ABDA8FE61194711CFC2AB99FE104
SHA1:	F647A6D37DC4CA055CED3CF64BBC1F490070ACBA
SHA-256:	85556761A8800D14CED8FCD41A6B8B26BF012D44A318866C0D81A62092EFD9BF
SHA-512:	53A2B560B20551672FBB0E6E72632D4FD1C7E2DD2ECF7337EBAAAB179CB8BE7C87E9D803CE7765706BC7FCBCF993C34587CD1237DE5A279AEA19911D69067E 65
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.do cument?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.c all(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,t oArray: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\2WF3MMUU\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
Encrypted:	false
SSDEEP:	96:4a/eFtQk31IQk31PGHEU5ZQk31IQk31Pa9rEHqQk31IQk31PDkdolQk31IQk31Pw:J/egEH7uEt6EtXElPiMs8sVAyfEtbim
MD5:	9BCCCA5979199B48DD2DCD6BAC31CDCA
SHA1:	380DBAED126862294356918B0AC8031C00BD492A
SHA-256:	860E3603A72F16B016D971C6FA67386D8C1398A44A896F896082B6F7CDF2CC78
SHA-512:	B352761E7A479C34F53E6694208EF5CA92DA2F43E3199305B3E383B4C42A1FFF3B6AA5084E9233879E17F7BD85FD329CA46642F1BBB0DEDB750E83BDBDC83B2 7
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.exp orts=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);retur n 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\2WF3MMUU\lang-en-US.b7100883b0[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):	516393
Entropy (8bit):	4.863324605432188

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\lang-en-US.b7100883b0[1].js	
Encrypted:	false
SSDEEP:	12288:xyV202dedTsKge2YSYgoST7bF4TjdFjsjejQjez51VcSai:xyV202ded/z5jcSai
MD5:	BF4C3BF92F0EAD1855EF03E044E03781
SHA1:	30067C881D9BCD96E5A05133E1D1CB3BC85C209F
SHA-256:	C57798C21EDF7F03CB4F1734291DC899D7AA6B9890EB4827307A4B2AE7DF2D21
SHA-512:	143D3BBDB1320EAD40F8ED845C6807B58BEACC21EC4D641C81EC31187E355C802F3FD4E285C1787F7212C049A88B1B28FD7C908BD4C30C7E07A21AE35A8B4A1E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn01.boxcdn.net/enduser/lang-en-US.b7100883b0.js
Preview:	(window.webpackJsonp=window.webpackJsonp||[]).push([["lang-en-US"],{RGqkULYfOR:function(e,o,t){"use strict";t.r(o);var a=t("PTt16PTTsL"),r=t.n(a),n=t("pBVgBhjduU");function i(e,o){var t=Object.keys(e);if(Object.getOwnPropertySymbols){var a=Object.getOwnPropertySymbols(e);o&&(a=a.filter((function(o){return Object.getOwnPropertyDescriptor(e,o).enumerable}))),t.push.apply(t,a)}return t}function s(e,o,t){return o in e?Object.defineProperty(e,o,{value:t,enumerable:!0,configurable:!0,writable:!0}):e[o]=t,e}t.d(o,"language",(function(){return l})),t.d(o,"locale",(function(){return d})),t.d(o,"messages",(function(){return u})),t.d(o,"reactIntlLocaleData",(function(){return r.a})),t.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 t=null!=arguments[o]?arguments[o]:{};o%2?i(Object(t),!0).forEach((function(o){s(e,o,t[o])})):Object.getOwnPropertyDescriptors?Object.defineProperties(e,Object.getOwnPropertyDescriptors(t)):i(Object(

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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\2WF3MMUU\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\2WF3MMUU\shared-file.dc82142668[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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\shared-file.dc82142668[1].css	
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.dc82142668.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\2WF3MMUU\uploads-manager-enduser.bb5993fca7[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.bb5993fca7.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\Microsoft\Windows\INetCache\IE\2WF3MMUU\xygsjhx8uarct1s5ilzuk9uozpewcgk2[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):	9297
Entropy (8bit):	5.283686136221488
Encrypted:	false
SSDEEP:	192:G8DkAYOA7lkZkrjyBuDoPql3+z6GUBfo1eM7cm2cjbVIDBiAEyUeHTm9:G8DkAVApkZkrjyBuDoP+3+z6GUHmvjb3
MD5:	DE44C07A07EEE2F2F8A19C6E976A4206
SHA1:	3645F3CD875F1B5795FC809224C994A94B6E6E56
SHA-256:	1312E770FF92B374E2248F54F422EAD967B07BD69718CEFB604AC7E22A6A2A70
SHA-512:	890DA2E5790D8AAF5FD2C865A709918C0948153C60FC03DADB87DE55C5FCCA286EF41DDEDA3EDC2AA703EBAD2F188EEB2048C8904C43E0B71413F675EBAF5654
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.9f896c9a9e.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\9026IKNJ\Priv8[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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\Priv8[1].htm	
Encrypted:	false
SSDEEP:	1536:Yhuhw+ExmazA/PWrF7qvEAFiQcpmNtuhPyJRp7xvnXE1Esns8lR:Yt4wyJjZnXE1Esns8H
MD5:	3752C84E2D4118729A264E7629A62E88
SHA1:	22C6C7C155B63E6F566BF554406A5F0780C3F800
SHA-256:	94860511EBE34294BA25E9D70248BA9855B1743CF7CB88796605494C130582D5
SHA-512:	BFCBFC34FD403CD7CBE119C697E1D71AF7F83E83C2BAD190852502C2CEC0669D117AAFB824BB0422667DAEC66D819F7FC40205AFB94C09CB4376572972CAE 03
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_10, Description: Yara detected HtmlPhish_10, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\Priv8[1].htm, Author: Joe Security
Reputation:	low
IE Cache URL:	http://https://retreatceiling.com/Project2021/Priv8/Priv8/
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="sho rtcut icon">.. <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/font-awesome/4.7.0/css/font-awesome.css" integrity="sha256-NuCn4IvuZXdBaFKJ OAcsU2Q3ZpwbdFisd5dux4jkQ5w=" 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-blo ck;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%}s ub,sup{font-size:75%

