ID: 384773
Cookbook: browseurl.jbs
Time: 19:39:24
Date: 09/04/2021
Version: 31.0.0 Emerald

Table of Contents

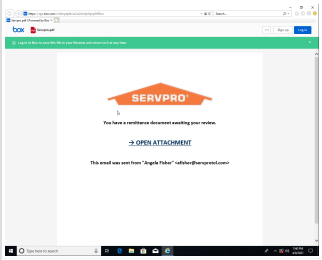
Analysis Report https://app.box.com/s/ldmpej4bczs3ra2…

Overview

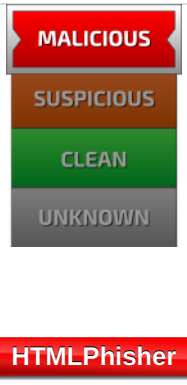
General Information

Sample URL:	http://https://app.box.com/s/ldmpej4bczs3ra2es3qlr0qrqifh99wc
Analysis ID:	384773
Infos:	

Most interesting Screenshot:



Detection

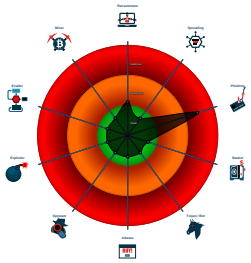


Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for URL or domain
- Yara detected HtmlPhish10
- Phishing site detected (based on im…
- Phishing site detected (based on log…
- HTML body contains low number of …
- HTML title does not match URL
- Invalid T&C link found
- Suspicious form URL found

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 6644 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6752 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6644 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

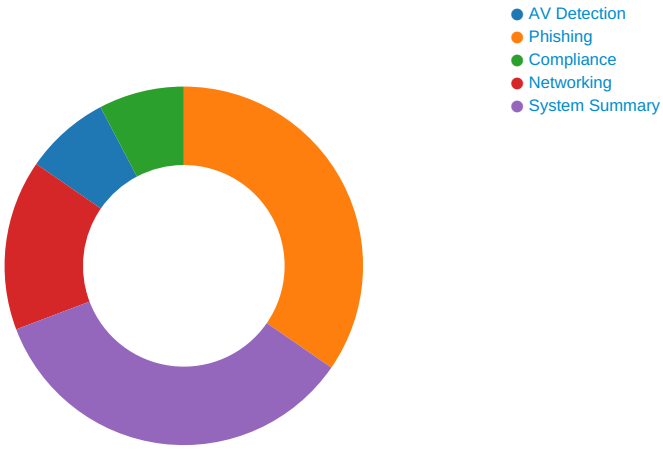
Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\li6orbsabcm5o36s3wlba8p8[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

Phishing:

Yara detected HtmlPhish10

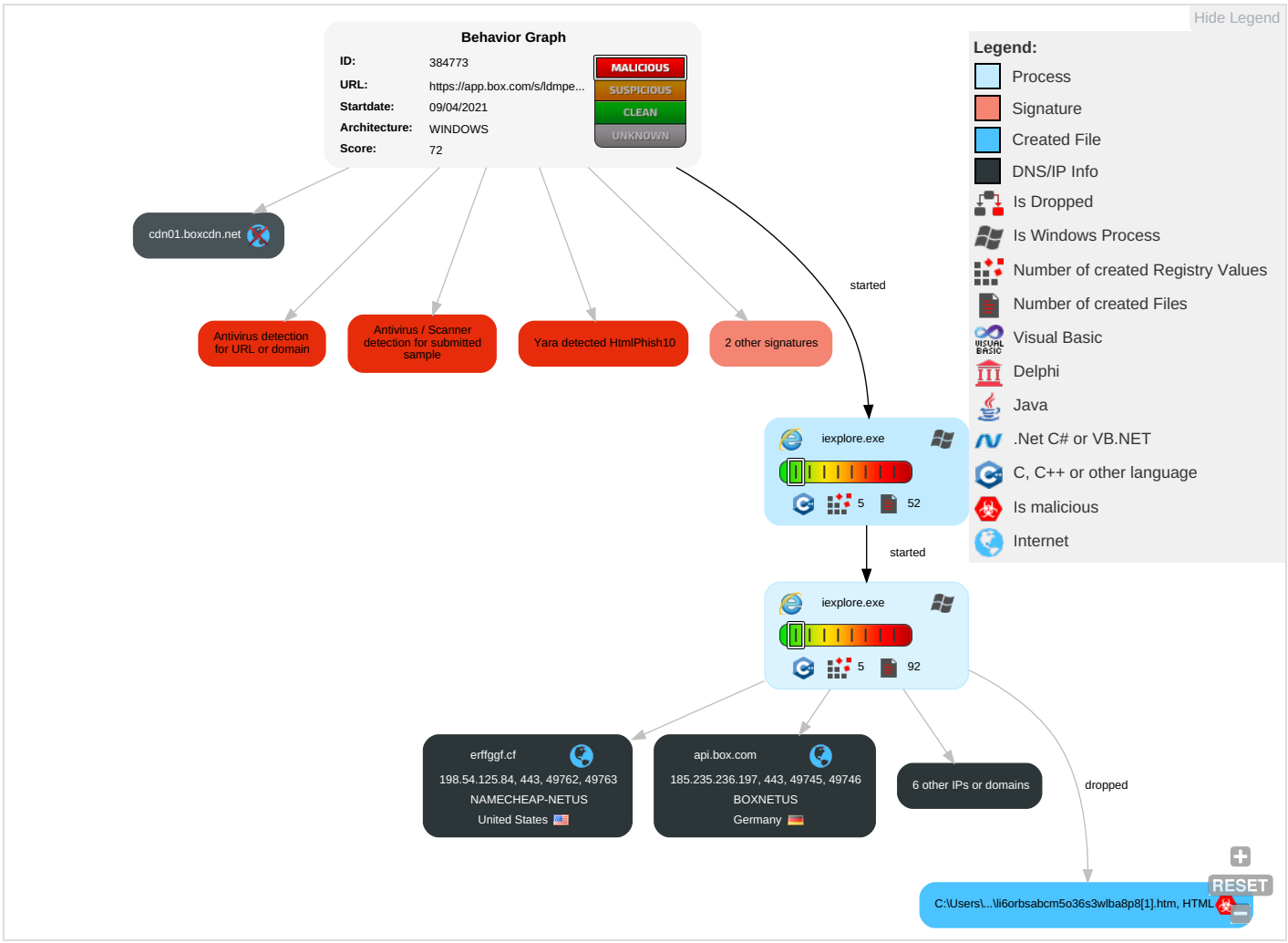
Phishing site detected (based on image similarity)

Phishing site detected (based on logo template match)

Mitre Att&ck Matrix

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

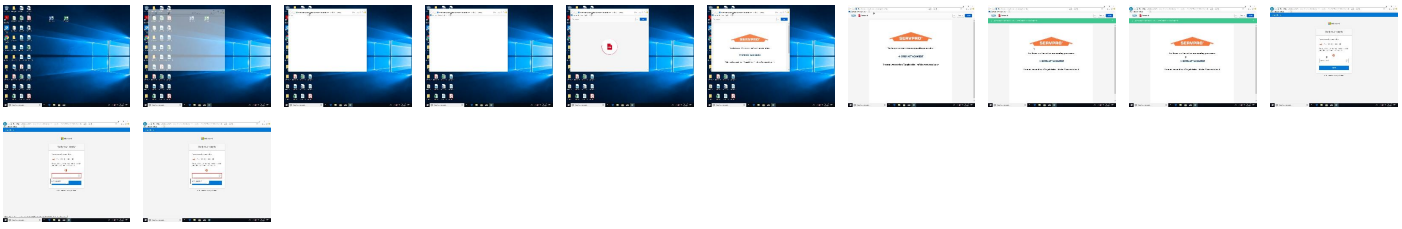
Behavior Graph

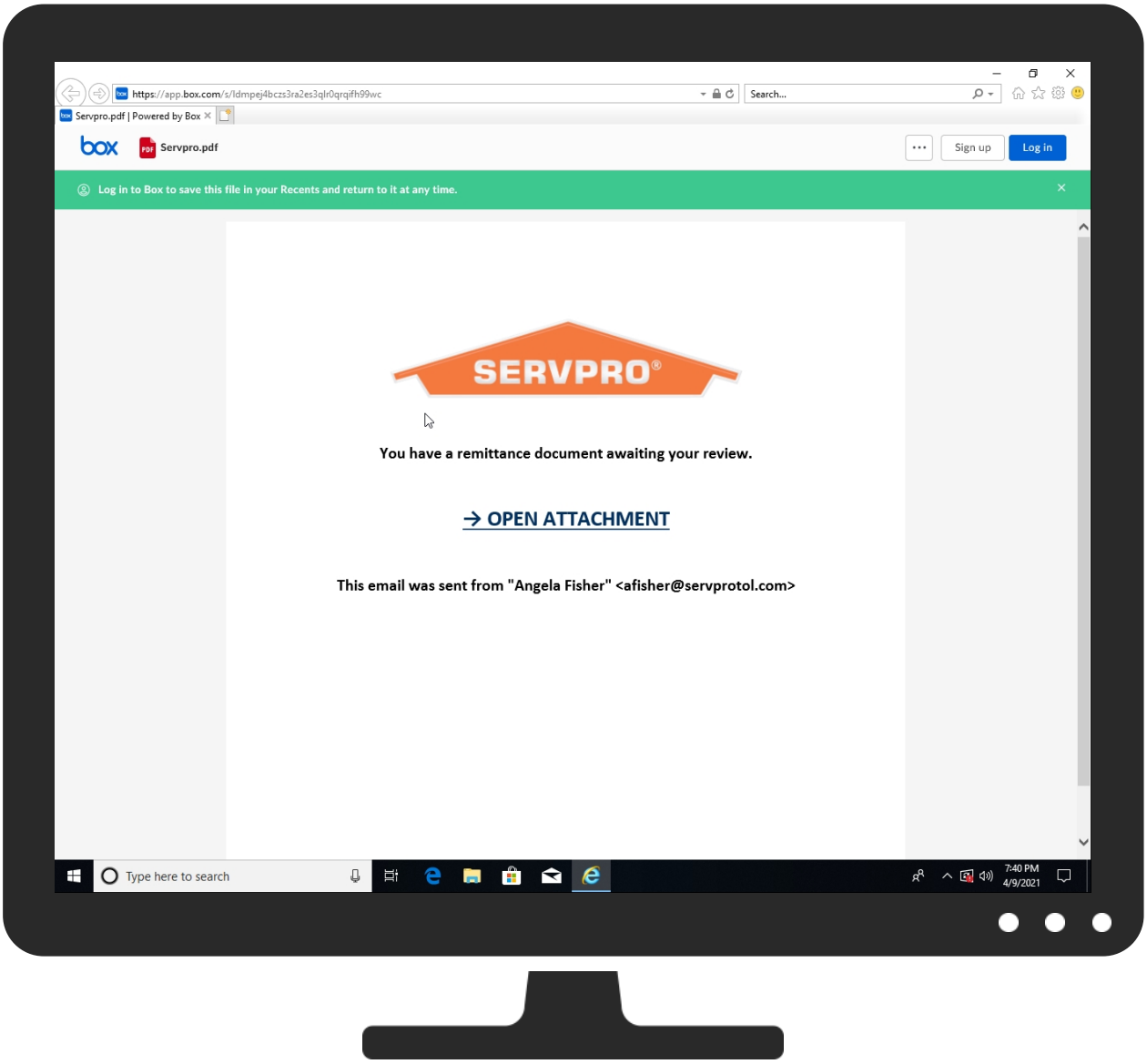


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://app.box.com/s/ldmpej4bczs3ra2es3qlr0qrqifh99wc	0%	Virustotal		Browse
http://https://app.box.com/s/ldmpej4bczs3ra2es3qlr0qrqifh99wc	0%	Avira URL Cloud	safe	
http://https://app.box.com/s/ldmpej4bczs3ra2es3qlr0qrqifh99wc	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
cdn01.boxcdn.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://erffggf.cf/jd/sharepoint-0/li6orbsabcm5o36s3wlba8p8.php?rand=13InboxLightaspxn.1774256418&fid&1252899642&fid.1&fav.1&email=	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://https://cdn01.boxcdn.net/_assets/img/favicons/notification-favicon-EHWWyP.ico	0%	URL Reputation	safe	
http://https://cdn01.boxcdn.net/_assets/img/favicons/notification-favicon-EHWWyP.ico	0%	URL Reputation	safe	
http://https://cdn01.boxcdn.net/_assets/img/favicons/notification-favicon-EHWWyP.ico	0%	URL Reputation	safe	
http://https://cdn01.boxcdn.net/_assets/img/favicons/notification-favicon-EHWWyP.ico	0%	URL Reputation	safe	
http://https://cdn01.boxcdn.net/fonts/1.0.2/lato/Lato-Regular.woff2)	0%	URL Reputation	safe	
http://https://cdn01.boxcdn.net/fonts/1.0.2/lato/Lato-Regular.woff2)	0%	URL Reputation	safe	
http://https://cdn01.boxcdn.net/fonts/1.0.2/lato/Lato-Regular.woff2)	0%	URL Reputation	safe	
http://https://cdn01.boxcdn.net/fonts/1.0.2/lato/Lato-Regular.woff2)	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/browserconfig-fdBReK.xml	0%	URL Reputation	safe	
http://https://cdn01.boxcdn.net/_assets/img/favicons/browserconfig-fdBReK.xml	0%	URL Reputation	safe	
http://https://app.box.csharepoint-0/li6orbsabcm5o36s3wlba8p8.php?rand=13InboxLightaspxnbox.com/s/ldmpej4bc	0%	Avira URL Cloud	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/_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%	URL Reputation	safe	
http://https://cdn01.boxcdn.net/fonts/1.0.2/lato/Lato-Bold.woff2)	0%	URL Reputation	safe	
http://https://cdn01.boxcdn.net/fonts/1.0.2/lato/Lato-Bold.woff2)	0%	URL Reputation	safe	
http://https://cdn01.boxcdn.net/fonts/1.0.2/lato/Lato-Bold.woff2)	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-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://cdn01.boxcdn.net/_assets/img/favicons/apple-touch-icon-76x76-ZVGnRV.png	0%	URL Reputation	safe	
http://https://cdn01.boxcdn.net/_assets/img/favicons/notification-favicon-16x16-Ou5N87.png	0%	URL Reputation	safe	
http://https://cdn01.boxcdn.net/_assets/img/favicons/notification-favicon-16x16-Ou5N87.png	0%	URL Reputation	safe	
http://https://cdn01.boxcdn.net/_assets/img/favicons/notification-favicon-16x16-Ou5N87.png	0%	URL Reputation	safe	
http://https://cdn01.boxcdn.net/_assets/img/favicons/notification-favicon-16x16-Ou5N87.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://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://jedwatson.github.io/classnames	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://erffggf.cf/jd/sharepoint-0/li6orbsabcm5o36s3wlba8p8.php?rand=13InboxLightaspxn	0%	Avira URL Cloud	safe	
http://https://cdn01.boxcdn.net/_assets/img/favicons/favicon-96x96-XU7UE1.png	0%	URL Reputation	safe	
http://https://cdn01.boxcdn.net/_assets/img/favicons/favicon-96x96-XU7UE1.png	0%	URL Reputation	safe	
http://https://cdn01.boxcdn.net/_assets/img/favicons/favicon-96x96-XU7UE1.png	0%	URL Reputation	safe	
http://https://erffggf.cf/jd/	0%	Avira URL Cloud	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%	URL Reputation	safe	
http://https://cdn01.boxcdn.net/_assets/img/favicons/favicon-16x16-_kQSW4.png	0%	URL Reputation	safe	
http://https://cdn01.boxcdn.net/_assets/img/favicons/favicon-16x16-_kQSW4.png	0%	URL Reputation	safe	
http://https://app.box.cRoot	0%	Avira URL Cloud	safe	
http://https://app.box.cbox.com/s/ldmpej4bczs3ra2es3qlr0qrqifh99wc	0%	Avira URL Cloud	safe	
http://https://cdn01.boxcdn.net/enduser/app.62d2420f86.css	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://cdn01.boxcdn.net/fonts/1.0.2/lato/Lato-Bold.woff)	0%	URL Reputation	safe	
http://https://cdn01.boxcdn.net/fonts/1.0.2/lato/Lato-Bold.woff)	0%	URL Reputation	safe	
http://https://cdn01.boxcdn.net/fonts/1.0.2/lato/Lato-Bold.woff)	0%	URL Reputation	safe	
http://https://cdn01.boxcdn.net/fonts/1.0.2/lato/Lato-woff.css	0%	URL Reputation	safe	
http://https://cdn01.boxcdn.net/fonts/1.0.2/lato/Lato-woff.css	0%	URL Reputation	safe	
http://https://cdn01.boxcdn.net/fonts/1.0.2/lato/Lato-woff.css	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/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://erffggf.cf/jd/ldmpej4bczs3ra2es3qlr0qrqifh99wc	0%	Avira URL Cloud	safe	
http://https://cdn01.boxcdn.net/_assets/img/favicons/notification-favicon-96x96-TOQ9Kg.png	0%	URL Reputation	safe	
http://https://cdn01.boxcdn.net/_assets/img/favicons/notification-favicon-96x96-TOQ9Kg.png	0%	URL Reputation	safe	
http://https://cdn01.boxcdn.net/_assets/img/favicons/notification-favicon-96x96-TOQ9Kg.png	0%	URL Reputation	safe	
http://https://erffggf.cf/jd/sharepoint-0/li6orbsabcm5o36s3wlba8p8.php?rand=13InboxLightaspxn.1774256418&fi	0%	Avira URL Cloud	safe	
http://https://cdn01.boxcdn.net/_assets/img/favicons/notification-favicon-32x32-brwW_W.png	0%	URL Reputation	safe	
http://https://cdn01.boxcdn.net/_assets/img/favicons/notification-favicon-32x32-brwW_W.png	0%	URL Reputation	safe	
http://https://cdn01.boxcdn.net/_assets/img/favicons/notification-favicon-32x32-brwW_W.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/_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%	URL Reputation	safe	
http://https://cdn01.boxcdn.net/fonts/1.0.2/lato/Lato-Regular.woff)	0%	URL Reputation	safe	
http://https://cdn01.boxcdn.net/fonts/1.0.2/lato/Lato-Regular.woff)	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/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://app.Root	0%	Avira URL Cloud	safe	
http://https://cdn01.boxcdn.net/_assets/img/favicons/favicon-yz-tj-.ico	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
api.box.com	185.235.236.197	true	false		high
public.boxcloud.com	185.235.236.200	true	false		high
app.box.com	185.235.236.201	true	false		high
erffggf.cf	198.54.125.84	true	false		unknown
cdn01.boxcdn.net	unknown	unknown	false	• 0%, Virustotal, Browse	unknown
955b0f04ec1842b79e6727b6d5210de0.svc.dynamics.com	unknown	unknown	false		high