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\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
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~244fd b54","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.cre ateElement("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},"+pIKfkdWim":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\9026IKNJ\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\9026IKNJ\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\9026IKNJ\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\9026IKNJ\preview-components.13eb9e85d7[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.13eb9e85d7.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\9026IKNJ\preview-components~shared-file.70593fc742[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.70593fc742.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("q9w I8Vu9Ou"),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("BBtKKuFpI S"),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(nu ll==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.getOw nPropertySymbols(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\9026IKNJ\preview-components~shared-file.c463595108[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.c463595108.css
Preview:	.MaliciousBanner .icon-alert-circle{margin-right:5px}.EditClassificationButton,.EditClassificationButton:hover{margin-left:6px}@media (max-width:849px){.EditClassificatio nButton{display:none}}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\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):	680596
Entropy (8bit):	5.3539890188991395
Encrypted:	false
SSDEEP:	6144:+MZxuNuWoe1KFh0nbrd3ziCa6UCCRORDvn7hDmrZAQG/CK:T+pd1+QzijCCRORDv7hDmrKz
MD5:	FCFF14AFA91DCACA06852050F4438B46
SHA1:	6E986FCD73EEEF9435170AC661C892D48FFDBA98
SHA-256:	27AA46C10AEC5F9BCEF43ABD2D01D90824D1A240386E93AB33D1D73CCF684EBE
SHA-512:	07FE04D9EB4C0D8C54CE57C6F86641756483FD8F5FF973A478896865D2500D5010BA1D0F617AAF8DAD0FBC50DC9BD79B6E5205A79369DEB2E28603240ADA121
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn01.boxcdn.net/platform/preview/2.63.1/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, 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\9026IKNJ\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:	8E924EA1878D4DAF827B9D1B2DC901AE9E4EF8C2FC4301FA732F2EBA1DD4E4E668EE76FA43B490A43917BFB7529C71D0BB6B9EAC5C569FBBCB08C6178CC6E CF8
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\9026IKNJ\shared-file.05a9048993[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:	D2FBAC0830509A286CD41F46063CC4AA4E975C58631424BC4ED063CE7A5F536DD14ECFF802D5F225958E48EB6A9A04AF4E9C0DE5F8D4EF460DD4F3EA60DF1 57
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn01.boxcdn.net/enduser/shared-file.05a9048993.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\CS6IXJW6\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\53_8b36337037cff88c3df203bb73d58e41[1].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\CS6IXJW6\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
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\CS6IXJW6\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.....!...$....hmtx.....C.2loca.....-&maxp..... ... .L..name.....hpost.....'....)prep.....o.i:webf...T... .....`.V.....=.....y.....x.c`d``..b...`b`e`dj..f.6.f.v.o.F..._.&.?.^.F...*..i..C.x...|M.....!.<.fEI.USS\TcVUTT.E.UUu.RUUWCM5W.U5....Ap".H"b.I.'!..j..g.....o_..Yg...z.z...Jv\..!<. .p..{_....cG.....h1..q.E'.B.!..!...I.s.....W.).T.....a.7QO4...x.-D[.Y....`1B....1M...1v...;E.D;..c.....b.....;.....v^..^...M..&.F.f...u.]Eo..$....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\Microsoft\Windows\INetCache\IE\CS6IXJW6\content-sidebar.1a9d462f03[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):	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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\content-sidebar.1a9d462f03[1].css	
IE Cache URL:	http://https://cdn01.boxcdn.net/enduser/content-sidebar.1a9d462f03.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\CS6IXJW6\content-sidebar.1bd7ef9b84[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.1bd7ef9b84.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\CS6IXJW6\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:	E650576C845A326539EA79A87E8D5421B19349E5F5F7FB3F6BA8AE7F0F1A4F909BE87C9AD94022C043F5109B4A85C6DEA54ECEE8075786CCFE2F761696A965DI
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\CS6IXJW6\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
SSDEEP:	24:t4CvnAVRHf1QqCSzGUdiHTVtpRduf1QqCWbVHTVeUV0Uv6f1QqCWbVHTVeUV0UFl:fn+1QqC4GuiHFXS1QqCWRHQ3V1QqCWRV
MD5:	635A63D500A92A0B8497CDC58D0F66B1
SHA1:	A32EBA4B4D139E8DA52C5801A13C1EE222B2B882
SHA-256:	61D7CCC5D2C41BF86BE6CEFB0063405067849BA64E9F219F60596EF09A54A942
SHA-512:	EFFE15E105FC5FA853E76917B533AAE6C75EBA9A256049FB5EAB88BBF319D63A4CE4AE3743A09D6A5F474B01649D6EDC5C8BCCC61B8CA9EA9E5C39E7AE724C16

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\ellipsis_635a63d500a92a0b8497cdc58d0f66b1[1].svg	
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-.607.607,1.107,1.107,0,0,1-.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-.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-.607,1.161,1.161,0,0,1,0-.893,1.164,1.164,0,0,1-.607-.607A1.107,1.107,0,0,1,14.857,8,1.107,1.107,0,0,1,14.857,6.857Z"/></svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\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\CS6IXJW6\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/2.63.1/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\CS6IXJW6\messagecenter~preview-components~uploads-manager-enduser.00e4aedbbd[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	258315
Entropy (8bit):	5.329535595008793
Encrypted:	false
SSDEEP:	3072:te3JHdzVr1YHZvk8H2RDyUlBgxIhVfwYgONQqwQfbk03rzRGtwMNBw6iJGU0QIMh:teugSiGoaXwS8q2
MD5:	B70776A770B1393CECDA3F91C6E9E8D5
SHA1:	0FB412D3513ED067208A60DA934991642E4D43C5
SHA-256:	279D2F39B269C55CB37310F69E90EED86F3815873AEAF727CF1D4E0DED7050C3
SHA-512:	B4C11D86D6622D120F33C52CE4D81453B5450984349147B1F698B5D6AE53ED9E617634AE40FF7A0243ADBD98B425B838A8976B7668A3C9B18BB77FB57FC167E2

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\messagecenter~preview-components~uploads-manager-enduser.00e4aedbbd[1].js	
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn01.boxcdn.net/enduser/messagecenter~preview-components~uploads-manager-enduser.00e4aedbbd.js
Preview:	/*! For license information please see messagecenter~preview-components~uploads-manager-enduser.00e4aedbbd.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\CS6IXJW6\messagecenter~preview-components~uploads-manager-enduser.22b2a1dc4b[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.22b2a1dc4b.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\CS6IXJW6\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:	C77215B729D0E60C97F075998E88775CD0F813B4D094DC2FDD13E5711D16F4E5993D4521D0FBD5BF7150B0DBE253D88B1B1FF60901F053113C5D7C1919852D58
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://aadcdn.msftauth.net/ests/2.1/content/images/microsoft_logo_ee5c8d9fb6248c938fd0dc19370e90bd.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-.611,3.184,3.184,0,0,0-1.15-.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,.813,2.338,2.936,2.936,0,0,0,2.209.837M65.4,8.343a2.952,2.952,0,0,1,.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\CS6IXJW6\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\picker_account_aad_9de70d1c5191d1852a0d5aac28b44a6c[1].svg	
SHA-256:	5D3357BD875B7335ACE42E8EE3A64578E4253BED1A4E279109DE403EEDAE3A69
SHA-512:	CAC13FC2FE30E10772008F2AFF70FCA031EA9918E1F8C5C8B91CB9E79463383183406EFAADF89360DE3A08573FCDF2716C14DA6411E24B7E260B96AF84F0076
Malicious:	false
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\CS6IXJW6\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\CS6IXJW6\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\OR0WKIO1\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\Lato-woff[1].css	
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,d09GRgABAAAA AdFcABMAAAADhOgAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABGRlRNAAABqAAAABwAAAccNlcTUdERUYAAAHEAAAANwAAADgSeA2uR1BPUwAAAf wAANZ6AAGuYg7b1pNHU1VCAADYeAAAAywAAAtGQYaNc09TLzIAANukAAAAXwAAAGBp8+XGY21hcAAA3AQAAATZAAAGoHgSIT5jdnQgAADg4AAAAHIAAADqPz mz1GZwZ20AAOFUAAAFqAAAC5fkFNvwZ2FzcAAA5vwAAAAIAAAACAAAABBnbHlmAADnBAAAwI4AAWHYuL0/gWhlYWQAAaeUAAAAMQAAADYO+nFm aGhlYQABp8gAAAAhAAAAJBEGCeFobXR4AAGn7AAACQ4AABIS60ObMmxvY2EAAbD8AAAI5AAACR6IDi0mbWF4cAABueAAAAAgAAAAIAZMAeluYW1lAAG6AAAA BQQAAA/ywsuuaHBvc3QAAb8EAAARqgAAJ+ABEAopcHJlcAAB0LAAAACiAAAAuW8KaTp3ZWJmAAHRVAAAAAYAAAAGYIZWjQAAAAEAAAAAzD2izwAAADR6Kh5 AAAAANKzEQR42mNgZGBg4ANiAwYQYGJgZWBkagLiZqY2BmamdhZvBkYWHxZfBiYWP5ZeBkYGFrAqBgBp7gRDAHjapL0JfE3X+v+/9t4h8zwPZkVJEVVTU1xU Y1ZVVFTVRbVVVXXbolJVVVdDTTVXFVU1z5XEHMFBcCKVSCJizEkaJyGhqmr932ed0+a06t77/f1vX5/9WWedtdd69nrW86zPSnZcoQkhPMQg8YFw6dS5e18R 8c/xY0eJBq