Contacted URLs

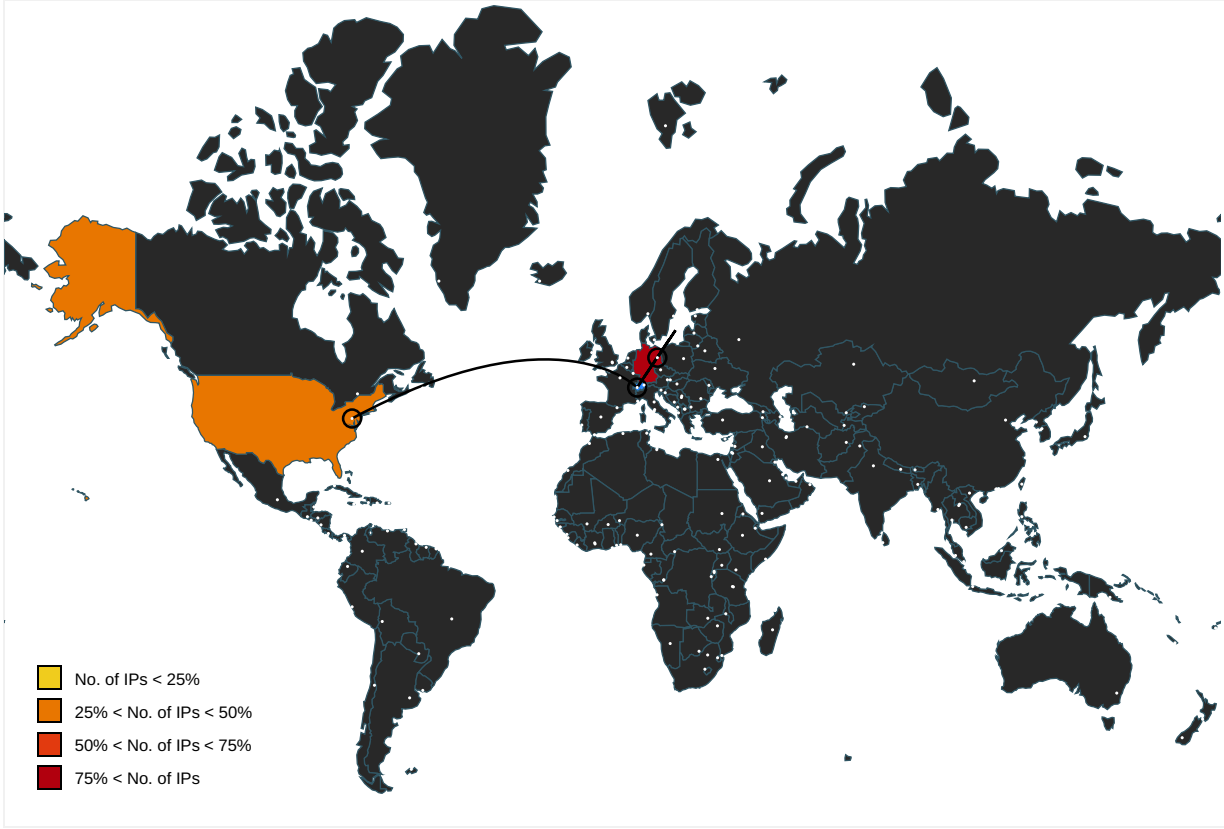
Name	Malicious	Antivirus Detection	Reputation
http://https://erffggf.cf/jd/sharepoint-0/li6orbsabcm5o36s3wlba8p8.php?rand=13InboxLightaspxn.1774256418&fid&1252899642&fid.1&fav.1&email=	true	• SlashNext: Fake Login Page type: Phishing & Social Engineering	unknown
http://https://app.box.com/s/ldmpej4bczs3ra2es3qlr0qrqifh99wc	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://cdn01.boxcdn.net/_assets/img/favicons/notification-favicon-EHWWyP.ico	ldmpej4bczs3ra2es3qlr0qrqifh99wc[1].htm.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://github.com/zloirock/core-js	core.min[1].js.4.dr	false		high
http://https://cdn01.boxcdn.net/fonts/1.0.2/lato/Lato-Regular.woff2)	messagecenter~preview-components~uploads-manager-enduser.de71b9769a[1].css.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://955b0f04ec1842b79e6727b6d5210de0.svc.dynamics.com/t/r/t1CFDnMTkqEtehk9U1_TVxBOL5s3sA69Juxjkt	Servpro[1].pdf.4.dr	false		high
http://https://cdn01.boxcdn.net/_assets/img/favicons/browserconfig-fdBReK.xml	ldmpej4bczs3ra2es3qlr0qrqifh99wc[1].htm.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://app.box.csharepoint-0/li6orbsabcm5o36s3wlba8p8.php?rand=13InboxLightaspxnbox.com/s/ldmpej4bc	{9EFB6EFB-995A-11EB-90EB-ECF4BBEA1588}.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdn01.boxcdn.net/_assets/img/favicons/apple-touch-icon-57x57-fLlEpj.png	ldmpej4bczs3ra2es3qlr0qrqifh99wc[1].htm.4.dr	false	• URL Reputation: safe • 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.de71b9769a[1].css.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://app.box.com/s/ldmpej4bczs3ra2es3qlr0qrqifh99wcRoot	{9EFB6EFB-995A-11EB-90EB-ECF4BBEA1588}.dat.2.dr	false		high
http://https://cdn01.boxcdn.net/_assets/img/favicons/apple-touch-icon-144x144-va9pYs.png	ldmpej4bczs3ra2es3qlr0qrqifh99wc[1].htm.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://cdn01.boxcdn.net/_assets/img/favicons/apple-touch-icon-76x76-ZVGnRV.png	ldmpej4bczs3ra2es3qlr0qrqifh99wc[1].htm.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://cdn01.boxcdn.net/_assets/img/favicons/notification-favicon-16x16-Ou5N87.png	ldmpej4bczs3ra2es3qlr0qrqifh99wc[1].htm.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://cdn01.boxcdn.net/_assets/img/favicons/android-chrome-192x192-96i97M.png	ldmpej4bczs3ra2es3qlr0qrqifh99wc[1].htm.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://jedwatson.github.io/classnames	preview[1].js.4.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdn01.boxcdn.net/_assets/img/favicons/safari-pinned-tab-jyt2W4.svg	ldmpej4bczs3ra2es3qlr0qrqifh99wc[1].htm.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://erffggf.cf/jd/sharepoint-0/li6orbsabcm5o36s3wlba8p8.php?rand=13InboxLightaspxn	{9EFB6EFB-995A-11EB-90EB-ECF4BBEA1588}.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdn01.boxcdn.net/_assets/img/favicons/favicon-96x96-XU7UE1.png	ldmpej4bczs3ra2es3qlr0qrqifh99wc[1].htm.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://erffggf.cf/jd/	{9EFB6EFB-995A-11EB-90EB-ECF4BBEA1588}.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdn01.boxcdn.net/_assets/img/favicons/apple-touch-icon-152x152-r5tWgh.png	ldmpej4bczs3ra2es3qlr0qrqifh99wc[1].htm.4.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	ldmpej4bczs3ra2es3qlr0qrqifh99wc[1].htm.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://cdn01.boxcdn.net/_assets/img/favicons/apple-touch-icon-72x72-7aVqne.png	ldmpej4bczs3ra2es3qlr0qrqifh99wc[1].htm.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://cdn01.boxcdn.net/_assets/img/favicons/favicon-16x16-_kQSW4.png	ldmpej4bczs3ra2es3qlr0qrqifh99wc[1].htm.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://app.box.cRoot	{9EFB6EFB-995A-11EB-90EB-ECF4BBEA1588}.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://app.box.cbox.com/s/ldmpej4bczs3ra2es3qlr0qrqifh99wc	{9EFB6EFB-995A-11EB-90EB-ECF4BBEA1588}.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://app.box.com/s/ldmpej4bczs3ra2es3qlr0qrqifh99wc	{9EFB6EFB-995A-11EB-90EB-ECF4BBEA1588}.dat.2.dr	false		high
http://https://cdn01.boxcdn.net/enduser/app.62d2420f86.css	ldmpej4bczs3ra2es3qlr0qrqifh99wc[1].htm.4.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://cdn01.boxcdn.net/fonts/1.0.2/lato/Lato-Bold.woff)	messagecenter~preview-components~uploads-manager-enduser.de71b9769a[1].css.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://app.box.com/s/ldmpej4bczs3ra2es3qlr0qrqifh99wc8Servpro.pdf	{9EFB6EFB-995A-11EB-90EB-ECF4BBEA1588}.dat.2.dr	false		high
http://blog.stevenlevithan.com/archives/parseuri	preview[1].js.4.dr	false		high
http://https://feross.org	preview[1].js.4.dr	false		high
http://https://github.com/derek-watson/jsUri	preview[1].js.4.dr	false		high
http://https://cdn01.boxcdn.net/fonts/1.0.2/lato/Lato-woff.css	ldmpej4bczs3ra2es3qlr0qrqifh99wc[1].htm.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://support.box.com	preview[1].js.4.dr	false		high
http://https://cdn01.boxcdn.net/_assets/img/favicons/apple-touch-icon-114x114-busq-D.png	ldmpej4bczs3ra2es3qlr0qrqifh99wc[1].htm.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://cdn01.boxcdn.net/_assets/img/favicons/manifest-rw1AEP.json	ldmpej4bczs3ra2es3qlr0qrqifh99wc[1].htm.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://erffggf.cf/jd/ldmpej4bczs3ra2es3qlr0qrqifh99wc	{9EFB6EFB-995A-11EB-90EB-ECF4BBEA1588}.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://rock.mit-license.org	core.min[1].js.4.dr	false		high
http://https://cdn01.boxcdn.net/_assets/img/favicons/notification-favicon-96x96-TOQ9Kg.png	ldmpej4bczs3ra2es3qlr0qrqifh99wc[1].htm.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://erffggf.cf/jd/sharepoint-0/li6orbsabcm5o36s3wlba8p8.php?rand=13InboxLightaspxn.1774256418&fi	{9EFB6EFB-995A-11EB-90EB-ECF4BBEA1588}.dat.2.dr, ~DF1D930BD22B0D5A83.TMP.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdn01.boxcdn.net/_assets/img/favicons/notification-favicon-32x32-brwW_W.png	ldmpej4bczs3ra2es3qlr0qrqifh99wc[1].htm.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://cdn01.boxcdn.net/_assets/img/favicons/apple-touch-icon-120x120-K-u4U5.png	ldmpej4bczs3ra2es3qlr0qrqifh99wc[1].htm.4.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.de71b9769a[1].css.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://cdn01.boxcdn.net/_assets/img/favicons/mstile-144x144-pllCM8.png	ldmpej4bczs3ra2es3qlr0qrqifh99wc[1].htm.4.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.4.dr, ldmpej4bczs3ra2es3qlr0qrqifh99wc[1].htm.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.box.com)	preview[1].css.4.dr	false	• Avira URL Cloud: safe	low
http://https://cdn01.boxcdn.net/_assets/img/favicons/apple-touch-icon-180x180-tV001c.png	ldmpej4bczs3ra2es3qlr0qrqifh99wc[1].htm.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://app.Root	{9EFB6EFB-995A-11EB-90EB-ECF4BBEA1588}.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdn01.boxcdn.net/_assets/img/favicons/favicon-yz-tj-.ico	ldmpej4bczs3ra2es3qlr0qrqifh99wc[1].htm.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.235.236.200	public.boxcloud.com	Germany		33011	BOXNETUS	false
185.235.236.197	api.box.com	Germany		33011	BOXNETUS	false
185.235.236.201	app.box.com	Germany		33011	BOXNETUS	false
198.54.125.84	erffggf.cf	United States		22612	NAMECHEAP-NETUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	384773
Start date:	09.04.2021
Start time:	19:39:24
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 26s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://app.box.com/s/ldmpej4bczs3ra2es3qlr0qrqifh99wc
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	15
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0

Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal72.phis.win@3/60@7/5
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browsing link: https://955b0f0 4ec1842b79e6727b6d5210de0.svc. dynamics.com/t/r/t1CFDnMTkqEte hk9U1_TVxBOL5s3sA69Juxjkt_Ucpk
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): 13.64.90.137, 40.88.32.150, 23.54.113.53, 168.61.161.212, 2.18.101.230, 104.16.74.20, 104.18.103.56, 104.43.193.48, 20.50.102.62, 52.169.10.20, 172.217.168.10, 23.10.249.26, 23.10.249.43, 152.199.19.161, 52.155.217.156, 20.54.26.129, 93.184.221.240 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, arc.msn.com, wu.azureedge.net, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcoleus15.cloudapp.net, e12564.dspb.akamaiedge.net, go.microsoft.com, audownload.windowsupdate.nsatc.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, arc.trafficmanager.net, mktsvcp102ne001.northeurope.cloudapp.azure.com, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, consumerrp-displaycatalog-aks2eap.md.mp.microsoft.com.akadns.net, wu.wpc.apr-52dd2.edgecastdns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, fonts.googleapis.com, ie9comview.vo.msecnd.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, wu.ec.azureedge.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, cdn01.boxcdn.net.cdn.cloudflare.net, displaycatalog-rp.md.mp.microsoft.com.akadns.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):	2491
Entropy (8bit):	5.0551920593800626
Encrypted:	false
SSDEEP:	48:wEabQzEabQzEabQzEabQzEasQzEasQOQzEasQnQzEasQnQ39IQzEasQnQzEasQ/T:mQ5Q5Q5QGQGQOQGQnQGQnQOQGQnQGQ/T
MD5:	58517F94C4DA332C486A46BE8ADDEE0B
SHA1:	E5A2F296EBB3C4A67C21C4242CE5AB2EB8FC5692
SHA-256:	295DC7E17902EE5AFF584636231D32758683ADADD32BE5BECB90EADD954FC0C5
SHA-512:	6745EE7A210F2F9E9A6F25C06C7046BAE1346578D958D5F3E8FB7A794000B486D25BF8859C834128236BA3225D4E318B9925F74260D459E4270FE9E082F37322
Malicious:	false
Reputation:	low
Preview:	<root></root><root></root><root></root><root></root><root></root><root></root><root><item name="localStore/0/bcu-uploads-reachability-cached-results" value="{}" ltime="1688239616" htime="30879079" /></root><root><item name="localStore/0/bcu-uploads-reachability-cached-results" value="{}" ltime="1688239616" htime="30879079" /></root><root><item name="localStore/0/bcu-uploads-reachability-cached-results" value="{}" ltime="1688239616" htime="30879079" /></root><root><item name="localStore/0/bcu-uploads-reachability-cached-results" value="{}" ltime="1688239616" htime="30879079" /></root><root><item name="localStore/0/bcu-uploads-reachability-cached-results" value="{}" ltime="1702589616" htime="30879079" /></root><root><item name="localStore/0/bcu-uploads-reachability-cached-results" value="{}" ltime="1702589616" htime="30879079" /><item name="bp-doc-current-page-map" value="{"797531939634":1}" ltime="1720869616" htime="30879079" /></root><root><item name="localStore/0/bcu-uploads

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{9EFB6EF9-995A-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8502987239159152
Encrypted:	false
SSDEEP:	192:rhZOZJ23WgtSlifycnJzMWBBYbD9sfTn0jX:rnaYGkS1yJUaQ8
MD5:	EA674F05C43B1C85E9A90DA8FD7E04C6
SHA1:	43831F441E8576C80C756AAE6660599EB4BEF401
SHA-256:	52443DCF8C58F53A3327EEA477A4FE75774535B6F6C993ABD68D00A7310A6265
SHA-512:	7F12E1853A9B388574C8242E3D63D01096C2C85908439AF2D5F5DFF5F8C3F99086C22D0C6AC636727E9C13D804FC204EB9428104C34B0E7080B38A3EFEF303EC
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{9EFB6EF9-995A-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\{9EFB6EFB-995A-11EB-90EB-ECF4BBEA1588}.dat

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	44768
Entropy (8bit):	2.222754948483136
Encrypted:	false
SSDEEP:	384:rnlNrGyY48wIXG1V1qjhAOt4AtdLxA0Bxdr1uZv1kvukvkkv1kv9o:dLEv7rwxCr9m2
MD5:	0FBCA5878EF2BD3F750B59C5FCBE0921
SHA1:	8F1877A29DA2B14027900BE7793416FB78FB424A
SHA-256:	2095CD2C96C173428440A9291F0D22D9CC808CA7F26454073500B62ED130F0D0
SHA-512:	35BC600682087FCB8EBC956F9D327628CDD21AC930FCEC5BA92387A0CD990BD743E4C305327277182C97CD45DAF49F96E138E3150583BF98FB41F6F8B67F7D5
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\{A571EC6F-995A-11EB-90EB-ECF4BBEA1588}.dat

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5649234730916166
Encrypted:	false
SSDEEP:	48:IwDGcpreGwpaZG4pQNGrapbSSGQpKEG7HpRKTGIpG:r5ZWQ76tBS6APTuA
MD5:	5221ED91E9CA58A080AA08486690CCEB
SHA1:	1897B8FB0C3EAA155E60A6C2F2FBF32DC8F3274B
SHA-256:	4B5AA2CD56129F4103DFD624DD071D3069385908A2BD3BF9D7D9350EC73A91DC
SHA-512:	E5AF402746A8AB184940623BB292926058575DB5CFB23A43EB1AFE6C366019FFB55F8A39A1F862E738AE913456F641DE3840D7E540DF1FE68D32C047DCB6C0BE
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:	dropped
Size (bytes):	1335
Entropy (8bit):	7.151718376015463
Encrypted:	false
SSDEEP:	24:1zaF2Cn2MkjvNSTHDyCbibxDx4fZ9qMfhkbOTKB6:1mF2C2djvA3bc9ENhkbA
MD5:	30F92B7A5163DC9B2852AB530841C198
SHA1:	7A38B89AE253A4185642829F4F89A9D459F08F7F
SHA-256:	5A421F6416B5A80BF8735345882897DB539A96F04FC78188DCB058E6797A47B4
SHA-512:	BC9E163F3201A71BB2FB72A24B1C7F57B0DBA0512450EDB44BBEED5EB94FA83286AEB980271C24F914C7EEE7A2BB6EDB272003A55BC6AE5BF90C46F660D1B3CA
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..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\Lato-Bold[1].woff

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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\2WF3MMUU\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\2WF3MMUU\Lato-woff[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	271824
Entropy (8bit):	6.004035154725513
Encrypted:	false
SSDEEP:	6144:7iSn14Pe5e8PMyBdu/gFU7Eu2bzHB1v1e/OHjl0Cl:eS18e5eqMy7RbT/v1QODl0Cl
MD5:	E1E5023A4D0B29824C8A6937ED303B03
SHA1:	93159BA90E4ACA126C45282D047E4E1D544AD100
SHA-256:	80745E4A131F2F16302232F53845BFA223915A3465369A40A9AA777D2C0A30BD
SHA-512:	09A87AA0383D5E78FAF21CD63E4EE6EB875AC39F52AAF0805224DDFE39B56E91ECEEA743B811C2C8473A0113BDA678C472EAD4FECA207004A37699D051EA68B6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn01.boxcdn.net/fonts/1.0.2/lato/Lato-woff.css
Preview:	@font-face {. font-family: 'Lato';. /* This is Base64 encoded from Lato-Regular.woff */. src: url('data:application/x-font-woff;charset=utf-8;base64,d09GRgABAAAA AdFcABMAAAADhOgAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABGRlRNAAABqAAAABwAAAAccNlcTUdERUYAAAHEAAAANwAAADgSeA2uR1BPUwAAAf wAANZ6AAGuYg7b1pNHU1VCAADYeAAAAywAAAtGQYaNc09TLzIAANukAAAAXwAAAGBp8+XGY21hcAAA3AQAAATZAAAGoHgSIT5jdnQgAADg4AAAAHIAAADqPz mz1GZwZ20AAOFUAAAFqAAAC5fkFNvwZ2FzcAAA5vwAAAAIAAAACAAAABBnbHlmAADnBAAAwI4AAWHYuL0/gWhlYWQAAaeUAAAAMQAAADYO+nFm aGhlYQABp8gAAAAhAAAAJBEGCeFobXR4AAGn7AAACQ4AABIS60ObMmxvY2EAAbD8AAAI5AAACR6IDi0mbWF4cAABueAAAAAgAAAAIAZMAeluYW1IAAG6AAAA BQQAAA/ywsuuaHBvc3QAAb8EAAARqgAAJ+ABEAopcHJlcAAB0LAAAACiAAAAuW8KaTp3ZWJmAAHRVAAAAAYAAAAGYIZWjQAAAAEAAAAAzD2izwAAAADR6Kh5 AAAAANKzEQR42mNgZGBg4ANiAwYQYGJgZWBkagLiZqY2BmamdhZvBkYWHxZfBiYWP5ZeBkYGFrAqBgBp7gRDAHjapL0JfE3X+v+/9t4h8zwPZkVJEVVTU1xU Y1ZVVFTVRbVVVXXbolJVVVdDTTVXFVU1z5XEHMFBcCKVSCJizEkaJyGhqmr932ed0+a06t77/f1vX5/9WWedtdd69nrW86zPSnZcoQkhPMQg8YFw6dS5e18R 8c/xY0eJBq