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\Priv8[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	259
Entropy (8bit):	5.135044672226177
Encrypted:	false
SSDEEP:	6:pn0+Dy9xwol6hEr6VX16hu9nPMQ1vS6p2+KqD:J0+ox0RJWWPdp9TT
MD5:	7A0E623D6ADE176E0EA796AB5937EB32
SHA1:	5E8939CEDD1FB95EDAEC6B6C5BAC895657C52BCF
SHA-256:	BD6A5466E4DB505154763B2BBDDD6F80D82A38FFA423D6ECFD7ECF0914C04111
SHA-512:	3479989CD8C5950BF3CE021C3F0740AAF8626B0F59BA6BBD96B51A71040F873B8C7AF48EA43A38494736527AE034A020BA00BBC48213C25AE2E1DBB5584ADD5 1
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">.<html><head>.<title>301 Moved Permanently</title>.</head><body>. Moved Permanently . The document has moved here. .</body></html>.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\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, 791x1024, frames 3
Category:	downloaded
Size (bytes):	37968
Entropy (8bit):	6.522458724694474
Encrypted:	false
SSDEEP:	384:FIa4643Kpq0T1TZhSRM+9y1dr88+CpFzT8t/BGlwP3IjyZH7XHT/quB:FI/VKp9hF1dreoNwfawQ+1HXB
MD5:	391B5D6794881054CBFC41C3207489D8
SHA1:	BACA7096071E1DAFD17773F3223C4DE9A3CCDBC1
SHA-256:	AA9B420A9B6F1628708BC0D9A8D7FB0263BCA4988AC7705CF1D6BAAAF965B8BC
SHA-512:	BB85B075E3A8B881769B1FC88A4B01582249B9CCFA7BC4CBA05DFDE03106C21FBE1749FF7E49B85F7FC43FAA18AAB75181585D5319B7CD738E005CB0B233E4 3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://public.boxcloud.com/api/2.0/internal_files/769061146049/versions/820635523649/representations/jpg_1024x1024/content/?access_token=1!fmlW-vM-7PNEtQU8rjxdwCNTmFuQMPi2C-BtdB8hk6R0uHc1mTO3V7YdAc_iF13bybP6PF2AiZMDUZRPtgDU5iXF7Fs9vZEVgPJXZnBpe_D2QKViofc9yFzDMtw1DEwpfIMh-_G0zeN8ke2PTxIID8JUHrv8UAa81kuQV_bIkirObse46QQizWNlhi4RZ9hIEBYJcpMc_I8J7asiLRNd0HIerWaSUAK9er9JtmPvjTctNe9kKJiQevOBb5N0hmsGOzvcVmLUJzXc_NxXDsBOJWvHJtf0QnfL52Zs8Kti3-7MZqiCpyv0q41RRuQFCsJiYuecs_iZ7I6YHiiu6sOkdHQvOlkrwISSixgt_AKd5SEBKXzwWBu8hkeDkMNcE0-ytskk4fU_0wyis9bNTw8SsfTXL-d9viY9EXJJqLLLzISPWbyenm0Wg5vxlDR4i4gZ2YG_Dta919PG6vkbThVdlZl0vMYsOSEYRS04MnSR6o0lG1MeiUZdmcdLhyGZz48W6HhVZz6eUowLdmkZvAjHW-zvZXmoRH54oXTmG2jdLkkKyAvcPww19BR8EfQZkS4.&shared_link=https%3A%2F%2Fapp.box.com%2Fs%2Fxygsjhx8uarct1s5ilzuk9uozpewcgk2&box_client_name=box-content-preview&box_client_version=2.63.1
Preview:	......JFIF.....Exif..MM.*.....J.....R.(.....i.....Z.....0232.....9.....0100.....ASCII...pdfWidth:612.00pts,pdfHeight:792.00pts,numPages:1....C.....C.....b.....!1."A....2QW...#VXa....7Bqv...36RUbu.....$%5Srs..&'(48CFf.cetw.....M.....!1..T.....AQSaq..."25s.....36Rr.#4bBC.....$%&D.....?.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\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:QSNTmTFxg4lyyyyyyyyyyyyio7eeeeeeeekzgsLsLsLsLsQZp:nfgyyyyyyyyyyyynzQQQQQO
MD5:	12E3DAC858061D088023B2BD48E2FA96

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\favicon_a_eupayfgghqiai7k9sol6lg2[1].ico	
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.........................................""""""""""""""""""""""""""""""" ...3
33333333333333333333333333333"""""""""""""""""""""""""""""""" ...33333333333333333333333333333"""""""""""""""""""""""""""""""" ...33333333333333333333333333333""""
"""""""""""""""""""""""""""" ...33333333333333333333333333333"""""""""""""""""""""""""""""""" ...33333333333333333333333333333"""""""""""""""""""""""""""""""" ...33333333333
333333333333333333""""""""""""""""""""""""""""""""" ...33333333333333333333333333333"""""""""""""""""""""""""""""""" ...33333333333333333333333333333"""""""""""""""""""""""""""""""""
"""""""" ...33333333333333333333333333333"""""""""""""""""""""""""""""""" ...33333333333333333333333333333"""""""""""""""""""""""""""""""" ...33333333333333333333
333333333"""""""""""""""""""""""""""""""" ...33333333333333333333333333333""""""""""""""""""""""""""""
```


C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\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:	E15B0AB4A5E0A254726DD07335E525FFCA73573AB19177E4446CF5041681C9B097FCC12FAF653C8C6360270CABAFB15514310CDE5DA50D7D84ABE1EC32FBC9 B
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("QbLZ
JtXF68"),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._onRe
size=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.pad
dingBottom,10)||0,h=i-d-u,f=l-s-c;(!t&&n.state.hei
```

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\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\OR0WKIO1\preview-components.960fd72025[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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\preview-components.960fd72025[1].js	
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.960fd72025.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\OR0WKIO1\preview[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	55663
Entropy (8bit):	5.022130019841686
Encrypted:	false
SSDEEP:	768:SSI0/vyIN136bUEcDefZYMki45g4vcqK7KOdUy7:BD36gETZV4RK7KOd3
MD5:	7AE9D873A308184A7B92E65BAF78118B
SHA1:	AF043306849A84645F8AADF500DF40720A500D35
SHA-256:	8E54B91D08B1193B9FB597DC92F7A993586DB33E90305846E79C8A0F0B186A45
SHA-512:	2A155177AFF6A3F8139F1FB50254CC04CAEFC885541D8BA08D34DF1258491C7CB542264FBECAACA31E6E17BC365C2506B144FDCA745716F88827D61C8A2A9F6F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn01.boxcdn.net/platform/preview/2.63.1/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, 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\OR0WKIO1\runtime.3f7647bcda[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):	46044
Entropy (8bit):	4.911066668998243
Encrypted:	false
SSDEEP:	768:lwTRzRUGVKxdta9Cvxt6z/q00aEBQUvM+q0CHGiRzRUGVKxdta9Cvxt6z/q2GHgK:8ROxsz/qnaz6M+RFcROxsz/q2WrCRjTA
MD5:	AA7C8799305791D11B9AC6611B3F0269
SHA1:	14981EAFA7D96E633739E115FE1C258697017D00
SHA-256:	F111499FEA000AD0D04660D54586DE0E094BBF9C26696999A6CC49C9F7EBEBB0
SHA-512:	F919392AFB3E239D93A65AE8B42BEF0A3B0BB81E032FC5E1A7B47657D0245DF16EFA3BDE0534A607D384ABD0BBE51AC1EE71D3AA029BFB8C221BB215CB6E1BA5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn01.boxcdn.net/enduser/runtime.3f7647bcda.js
Preview:	!function(e){function a(a){for(var t,l,s=a[0],i=a[1],r=a[2],c=0,f=[];c<s.length;c++)l=s[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 d.push.apply(d,r||[]),o()}function o(){for(var e,a=0;a<d.length;a++){for(var o=d[a],t=!0,l=1;l<o.length;l++){var i=o[l];0!==n[i]&&(t=!1)}t&&(d.splice(a--,1),e=s(s.s=o[0]))}return e}var t={},l={runtime:0},n={runtime:0},d=[];function s(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,s),o.l=!0,o.exports}s.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\OR0WKIO1\uploads-manager-enduser.dd5d6cf4cc[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\uploads-manager-enduser.dd5d6cf4cc[1].js	
Size (bytes):	96149
Entropy (8bit):	5.3214898330231115
Encrypted:	false
SSDEEP:	1536:8QgaSb0h7ChdEF6QgNWCONl6CGKduS2z3Vh8MXBJ6P:Dh7C4YQgNWCqoCpduSwVhvXBJ6P
MD5:	1F7261803D7D358388889FA600202922
SHA1:	047CF1491093D8192269380808374433442636AA
SHA-256:	AB5219B3F8B4A49EC5E962C6F501A7FA969B76C061438F4E41CF02C9F0866A49
SHA-512:	E1780175063CF039EED5A5878662CEE8933B46458857D619071DBD67F00CCF22814E9FCD1495087AC48DDF939B5E222BFAED9B1C9E6F787C956E0453CD6273A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn01.boxcdn.net/enduser/uploads-manager-enduser.dd5d6cf4cc.js
Preview:	/*! For license information please see uploads-manager-enduser.dd5d6cf4cc.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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\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:	F7B433D5671DE6418BACBCA18E1DB2755F6A00C2845149FB0B3BEFFEFBB6EF3D2C6DAEA24BE5646FBD8391E2C7515D3B033BD4F431D505D67D67E2005F4D0I 2B
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("t2Dn8I5vat"),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\Temp\dat9AF4.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:	F7D639520F4C3A3539AD7506EC1CEBED8107C2A264316FE0E98A15132ACCFE6212A22391F4A7203B6D8304B3222B603F0137BA9ACAC7478F217363EEF4556DEI
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\dat9B24.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

C:\Users\user\AppData\Local\Temp\dat9B24.tmp	
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\datB813.tmp	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	OpenType font data
Category:	dropped
Size (bytes):	1120
Entropy (8bit):	3.2472609733085966
Encrypted:	false
SSDEEP:	12:+51lR921oNY0p9b1IfSly/VAAc5EK/HU1qsG1bhCEo8+R5+ddmq0/gNV11Mp1VKa:+Dz9fuUx1IfSljAP3G6M3B8PKnAo/K
MD5:	1024ABADCA5CA30E187330CB99DF5508
SHA1:	8C68B7E5848941CC930FEDDBF136B76D2FCFF9B1
SHA-256:	26B4789FDA6EB8C31CDD52798D32D446AF69F0788934DF2B47B5FF5186FAE0E7
SHA-512:	812ACAC8D519BB509D9BB43D8BFA85F8A2F7414230E86F4B11DFCF7831191ABB563133314F4EB32A9B863CB85377756BDFD36DB70B3046742E3076E852D8B89
Malicious:	false
Reputation:	low
Preview:	OTTO.....0CFF ..{.....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...!.....|..... .!XXXlt16117774100220XXXXXXXX

C:\Users\user\AppData\Local\Temp\~DF230665274301A536.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	59137
Entropy (8bit):	0.7826243050689188
Encrypted:	false
SSDEEP:	192:kBqoxKAuqR+yU+XkN1h41xAi4NT18Ni4NT18q28qEPqESmv:kBqoxKAuqR+yU+XkN1y1yOT28/imv
MD5:	F0355CB7143DD97CDB1096F913D2315F
SHA1:	85ED9447A2B9D4737162E2254ACF42DD847AA8FD
SHA-256:	301D0C0A66C83309867CED4B6981F710E23D92DCB0262296B270B3846EF80DE9
SHA-512:	6724D3CCE9C458118CE6B3E5AFFAE86BA9D771422CA5A6883FFA91687A7BE97E0715B2C3F0E8245985E1397E0C306566B9F3DC300372CAA90FE858EB232B9FC 6
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF2C2A06D5A055137F.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.3231282143796146
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laAV:kBqoxxJhHWSVSEabV
MD5:	6C48679CB8607F6DD468CEF2A9FADEE5

C:\Users\user\AppData\Local\Temp\~DF2C2A06D5A055137F.TMP	
SHA1:	1830FC7DEC3E4ADB7131869629A2F3E86D79D6B0
SHA-256:	BFE80BEBAADCC33AB04726217BE5DE8FB32D0F170B58894C7E7A145518BC9F7B
SHA-512:	B7849C4BA6A52F9056514F787B974786067F24CECFDF34CAD948C7440D1C487C877C14B7C1D0B87C72EFBFCEA6BB09695A106C2CF13E7C935E0D7AADCFB817C0
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