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\Servpro[1].pdf	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PDF document, version 1.5
Category:	downloaded
Size (bytes):	384539
Entropy (8bit):	**7.991014286950824**
Encrypted:	**true**
SSDEEP:	6144:LcrqvRhuj05lCtIDUV+QZUd52mXQDRd6n+nad1g9r0YVjarE6ssEWUsEigxBh:LcrihujrCiIhUfQNd6+ad1k4eurzsPrH
MD5:	3670EB343ABF0EC0350A8150ABBC48AF
SHA1:	7DDB6C11DDF5753C8CCC4684ABAD11918F0C622B
SHA-256:	8223A0C225CF74A1D1D539A973683AE2652F3FE1911B023BB466A297DF8A33F6
SHA-512:	020350F126FF3C86D382E765627F272D27AF4D71A4B172123A65A0C8F207F514FB8F22C8153072B53B97B3D093D2C48D4E1BA39B1D936E49AE1A4C98EF49E721
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://public.boxcloud.com/api/2.0/files/797531939634/content?preview=true&version=852889767234&access_token=1!njIT8VPswMD6-FhGnf5Sg6ngjcePllMVMXIPJUNrryKT4ZNkRGP1ZYvo8zmSD2Wb9HLZWwAnxH6oWoNy4ykuINGq8tdQ8lOJN9YhCnvMR8Ci-uYg1gNBsgGJ6rqR3YdeF8m4oqN0wctIFTh1wA5nK8fsGju46kXVYFyNKDOM-uvN2gAvgMs3vPB9mM4kRDJqz-CXYWV0svEJgVfdIuB3wjwPXAa7xDTqhiMqVdm7NL6fUDWZbG3KI_A4Vzpprmpq8b2X9vItlOix0nlw585BgrVaJcwuJCBnAYyfuHAugr7JvyI3fp9_KixGam8CoqpCuqdKTxhio7q3E5ufZDQbdWcF4TZ582duJtOcxKee86bFkx1yg-mdvG64ZNNIoVbhXmnvf1iifI2Xi1_TeT6ebsj9FJGMuu7G9ZvRupcvH-IUh-ktpgL6A9WP5I5FF4ZcGm_aftk5Uufzv7cOAlz2U3bBGuTAtoSgniy1WjeDb5tKGEnncq_CpUtXf4EaxdXXmKLI6-J3xHAAvb6baEziMEUBVn8WSKIsAbx66mkjxeLodF0ywL5DWbKVhY4Elc.&shared_link=https%3A%2F%2Fapp.box.com%2Fs%2Fldmpej4bczs3ra2es3qlr0qrqifh99wc&box_client_name=box-content-preview&box_client_version=2.69.0&encoding=gzip
Preview:	%PDF-1.5..%.....1 0 obj..<</Type/Catalog/Pages 2 0 R/Lang(en-US) /StructTreeRoot 20 0 R/MarkInfo<</Marked true>>>>..endobj..2 0 obj..<</Type/Pages/Count 1/Kids[3 0 R] >>..endobj..3 0 obj..<</Type/Page/Parent 2 0 R/Resources<</Font<</F1 5 0 R/F2 9 0 R/F3 12 0 R>>/ExtGState<</GS7 7 0 R/GS8 8 0 R>>/XObject<</Image17 17 0 R>>/ProcSet[/PDF/Text/ImageB/ImageC/ImageI] >>/Annots[11 0 R] /MediaBox[0 0 504 504] /Contents 4 0 R/Group<</Type/Group/S/Transparency/CS/DeviceRGB>>/Tabs/S/StructParents 0>>..endobj..4 0 obj..<</Filter/FlateDecode/Length 648>>..stream..x..Umk.A..~p.a.'/p.....IH!.&B).....I...x.c....{.;;/...=....h.Z.m.e..v.~.....Hp.....)L..I.....;.4!=..L...`.....n......"M.. ...Oir.....]..60.#`.N....$.cb(.D..D..cm.W....Q..U.o.,....n.\.Y.j.Y.k...%..."I.t|..E.x...{}..OZN{Ynj.....Y.....r..G..eM.9u..a.....bY....L9...J.6.V..\!.5.....).....n.5.{ ....._.gpB..!.P.@W!Z.B.....n.5AmH.B....0R.f.q."%qV..ut\..-s...4J-7dJ..'.bMk.....~5../.UU.+...4'-=.mpUI....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\app.62d2420f86[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):	162399
Entropy (8bit):	5.027453265537666
Encrypted:	false
SSDEEP:	3072:4dyg6zSqfO6QAQlkkBh39AiDQyUyoTwTrhmvECUYOSs/Mn:4dyg6zSqfO6QAQlkkBh39AiDQyUyoTwE
MD5:	46301A03C019930B0FDEACFB8578A805
SHA1:	ED904D489426AE81C9C67261F21739788531C50C
SHA-256:	3BB86F3AEFA77288466913EB064D4A9639A2086654F825F2C6E54CA5525134DE
SHA-512:	2C0D498BBCF77AF6CBF3AE2871C5FADEB1BACEE631FC41A9911769054680AF04E457A887981C5A7859AA8FDEAD62E62E848A6D24E6F314D12ACA36BAD73EDA99
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn01.boxcdn.net/enduser/app.62d2420f86.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\ldmpej4bczs3ra2es3qlr0qrqifh99wc[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):	9361
Entropy (8bit):	5.2831813407785635
Encrypted:	false
SSDEEP:	192:G8AkAYOA7lkZkrjyBuDoPql3+z6GUBfo1eM7c32ULjDQlcDBN7yOeihW:G8AkAVApkZkrjyBuDoP+3+z6GUH39Lj2
MD5:	EA1C7286FFABC4AA0102EE557ACFD5F4
SHA1:	9F60D315F427C66D4AE13D4C61E1DAEEB7D419B8
SHA-256:	DDC5E68004CA989F977EA29FA05EC07E639A05E0F806CF0AF3283EEE5F095B0C
SHA-512:	079C3B477B7E5A814CC8E82904AFE08D02B578D367D3916D6B2A4FDECD7EB5D4473CCDA883B5B59F5E824F2D2D4A8E1767B5C2BFB466D06FF4FD05C9A8099F27
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\ldmpej4bczs3ra2es3qlr0qrqifh99wc[1].htm	
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.62d2420f86.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\2WF3MMUU\logo_strip[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 624 x 96, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	7541
Entropy (8bit):	7.91795414069011
Encrypted:	false
SSDEEP:	192:XoONgOLPXsAYnpSFGhkzR7VzyxU5zkjxRx:YOWOLv5qQFekBVzN5zkjxRx
MD5:	1228BD64AD39DAFE43AC5B6A865B639B
SHA1:	209C7B6DDF2A470E28541FD920F6CF3F3634A11B
SHA-256:	D1F126B54D456B3D15BE32E56FA230CB8A9D4B5B3CFA8E0E2B0386431C869FBA
SHA-512:	E2031C81D3DE640282A054FAF49B324822CBBD102BB640BF359BD8C82CC4E8BCEC4F9F43B9588503C607083C236AF840EDCDC690DCBB62554B3A3358A39839C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://erffggf.cf/jd/sharepoint-0/img/logo_strip.png
Preview:	.PNG.....IHDR...p...`.....ZO.....gAMA....|.Q.... cHRM.....R...@..}y.....<.....s<.w...9iCCPPhotoshop ICC profile..H..wTT....wz..0.R.....{.^Ea..`(..34.!...ED."HP..P$VD...T..$.(1.ET,oF.....o.....Z..../...K.....<....Qt.....`.).LVF._.{.....!r._...zX..p..3.N....Y.|.....9.,...8%K.....,f.%f.(A..9a..>.,....<...9..S.b...L!G....3..,....F.0.+.7..T.3...Il.pX."6.1...."....H._q.W,.d..rIK..s...t.....A..d.p....&+..g.].R.....Y2...EE.4...4432..P.u.oJ..Ez...g.....`.j..-....-....b.8....o....M</..A...qVV....2.....O.....g$>...]9.La.....+-%M.g.3Y.....u..A.x....E.....K.....i<:. .....Pc...u*@~..(.. ...]..o..0 ~y.*..s..7.g...%...9.%(....3.....H.*...@...C`...-p.n.....V..H.....@....A1....jP..A3h..A'8..K....n..`.L.g`.....a!2D..!.H... .d..A.P....B....By.f..*...z.... :....@..]h...~....L.....C.Up.....p%....;...5.6<.?....."....G..x...G.....iE..>.&2.. oQ...EG..lQ..P.....U..F.Fu.zQ7Qc.Y.G4....G.....t...].nB../.o.'.1.....xb"1I.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\messagecenter~preview-components~uploads-manager-enduser.46e89c9bf1[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	258386
Entropy (8bit):	5.329767821017335
Encrypted:	false
SSDEEP:	3072:fF3Jh2zsrmYnGvB8H2RDyUlBgxPvVdwfPOWQ3w2RO993rzRVTwCQ7wTiJGU05JPl:fFij1i4oBXw48q2
MD5:	94CCEEBDAF9136761D3D1854870FD329
SHA1:	C499201C7AA531E597622C05280BD07A6BCC321F
SHA-256:	C3852D620222BF6E3C556AC62FAEFB957CD406654345E15480F0B860095D4B3F
SHA-512:	D6108E2ED31C08E6F932FBE89A81E6091BB2ABDF91770C0D1BDEB0618E03AC43618DDB08CCE6263306BC3D93537B2958E8A1F4715E250F2C764E839B3AA22DB
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn01.boxcdn.net/enduser/messagecenter~preview-components~uploads-manager-enduser.46e89c9bf1.js
Preview:	/*! For license information please see messagecenter~preview-components~uploads-manager-enduser.46e89c9bf1.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\2WF3MMUU\messagecenter~preview-components~uploads-manager-enduser.de71b9769a[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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\messagecenter~preview-components~uploads-manager-enduser.de71b9769a[1].css	
SHA-512:	EE40B6383A6394FB528C77C90366412A8BC2BF3FD6AE688FDA33521185680EDFA2232C3EFBC4074DC555976A5DADACC44C6B411A0AFF767B5C67CBAD6E5B0B8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn01.boxcdn.net/enduser/messagecenter~preview-components~uploads-manager-enduser.de71b9769a.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\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[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	6830
Entropy (8bit):	7.849424154989951
Encrypted:	false
SSDEEP:	192:n6ND9AxRGozwHD0Ksf+GQUAU6Z0WoYGoKUcsgYRU:6xWRXwHmtfYGLUYIU
MD5:	F1E3F187F7C23FA8D1555004F3800356
SHA1:	E71E52A142E754399AE39EF38584789B66E9EA00
SHA-256:	DB307FCEF7F95139689007D7A623B340EC21282BD421C4E4B2BA09078F230545
SHA-512:	BD568B1C92D7C3B586E2EA7E9C47B08FD1171FF6615FA4F670F12950DC62315B58E6BB5336F50B111FF42B27558398DFF9715054A8E44F0A8B9CD1541F0BC07D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://erffggf.cf/jd/sharepoint-0/img/pdf.png
Preview:	.PNG.....IHDR.....\r.f... cHRM..z&.....u0...`..:....p..Q<....bKGD.....7IDATx..K....j.[....{..&....V6....np3...-.. $.qF..0.a....a6y.....&D.g.#.....;..aC..q.5.k....n..SU.T...Oj.[..w.....:.....Nz....P.0.,.....b`..X.....`10.,.....b`..X.....U.@...?...Dfs..S....".....y.I.'q.s...^.9.....u.~qnn.....p.....?\u..Pz..&.>.E....)O....zzz.?..k.q#...;0..`Y...jaA.....S.\HF...#"...".dY:.O./..@.C).....f.I...<..;o.9..0... ..B.....I..&`.4...|..1..9z...o.E...P..h...R..P.q...l....1....8....$..v.....q.q.j6.4555Vw.g..=:TJ.....v\.6.%.).H(...._'..._.>.f...s].&.....j.U]..?2..-..rs....U.....7T0._.p..<.....*.4.".|S...C....L@=...Q..(,.^.S...`?@...f...1x.....w.6.~....F.....7....{.\....z..B.....d..;.....F.&.... 3\.T.....q..Fcq...9|.&....A.....<.....{..L 3,. ..1a...!(.`- .F.ASK&px..<p...D...d....*W~g].....h.j.0.Y.....d...4dK. .F...`.Y`j..\.7SQ{_.f.AS.....\....S..

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\pdf_viewer.min[1].css	
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\uploads-manager-enduser.1447e4d8b7[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:	6557DF16669DDFB8E5BF239CC8004991B1483568090013310857002CD051B85A
SHA-512:	7F175FB31672C46A14A8C666E835D85D8CD06C7AD41B07B833DB8FD56C8F6C7AFB02B47979C5E007E6BE189FC7C411D85C2C66E4911369F901CF4CF73850A2F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn01.boxcdn.net/enduser/uploads-manager-enduser.1447e4d8b7.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\9026IKNJ\app.80bc6631ed[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):	1384975
Entropy (8bit):	5.449069874721862
Encrypted:	false
SSDEEP:	24576:fuz1l/VdN/+YY++XPGPAtOt8Xew7FNCgomfFJVU1SqTu4XLMKzQ68WoHJ9:f61l/VdN/+YY++fGPAtOt8Xew7FNCgoc
MD5:	BE30D5FD0FD48603B5A75F17740C2F23
SHA1:	81C251A61C7C8F1C297B6481AE7FAFA754D89068
SHA-256:	28A27EA2F23226CBA224A1C6F059C98FBB9DC7020ECD5A7C3CE5268A00C0C026
SHA-512:	C0A38DEE9375E3051CF82FF0B8B0C65EFA49814F761886DDF6A1A429D3A5BA623CF4372742214008B08DA895DDB5AD16056F94C281159C41FFD4E367852336CI
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn01.boxcdn.net/enduser/app.80bc6631ed.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\9026IKNJ\content-sidebar.aadc94c993[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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\content-sidebar.aadc94c993[1].css	
SHA-512:	C746CF7D3F795CEFAB5EBA4CAC86633563D9C8FF78BE867EB52721D8B55AC927662C5DB71EE80A82D3CB2DE0710329261BEBF1871BFC8EFFA82F462AC8DE5AC3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn01.boxcdn.net/enduser/content-sidebar.aadc94c993.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\9026IKNJ\css[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	188
Entropy (8bit):	5.119072399147113
Encrypted:	false
SSDEEP:	3:0SYWFFWIIYCiF15RI5XwDKLRIHDfFTo/TfqzrZqcdJ2dTi8EuRlGlL+9JYARNin:0IFFm15+56ZTo/Tizlpd0celdJNin
MD5:	4CFC4658F748E1FC67D2EA27F9B3692F
SHA1:	82C520D112F48E337E99DF00067BFAA75D0F9CA2
SHA-256:	ABC5A61E85F95E54C925FE9589099AD680912480E7C97052AF0496CBC6D111B8
SHA-512:	BFDDD6D4E0225EF444FD621B2CC20D022C02E30AB3E8AACA197E8F6304AA95E8C253815C6DC329646E5F39BBAF0B953A0667B296D15AB6BCECE788D1BFDC614B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.googleapis.com/css?family=Open+Sans:600
Preview:	@font-face {. font-family: 'Open Sans';. font-style: normal;. font-weight: 600;. src: url(https://fonts.gstatic.com/s/opensans/v18/mem5YaGs126MiZpBA-UNirkOUuhv.woff) format('woff');.}.

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\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\lang-en-AU~lang-en-CA~lang-en-GB~lang-en-US~lang-en-x-pseudo.57dba5f597[1].js	
SHA-512:	B352761E7A479C34F53E6694208EF5CA92DA2F43E3199305B3E383B4C42A1FFF3B6AA5084E9233879E17F7BD85FD329CA46642F1BBB0DEDB750E83BDBDC83B27
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn01.boxcdn.net/enduser/lang-en-AU~lang-en-CA~lang-en-GB~lang-en-US~lang-en-x-pseudo.57dba5f597.js
Preview:	(window.webpackJsonp=window.webpackJsonp||[]).push([["lang-en-AU~lang-en-CA~lang-en-GB~lang-en-US~lang-en-x-pseudo"],{PTt16PTTsL:function(e,a,t){e.exports=function(){"use strict";return[{locale:"en",pluralRuleFunction:function(e,a){var t=String(e).split("."),o=!t[1],n=Number(t[0])==e,r=n&&t[0].slice(-1),i=n&&t[0].slice(-2);return a?1==r&&11!=i?"one":2==r&&12!=i?"two":3==r&&13!=i?"few":"other":1==e&&o?"one":"other"},fields:{year:{displayName:"year",relative:{0:"this year",1:"next year","-1":"last year"},relativeTime:{future:{one:"in {0} year",other:"in {0} years"},past:{one:"{0} year ago",other:"{0} years ago"}}},"year-short":{displayName:"yr.",relative:{0:"this yr.",1:"next yr.","-1":"last yr."},relativeTime:{future:{one:"in {0} yr.",other:"in {0} yr."},past:{one:"{0} yr. ago",other:"{0} yr. ago"}}},month:{displayName:"month",relative:{0:"this month",1:"next month","-1":"last month"},relativeTime:{future:{one:"in {0} month",other:"in {0} months"},past:{one:"{0} month ago",other:"{0} mo

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\lang-en-US.d8cbc90473[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):	526173
Entropy (8bit):	4.863962199926709
Encrypted:	false
SSDEEP:	12288:tyV20XTeM8sKge2YSYgoST7bF4TjdFjsjejQjeASf6uSAM:tyV20XTeMcASCuSAM
MD5:	77D050B5D2362E2848A3BC61551844BE
SHA1:	D43F29BB8638CF123B165DFD34F06C996D016792
SHA-256:	34B2E3E12C2A49D52E9046590FB28AD68CF78903810698B179565A6E1857C6B5
SHA-512:	99D5EB1026A38020F42F6107FAC2F164166F0260A957BBA49AB654C14AD3F1CA53C6E5CFC34575B9D3FBF547D4A64C2E3B8B181E2472B8F3D9382BBC419B95BA
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn01.boxcdn.net/enduser/lang-en-US.d8cbc90473.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.default}));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(O

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\messagecenter~uploads-manager-enduser.e83b2dda31[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	46540
Entropy (8bit):	5.2638289199792485
Encrypted:	false
SSDEEP:	768:vj13k4lZZZsGcXaKxdk2S/4N2S/J67EKB3ipef8QScD8gtEwQThwdOwaleOFDX2g:4xdk2S/4N2S/J67EKB3ipef8QScD8g1o
MD5:	0301C1A9C6BFCA3D5F81EF8A64E77C2E
SHA1:	3CD3BB4391C82A29191B5B0C9ABB4EE01AFCE8DA
SHA-256:	218F4E999ED4F2B19EEAC806BC5D64C8E71F63E7D3336A6FAECE22FB784214FD
SHA-512:	E15B0AB4A5E0A254726DD07335E525FFCA73573AB19177E4446CF5041681C9B097FCC12FAF653C8C6360270CABAFB15514310CDE5DA50D7D84ABE1EC32FBC9B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn01.boxcdn.net/enduser/messagecenter~uploads-manager-enduser.e83b2dda31.js
Preview:	(window.webpackJsonp=window.webpackJsonp||[]).push([["messagecenter~uploads-manager-enduser"],{"7G9T0A7Q2t":function(e,t,o){"use strict";var n=o("QbLZJtXF68"),r=o.n(n),i=o("Yz+Y0CAZeS"),l=o.n(i),a=o("iCc5sPGOWs"),s=o.n(a),c=o("V7oCdLSCTo"),d=o.n(c),u=o("FYw3c9QbSe"),h=o.n(u),f=o("mRg0wtBNeT"),S=o.n(f),p=o("q1tIBJhxTW"),m=o("m0AvLASv6a"),_=(o("17x9q+7QrQ"),function(e){function t(){var e,o,n,r;s()(this,t);for(var i=arguments.length,a=Array(i),c=0;c<i;c++)a[c]=arguments[c];return o=n=h()(this,(e=t.__proto__||l()(t)).call.apply(e,[this].concat(a))),n.state={height:n.props.defaultHeight||0,width:n.props.defaultWidth||0},n._onResize=function(){var e=n.props,t=e.disableHeight,o=e.disableWidth,r=e.onResize;if(n._parentNode){var i=n._parentNode.offsetHeight||0,l=n._parentNode.offsetWidth||0,a=window.getComputedStyle(n._parentNode)||{},s=parseInt(a.paddingLeft,10)||0,c=parseInt(a.paddingRight,10)||0,d=parseInt(a.paddingTop,10)||0,u=parseInt(a.paddingBottom,10)||0,h=i-d-u,f=l-s-c;(!t&&n.state.hei