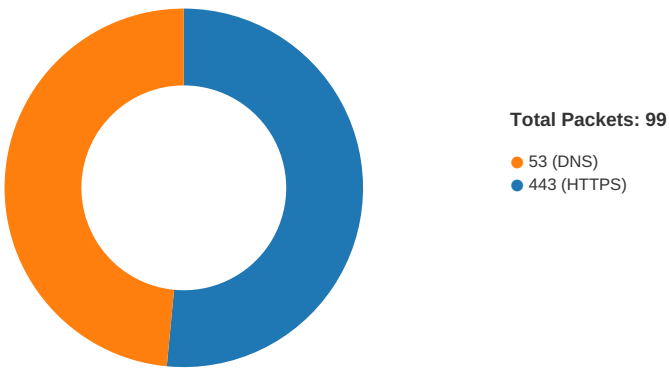
C:\Users\user\AppData\Local\Temp\~DFB9D3966484AB6D52.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.47666552801181133
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loBS9loBC9lWBIbmFasFYzYlPvsv3:kBqoIBdBbBIyFasFYzYpvsv3
MD5:	AA7B88FA29CF3179FB72CB77167FF5A3
SHA1:	572FC62909DB247F8B7DF366B52FB0377DEE0B90
SHA-256:	871B58C8A6AF80B040A51521779F2D2532C142E9C6CC0AAC5AEC023DC291793F
SHA-512:	5ABE081C562B73082F14AD1EBEBF3BAE50C4F12D58DA7770050637AEB8D7CD2BEC9F31E6313175826880C5BD160C260D0C3453842A00F888A6347D240BCBE63
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 20:56:42.083101034 CET	49729	443	192.168.2.4	185.235.236.201

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 20:56:42.083493948 CET	49730	443	192.168.2.4	185.235.236.201
Jan 27, 2021 20:56:42.128700018 CET	443	49729	185.235.236.201	192.168.2.4
Jan 27, 2021 20:56:42.128798008 CET	49729	443	192.168.2.4	185.235.236.201
Jan 27, 2021 20:56:42.128962994 CET	443	49730	185.235.236.201	192.168.2.4
Jan 27, 2021 20:56:42.129043102 CET	49730	443	192.168.2.4	185.235.236.201
Jan 27, 2021 20:56:42.138180017 CET	49729	443	192.168.2.4	185.235.236.201
Jan 27, 2021 20:56:42.138415098 CET	49730	443	192.168.2.4	185.235.236.201
Jan 27, 2021 20:56:42.183650017 CET	443	49729	185.235.236.201	192.168.2.4
Jan 27, 2021 20:56:42.183715105 CET	443	49730	185.235.236.201	192.168.2.4
Jan 27, 2021 20:56:42.184581041 CET	443	49729	185.235.236.201	192.168.2.4
Jan 27, 2021 20:56:42.184598923 CET	443	49729	185.235.236.201	192.168.2.4
Jan 27, 2021 20:56:42.184608936 CET	443	49729	185.235.236.201	192.168.2.4
Jan 27, 2021 20:56:42.184658051 CET	443	49730	185.235.236.201	192.168.2.4
Jan 27, 2021 20:56:42.184665918 CET	49729	443	192.168.2.4	185.235.236.201
Jan 27, 2021 20:56:42.184674978 CET	443	49730	185.235.236.201	192.168.2.4
Jan 27, 2021 20:56:42.184684992 CET	49729	443	192.168.2.4	185.235.236.201
Jan 27, 2021 20:56:42.184689045 CET	443	49730	185.235.236.201	192.168.2.4
Jan 27, 2021 20:56:42.184725046 CET	49730	443	192.168.2.4	185.235.236.201
Jan 27, 2021 20:56:42.184756041 CET	49730	443	192.168.2.4	185.235.236.201
Jan 27, 2021 20:56:42.225394964 CET	49729	443	192.168.2.4	185.235.236.201
Jan 27, 2021 20:56:42.228389025 CET	49730	443	192.168.2.4	185.235.236.201
Jan 27, 2021 20:56:42.231785059 CET	49729	443	192.168.2.4	185.235.236.201
Jan 27, 2021 20:56:42.271600008 CET	443	49729	185.235.236.201	192.168.2.4
Jan 27, 2021 20:56:42.271697998 CET	49729	443	192.168.2.4	185.235.236.201
Jan 27, 2021 20:56:42.275031090 CET	443	49730	185.235.236.201	192.168.2.4
Jan 27, 2021 20:56:42.275124073 CET	49730	443	192.168.2.4	185.235.236.201
Jan 27, 2021 20:56:42.316648960 CET	443	49729	185.235.236.201	192.168.2.4
Jan 27, 2021 20:56:42.573462963 CET	443	49729	185.235.236.201	192.168.2.4
Jan 27, 2021 20:56:42.573497057 CET	443	49729	185.235.236.201	192.168.2.4
Jan 27, 2021 20:56:42.573633909 CET	49729	443	192.168.2.4	185.235.236.201
Jan 27, 2021 20:56:42.701533079 CET	443	49729	185.235.236.201	192.168.2.4
Jan 27, 2021 20:56:42.701555014 CET	443	49729	185.235.236.201	192.168.2.4
Jan 27, 2021 20:56:42.701612949 CET	49729	443	192.168.2.4	185.235.236.201
Jan 27, 2021 20:56:42.701641083 CET	49729	443	192.168.2.4	185.235.236.201
Jan 27, 2021 20:56:42.759001970 CET	443	49729	185.235.236.201	192.168.2.4
Jan 27, 2021 20:56:42.759025097 CET	443	49729	185.235.236.201	192.168.2.4
Jan 27, 2021 20:56:42.759109974 CET	49729	443	192.168.2.4	185.235.236.201
Jan 27, 2021 20:56:42.761488914 CET	49729	443	192.168.2.4	185.235.236.201
Jan 27, 2021 20:56:44.446897984 CET	49729	443	192.168.2.4	185.235.236.201
Jan 27, 2021 20:56:44.494687080 CET	443	49729	185.235.236.201	192.168.2.4
Jan 27, 2021 20:56:45.086654902 CET	443	49729	185.235.236.201	192.168.2.4
Jan 27, 2021 20:56:45.086679935 CET	443	49729	185.235.236.201	192.168.2.4
Jan 27, 2021 20:56:45.086813927 CET	49729	443	192.168.2.4	185.235.236.201
Jan 27, 2021 20:56:46.974108934 CET	49729	443	192.168.2.4	185.235.236.201
Jan 27, 2021 20:56:46.977154970 CET	49729	443	192.168.2.4	185.235.236.201
Jan 27, 2021 20:56:46.990907907 CET	49730	443	192.168.2.4	185.235.236.201
Jan 27, 2021 20:56:47.019742966 CET	443	49729	185.235.236.201	192.168.2.4
Jan 27, 2021 20:56:47.022708893 CET	443	49729	185.235.236.201	192.168.2.4
Jan 27, 2021 20:56:47.036539078 CET	443	49730	185.235.236.201	192.168.2.4
Jan 27, 2021 20:56:47.218039989 CET	443	49730	185.235.236.201	192.168.2.4
Jan 27, 2021 20:56:47.218426943 CET	49730	443	192.168.2.4	185.235.236.201
Jan 27, 2021 20:56:47.235125065 CET	443	49729	185.235.236.201	192.168.2.4
Jan 27, 2021 20:56:47.235158920 CET	443	49729	185.235.236.201	192.168.2.4
Jan 27, 2021 20:56:47.235450029 CET	49729	443	192.168.2.4	185.235.236.201
Jan 27, 2021 20:56:47.341296911 CET	49739	443	192.168.2.4	185.235.236.197
Jan 27, 2021 20:56:47.341420889 CET	49740	443	192.168.2.4	185.235.236.197
Jan 27, 2021 20:56:47.388400078 CET	443	49739	185.235.236.197	192.168.2.4
Jan 27, 2021 20:56:47.388444901 CET	443	49740	185.235.236.197	192.168.2.4
Jan 27, 2021 20:56:47.388521910 CET	49739	443	192.168.2.4	185.235.236.197
Jan 27, 2021 20:56:47.388561964 CET	49740	443	192.168.2.4	185.235.236.197
Jan 27, 2021 20:56:47.389501095 CET	49740	443	192.168.2.4	185.235.236.197
Jan 27, 2021 20:56:47.389919043 CET	49739	443	192.168.2.4	185.235.236.197
Jan 27, 2021 20:56:47.435595989 CET	443	49740	185.235.236.197	192.168.2.4
Jan 27, 2021 20:56:47.435920954 CET	443	49739	185.235.236.197	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 20:56:47.437108994 CET	443	49739	185.235.236.197	192.168.2.4
Jan 27, 2021 20:56:47.437150955 CET	443	49739	185.235.236.197	192.168.2.4
Jan 27, 2021 20:56:47.437187910 CET	443	49740	185.235.236.197	192.168.2.4
Jan 27, 2021 20:56:47.437222958 CET	443	49740	185.235.236.197	192.168.2.4
Jan 27, 2021 20:56:47.437248945 CET	49739	443	192.168.2.4	185.235.236.197
Jan 27, 2021 20:56:47.437283993 CET	443	49740	185.235.236.197	192.168.2.4
Jan 27, 2021 20:56:47.437314034 CET	443	49739	185.235.236.197	192.168.2.4
Jan 27, 2021 20:56:47.437329054 CET	49739	443	192.168.2.4	185.235.236.197
Jan 27, 2021 20:56:47.437360048 CET	49740	443	192.168.2.4	185.235.236.197
Jan 27, 2021 20:56:47.437429905 CET	49740	443	192.168.2.4	185.235.236.197
Jan 27, 2021 20:56:47.437973976 CET	49739	443	192.168.2.4	185.235.236.197
Jan 27, 2021 20:56:47.453700066 CET	49740	443	192.168.2.4	185.235.236.197
Jan 27, 2021 20:56:47.454072952 CET	49739	443	192.168.2.4	185.235.236.197
Jan 27, 2021 20:56:47.454216003 CET	49740	443	192.168.2.4	185.235.236.197
Jan 27, 2021 20:56:47.500062943 CET	443	49740	185.235.236.197	192.168.2.4
Jan 27, 2021 20:56:47.500098944 CET	443	49739	185.235.236.197	192.168.2.4
Jan 27, 2021 20:56:47.500216007 CET	49740	443	192.168.2.4	185.235.236.197
Jan 27, 2021 20:56:47.500278950 CET	49739	443	192.168.2.4	185.235.236.197
Jan 27, 2021 20:56:47.540074110 CET	443	49740	185.235.236.197	192.168.2.4
Jan 27, 2021 20:56:47.642697096 CET	443	49740	185.235.236.197	192.168.2.4
Jan 27, 2021 20:56:47.642831087 CET	49740	443	192.168.2.4	185.235.236.197
Jan 27, 2021 20:56:47.649180889 CET	49740	443	192.168.2.4	185.235.236.197
Jan 27, 2021 20:56:47.695084095 CET	443	49740	185.235.236.197	192.168.2.4
Jan 27, 2021 20:56:47.695130110 CET	443	49740	185.235.236.197	192.168.2.4
Jan 27, 2021 20:56:47.955008030 CET	443	49740	185.235.236.197	192.168.2.4
Jan 27, 2021 20:56:47.955060959 CET	443	49740	185.235.236.197	192.168.2.4
Jan 27, 2021 20:56:47.955229998 CET	49740	443	192.168.2.4	185.235.236.197
Jan 27, 2021 20:56:49.006270885 CET	49740	443	192.168.2.4	185.235.236.197
Jan 27, 2021 20:56:49.052442074 CET	443	49740	185.235.236.197	192.168.2.4
Jan 27, 2021 20:56:49.074139118 CET	49742	443	192.168.2.4	185.235.236.200
Jan 27, 2021 20:56:49.091578960 CET	49743	443	192.168.2.4	185.235.236.200
Jan 27, 2021 20:56:49.121886969 CET	443	49742	185.235.236.200	192.168.2.4
Jan 27, 2021 20:56:49.122145891 CET	49742	443	192.168.2.4	185.235.236.200
Jan 27, 2021 20:56:49.137208939 CET	443	49743	185.235.236.200	192.168.2.4
Jan 27, 2021 20:56:49.137320042 CET	49743	443	192.168.2.4	185.235.236.200

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 20:56:37.000034094 CET	62389	53	192.168.2.4	8.8.8.8
Jan 27, 2021 20:56:37.050812960 CET	53	62389	8.8.8.8	192.168.2.4
Jan 27, 2021 20:56:38.032367945 CET	49910	53	192.168.2.4	8.8.8.8
Jan 27, 2021 20:56:38.080231905 CET	53	49910	8.8.8.8	192.168.2.4
Jan 27, 2021 20:56:40.978620052 CET	55854	53	192.168.2.4	8.8.8.8
Jan 27, 2021 20:56:41.038850069 CET	53	55854	8.8.8.8	192.168.2.4
Jan 27, 2021 20:56:41.990494013 CET	64549	53	192.168.2.4	8.8.8.8
Jan 27, 2021 20:56:42.070885897 CET	53	64549	8.8.8.8	192.168.2.4
Jan 27, 2021 20:56:42.423512936 CET	63153	53	192.168.2.4	8.8.8.8
Jan 27, 2021 20:56:42.471510887 CET	53	63153	8.8.8.8	192.168.2.4
Jan 27, 2021 20:56:42.649131060 CET	52991	53	192.168.2.4	8.8.8.8
Jan 27, 2021 20:56:42.707439899 CET	53	52991	8.8.8.8	192.168.2.4
Jan 27, 2021 20:56:45.999100924 CET	53700	53	192.168.2.4	8.8.8.8
Jan 27, 2021 20:56:46.048692942 CET	53	53700	8.8.8.8	192.168.2.4
Jan 27, 2021 20:56:47.269032955 CET	51726	53	192.168.2.4	8.8.8.8
Jan 27, 2021 20:56:47.337168932 CET	53	51726	8.8.8.8	192.168.2.4
Jan 27, 2021 20:56:47.379220009 CET	56794	53	192.168.2.4	8.8.8.8
Jan 27, 2021 20:56:47.427166939 CET	53	56794	8.8.8.8	192.168.2.4
Jan 27, 2021 20:56:48.793329954 CET	56534	53	192.168.2.4	8.8.8.8
Jan 27, 2021 20:56:48.873526096 CET	53	56534	8.8.8.8	192.168.2.4
Jan 27, 2021 20:56:49.986251116 CET	56627	53	192.168.2.4	8.8.8.8
Jan 27, 2021 20:56:50.037313938 CET	53	56627	8.8.8.8	192.168.2.4
Jan 27, 2021 20:56:50.991848946 CET	56621	53	192.168.2.4	8.8.8.8
Jan 27, 2021 20:56:51.044514894 CET	53	56621	8.8.8.8	192.168.2.4
Jan 27, 2021 20:56:51.801371098 CET	63116	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 20:56:51.851566076 CET	53	63116	8.8.8.8	192.168.2.4
Jan 27, 2021 20:56:52.989106894 CET	64078	53	192.168.2.4	8.8.8.8
Jan 27, 2021 20:56:53.042331934 CET	53	64078	8.8.8.8	192.168.2.4
Jan 27, 2021 20:56:53.922698021 CET	64801	53	192.168.2.4	8.8.8.8
Jan 27, 2021 20:56:53.981288910 CET	53	64801	8.8.8.8	192.168.2.4
Jan 27, 2021 20:56:54.945776939 CET	61721	53	192.168.2.4	8.8.8.8
Jan 27, 2021 20:56:54.997560024 CET	53	61721	8.8.8.8	192.168.2.4
Jan 27, 2021 20:56:59.065907955 CET	51255	53	192.168.2.4	8.8.8.8
Jan 27, 2021 20:56:59.118026018 CET	53	51255	8.8.8.8	192.168.2.4
Jan 27, 2021 20:56:59.839464903 CET	61522	53	192.168.2.4	8.8.8.8
Jan 27, 2021 20:56:59.890142918 CET	53	61522	8.8.8.8	192.168.2.4
Jan 27, 2021 20:57:00.643385887 CET	52337	53	192.168.2.4	8.8.8.8
Jan 27, 2021 20:57:00.701803923 CET	53	52337	8.8.8.8	192.168.2.4
Jan 27, 2021 20:57:00.753429890 CET	55046	53	192.168.2.4	8.8.8.8
Jan 27, 2021 20:57:00.794066906 CET	49612	53	192.168.2.4	8.8.8.8
Jan 27, 2021 20:57:00.803826094 CET	53	55046	8.8.8.8	192.168.2.4
Jan 27, 2021 20:57:00.841835976 CET	53	49612	8.8.8.8	192.168.2.4
Jan 27, 2021 20:57:04.595957994 CET	49285	53	192.168.2.4	8.8.8.8
Jan 27, 2021 20:57:04.927248955 CET	53	49285	8.8.8.8	192.168.2.4
Jan 27, 2021 20:57:05.797003031 CET	50601	53	192.168.2.4	8.8.8.8
Jan 27, 2021 20:57:05.847790956 CET	53	50601	8.8.8.8	192.168.2.4
Jan 27, 2021 20:57:06.188580990 CET	60875	53	192.168.2.4	8.8.8.8
Jan 27, 2021 20:57:06.253616095 CET	53	60875	8.8.8.8	192.168.2.4
Jan 27, 2021 20:57:06.370345116 CET	56448	53	192.168.2.4	8.8.8.8
Jan 27, 2021 20:57:06.418323994 CET	53	56448	8.8.8.8	192.168.2.4
Jan 27, 2021 20:57:07.547945023 CET	59172	53	192.168.2.4	8.8.8.8
Jan 27, 2021 20:57:07.611231089 CET	53	59172	8.8.8.8	192.168.2.4
Jan 27, 2021 20:57:10.985579014 CET	62420	53	192.168.2.4	8.8.8.8
Jan 27, 2021 20:57:11.034861088 CET	53	62420	8.8.8.8	192.168.2.4
Jan 27, 2021 20:57:11.639101982 CET	60579	53	192.168.2.4	8.8.8.8
Jan 27, 2021 20:57:11.689758062 CET	53	60579	8.8.8.8	192.168.2.4
Jan 27, 2021 20:57:12.027564049 CET	62420	53	192.168.2.4	8.8.8.8
Jan 27, 2021 20:57:12.076078892 CET	53	62420	8.8.8.8	192.168.2.4
Jan 27, 2021 20:57:12.662127018 CET	60579	53	192.168.2.4	8.8.8.8
Jan 27, 2021 20:57:12.710066080 CET	53	60579	8.8.8.8	192.168.2.4
Jan 27, 2021 20:57:13.204858065 CET	62420	53	192.168.2.4	8.8.8.8
Jan 27, 2021 20:57:13.252743959 CET	53	62420	8.8.8.8	192.168.2.4
Jan 27, 2021 20:57:13.680162907 CET	60579	53	192.168.2.4	8.8.8.8
Jan 27, 2021 20:57:13.741640091 CET	53	60579	8.8.8.8	192.168.2.4
Jan 27, 2021 20:57:15.225133896 CET	62420	53	192.168.2.4	8.8.8.8
Jan 27, 2021 20:57:15.273211002 CET	53	62420	8.8.8.8	192.168.2.4
Jan 27, 2021 20:57:15.675144911 CET	60579	53	192.168.2.4	8.8.8.8
Jan 27, 2021 20:57:15.723786116 CET	53	60579	8.8.8.8	192.168.2.4
Jan 27, 2021 20:57:19.238157988 CET	62420	53	192.168.2.4	8.8.8.8
Jan 27, 2021 20:57:19.294503927 CET	53	62420	8.8.8.8	192.168.2.4
Jan 27, 2021 20:57:19.691044092 CET	60579	53	192.168.2.4	8.8.8.8
Jan 27, 2021 20:57:19.747602940 CET	53	60579	8.8.8.8	192.168.2.4
Jan 27, 2021 20:57:22.680011034 CET	50183	53	192.168.2.4	8.8.8.8
Jan 27, 2021 20:57:22.740631104 CET	53	50183	8.8.8.8	192.168.2.4
Jan 27, 2021 20:57:23.451667070 CET	61531	53	192.168.2.4	8.8.8.8
Jan 27, 2021 20:57:23.510921955 CET	53	61531	8.8.8.8	192.168.2.4
Jan 27, 2021 20:57:24.159921885 CET	49228	53	192.168.2.4	8.8.8.8
Jan 27, 2021 20:57:24.201653004 CET	59794	53	192.168.2.4	8.8.8.8
Jan 27, 2021 20:57:24.220881939 CET	53	49228	8.8.8.8	192.168.2.4
Jan 27, 2021 20:57:24.273008108 CET	53	59794	8.8.8.8	192.168.2.4
Jan 27, 2021 20:57:24.648906946 CET	55916	53	192.168.2.4	8.8.8.8
Jan 27, 2021 20:57:24.707535982 CET	53	55916	8.8.8.8	192.168.2.4
Jan 27, 2021 20:57:25.070554018 CET	52752	53	192.168.2.4	8.8.8.8
Jan 27, 2021 20:57:25.131892920 CET	53	52752	8.8.8.8	192.168.2.4
Jan 27, 2021 20:57:25.189759970 CET	60542	53	192.168.2.4	8.8.8.8
Jan 27, 2021 20:57:25.249337912 CET	53	60542	8.8.8.8	192.168.2.4
Jan 27, 2021 20:57:25.814301014 CET	60689	53	192.168.2.4	8.8.8.8
Jan 27, 2021 20:57:25.864604950 CET	53	60689	8.8.8.8	192.168.2.4
Jan 27, 2021 20:57:26.625644922 CET	64206	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 20:57:26.684880972 CET	53	64206	8.8.8.8	192.168.2.4
Jan 27, 2021 20:57:27.425050020 CET	50904	53	192.168.2.4	8.8.8.8
Jan 27, 2021 20:57:27.482218027 CET	53	50904	8.8.8.8	192.168.2.4
Jan 27, 2021 20:57:28.801938057 CET	57525	53	192.168.2.4	8.8.8.8
Jan 27, 2021 20:57:28.858516932 CET	53	57525	8.8.8.8	192.168.2.4
Jan 27, 2021 20:57:29.683808088 CET	53814	53	192.168.2.4	8.8.8.8
Jan 27, 2021 20:57:29.740478039 CET	53	53814	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 27, 2021 20:56:41.990494013 CET	192.168.2.4	8.8.8.8	0x3a05	Standard query (0)	app.box.com	A (IP address)	IN (0x0001)
Jan 27, 2021 20:56:42.649131060 CET	192.168.2.4	8.8.8.8	0xbdc2	Standard query (0)	cdn01.boxcdn.net	A (IP address)	IN (0x0001)
Jan 27, 2021 20:56:47.269032955 CET	192.168.2.4	8.8.8.8	0x1ae8	Standard query (0)	api.box.com	A (IP address)	IN (0x0001)
Jan 27, 2021 20:56:48.793329954 CET	192.168.2.4	8.8.8.8	0x24b5	Standard query (0)	public.box cloud.com	A (IP address)	IN (0x0001)
Jan 27, 2021 20:57:00.643385887 CET	192.168.2.4	8.8.8.8	0xd1e0	Standard query (0)	cdn01.boxcdn.net	A (IP address)	IN (0x0001)
Jan 27, 2021 20:57:04.595957994 CET	192.168.2.4	8.8.8.8	0x7245	Standard query (0)	retreatceiling.com	A (IP address)	IN (0x0001)
Jan 27, 2021 20:57:05.797003031 CET	192.168.2.4	8.8.8.8	0x8e99	Standard query (0)	cdnjs.clou dflare.com	A (IP address)	IN (0x0001)
Jan 27, 2021 20:57:06.188580990 CET	192.168.2.4	8.8.8.8	0x984f	Standard query (0)	aadcdn.msf tauth.net	A (IP address)	IN (0x0001)
Jan 27, 2021 20:57:06.370345116 CET	192.168.2.4	8.8.8.8	0x88e2	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 27, 2021 20:56:42.070885897 CET	8.8.8.8	192.168.2.4	0x3a05	No error (0)	app.box.com		185.235.236.201	A (IP address)	IN (0x0001)
Jan 27, 2021 20:56:42.707439899 CET	8.8.8.8	192.168.2.4	0xbdc2	No error (0)	cdn01.boxc dn.net	cdn01.boxcdn.net.cdn.clo udflare.net		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 20:56:47.337168932 CET	8.8.8.8	192.168.2.4	0x1ae8	No error (0)	api.box.com		185.235.236.197	A (IP address)	IN (0x0001)
Jan 27, 2021 20:56:48.873526096 CET	8.8.8.8	192.168.2.4	0x24b5	No error (0)	public.box cloud.com		185.235.236.200	A (IP address)	IN (0x0001)
Jan 27, 2021 20:57:00.701803923 CET	8.8.8.8	192.168.2.4	0xd1e0	No error (0)	cdn01.boxc dn.net	cdn01.boxcdn.net.cdn.clo udflare.net		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 20:57:04.927248955 CET	8.8.8.8	192.168.2.4	0x7245	No error (0)	retreatcei ling.com		69.49.228.205	A (IP address)	IN (0x0001)
Jan 27, 2021 20:57:05.847790956 CET	8.8.8.8	192.168.2.4	0x8e99	No error (0)	cdnjs.clou dflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Jan 27, 2021 20:57:05.847790956 CET	8.8.8.8	192.168.2.4	0x8e99	No error (0)	cdnjs.clou dflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Jan 27, 2021 20:57:06.253616095 CET	8.8.8.8	192.168.2.4	0x984f	No error (0)	aadcdn.msf tauth.net	aadcdnoriginneu.azureed ge.net		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 20:57:06.253616095 CET	8.8.8.8	192.168.2.4	0x984f	No error (0)	cs1100.wpc .omegacdn.net		152.199.23.37	A (IP address)	IN (0x0001)
Jan 27, 2021 20:57:06.418323994 CET	8.8.8.8	192.168.2.4	0x88e2	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

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 27, 2021 20:56:42.184608936 CET	185.235.236.201	443	192.168.2.4	49729	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	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 27, 2021 20:56:42.184689045 CET	185.235.236.201	443	192.168.2.4	49730	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	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 27, 2021 20:56:47.437283993 CET	185.235.236.197	443	192.168.2.4	49740	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	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		
Jan 27, 2021 20:56:47.437314034 CET	185.235.236.197	443	192.168.2.4	49739	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	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		
Jan 27, 2021 20:56:49.185444117 CET	185.235.236.200	443	192.168.2.4	49743	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	Wed Feb 07 01:00:00 CET 2018	Fri Feb 19 13:00:00 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
Jan 27, 2021 20:56:49.194365978 CET	185.235.236.200	443	192.168.2.4	49742	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 27, 2021 20:57:05.250536919 CET	69.49.228.205	443	192.168.2.4	49757	CN=retreatceiling.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 24 01:00:00 CET 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Sun Apr 25 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 27, 2021 20:57:05.251398087 CET	69.49.228.205	443	192.168.2.4	49756	CN=retreatceiling.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 24 01:00:00 CET 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Sun Apr 25 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 27, 2021 20:57:05.940577030 CET	104.16.19.94	443	192.168.2.4	49758	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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 27, 2021 20:57:06.019237041 CET	104.16.19.94	443	192.168.2.4	49759	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 27, 2021 20:57:06.433592081 CET	152.199.23.37	443	192.168.2.4	49760	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 27, 2021 20:57:06.436614990 CET	152.199.23.37	443	192.168.2.4	49762	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 27, 2021 20:57:06.439728975 CET	152.199.23.37	443	192.168.2.4	49764	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

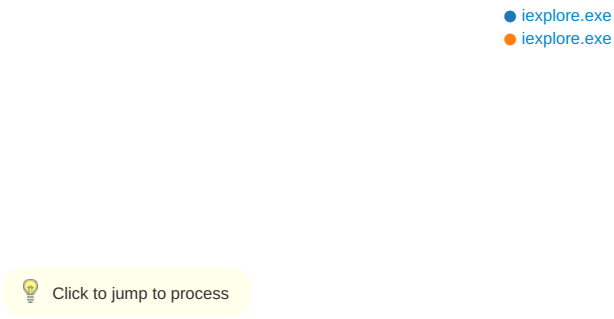
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 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 27, 2021 20:57:06.439980984 CET	152.199.23.37	443	192.168.2.4	49763	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 27, 2021 20:57:06.441705942 CET	152.199.23.37	443	192.168.2.4	49765	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 27, 2021 20:57:06.442387104 CET	152.199.23.37	443	192.168.2.4	49761	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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=DigiCert Global Root 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



System Behavior

Analysis Process: iexplore.exe PID: 6836 Parent PID: 800

General

Start time:	20:56:40
Start date:	27/01/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff739760000
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: 6880 Parent PID: 6836

General

Start time:	20:56:40
Start date:	27/01/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6836 CREDAT:17410 /prefetch:2
Imagebase:	0x12d0000
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