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\pdf.min[1].js	
MD5:	9A9AC5F2FB76274116C651226A647C95
SHA1:	EEDC500FC742C9762BF5789AE470132B2011AF77
SHA-256:	6CF4C965636CFA49500C3A95FDEF2C5F4722FD0367ED26D70A19F1A13DFFE173
SHA-512:	13132DAB411AEB5C8204171B3B350FE9B372B3ABA057F6BC3EABCE2BB5218212DDDA1A2020D9B00A986162AE5D85B88F7B3E1AAA4E7F8F7C4F63329DE48C760A
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].exports;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,{enumerable:!0,get:h})};d.r=function(a){"undefined"!==typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(a,Symbol.toStringTag,{value:"Module"});Object.defineProperty(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);Object.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\9026IKNJ\preview-components.87c76e14ef[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):	358758
Entropy (8bit):	5.495486644351831
Encrypted:	false
SSDEEP:	6144:WK2Y53gGJc95uGZWvfEVXHsz+DuWgO+QploG9/h:WD6K95qinaLjG9/h
MD5:	7614A77F883CDFF0070B898F1A18AF98
SHA1:	811875B8F262DDE141CFA1EB6BCBD6BC1295859E
SHA-256:	2BDEF9AB99EBED98E563844EE73BA09F3AF62CE4A3BE4FCEE266BBB89FF9BB9A
SHA-512:	EE8825B38698BAED45A65CB3EDE206DBA2102EE7C979C5D6EFD9E1BA37FE9CD0503B62C741E92C9CCA5888C1EF25217C930B8A0079933F95142EC6CA5774E92A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn01.boxcdn.net/enduser/preview-components.87c76e14ef.js
Preview:	(window.webpackJsonp=window.webpackJsonp||[]).push([["preview-components"],{"+2fdFMMSXi":function(e,t,n){},"+BZej3U4u/":function(e,t,n){"use strict";var r=n("q1tIBJhxTW"),o=n("vN+2lcUykn"),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.getOwnProper

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\uploads-manager-enduser.701384c70f[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	96957
Entropy (8bit):	5.32212061163114
Encrypted:	false
SSDEEP:	1536:X8gXSb0h7Ch+uPAQgNWCOn3gEbENuSEzz7foXBf6A:rh7C1YQgNWCAQEINuSK7AXBf6A
MD5:	96723514F5280594E9AC585346EBF3A7
SHA1:	A07B97A4267B275E79378DA9FA85B0A130A98557
SHA-256:	5CB650781C37BE4DDB5710E4FE0B4F2708351FBD501D338BACC0C5E1BF33E39D
SHA-512:	E84E7CA03B88786C7293CA39CB36BA3F0E0E7D0DC94F8ED5978956431145A7E087451C21AC162F59AF9D7C8F1750C67FE806D15F130DAA747EAE52BA7301159
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn01.boxcdn.net/enduser/uploads-manager-enduser.701384c70f.js
Preview:	/*! For license information please see uploads-manager-enduser.701384c70f.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\CS6IXJW6\content-sidebar.d5bb78ae93[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):	49888
Entropy (8bit):	5.388970931395125

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\content-sidebar.d5bb78ae93[1].js	
Encrypted:	false
SSDEEP:	768:fsoVCjHEsHlmdndYfBf/37FDvuMtvvzeKQ2rsr5HusUGp:aFJ/37FzumvwlHl
MD5:	90DCA29899AC24B518E6FA6F10DE24D8
SHA1:	40E82DF85CEBFF3B930374C4CB44D77A02BAC200
SHA-256:	911B496D51030A2FFCDDACFBCA99A15AF5FC38B0F9040AA0A465A1FE20882931
SHA-512:	3338B63E4AEE5D04FC7E249C9F350AA69F958CFCC11315E582D60945DA7023AC5ECC3C3E4C588E6BE80A0E981AFB1417D77B4BD21C877BCE56A1E82CF03F5D33
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn01.boxcdn.net/enduser/content-sidebar.d5bb78ae93.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+2lcUykn"),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:	E650576C845A326539EA79A87E8D5421B19349E5F5F7FB3F6BA8AE7F0F1A4F909BE87C9AD94022C043F5109B4A85C6DEA54ECEE8075786CCFE2F761696A965D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn01.boxcdn.net/polyfills/core-js/2.5.3/core.min.js
Preview:	/**. * core-js 2.5.3. * https://github.com/zloirock/core-js. * License: http://rock.mit-license.org. * . 2017 Denis Pushkarev. */.!function(t,n,r){"use strict";!function(t){function __webpack_require__(r){if(n[r])return n[r].exports;var e=n[r]={i:r,l:!1,exports:{}};return t[r].call(e.exports,e,e.exports,__webpack_require__),e.l=!0,e.exports}var n={};__webpack_require__.m=t,__webpack_require__.c=n,__webpack_require__.d=function(t,n,r){__webpack_require__.o(t,n)||Object.defineProperty(t,n,{configurable:!1,enumerable:!0,get:r})},__webpack_require__.n=function(t){var n=t&&t.__esModule?function getDefault(){return t["default"]}:function getModuleExports(){return t};return __webpack_require__.d(n,"a",n),n},__webpack_require__.o=function(t,n){return Object.prototype.hasOwnProperty.call(t,n)},__webpack_require__.p="",__webpack_require__(__webpack_require__.s=129)}([function(t,n,e){var i=e(2),o=e(18),u=e(13),c=e(14),f=e(19),a="prototype",s=function(t,n,e){var l,h,p,v,g=t&s.F,y=t&s.G,d=t&s.P,_=

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\loading[1].gif	
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/2.69.0/en-US/loading.gif
Preview:	GIF89a.....<..a.....!..NETSCAPE2.0.....!..ImageMagick.gamma=0.45455.!.....,.....V.....Zeo.\..u\..be.....~c}.....M.2..../.L..D..:..p;....>..o9..:.....#..!..ImageMagick.gamma=0.45455.!.....,.....!..ImageMagick.gamma=0.45455.!.....,.....V..!..ImageMagick.gamma=0.45455.!.....,.....!..ImageMagick.gamma=0.45455.!.....,.....F.....X...Ek. O{y.....X...,m..q.....?3..:.iJ.p..5s..J\6.....(..!..ImageMagick.gamma=0.45455.!.....,.....V..!..ImageMagick.gamma=0.45455.!.....,.....!..ImageMagick.gamma=0.45455.!.....,.....F.....X...Ek. O{y.....X...,m..q.....?3..:.iJ.p..5s..J\6.....(..!..ImageMagick.gamma=0.45455.!.....,.....V..!..ImageMagick.gamma=0.45455.!.....,.....;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\logo[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 226 x 48, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	3331
Entropy (8bit):	7.927896166439245
Encrypted:	false
SSDEEP:	96:zHjOKn3csE3x5liVsCo4GcPIZpV6x5cge8oo9:zDOK3zE3x5TCwcP4LQNeq
MD5:	EF884BDEDEF280DF97A4C5604058D8DB
SHA1:	6F04244B51AD2409659E267D308B97E09CE9062B
SHA-256:	825DE044D5AC6442A094FF95099F9F67E9249A8110A2FBD57128285776632ADB
SHA-512:	A083381C53070B65B3B8A7A7293D5D2674D2F6EC69C0E19748823D3FDD6F527E8D3D31D311CCEF8E26FC531770F101CDAF95F23ECC990DB405B5EF48B0C91B2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://erffggf.cf/jd/sharepoint-0/img/logo.png
Preview:	.PNG.....IHDR.....0.....sRGB.....IDATx..=w....G.z..L.4fN.k\dS..._`.....r...~.F..e._.RZ.0.K.\..CB...1.{qq/..^|.G..o.....?....Or.....y~....]..V.a.mM...M.\k*H..@B`s.$"n...)!.@"b#4. !.9...7.u...hD ....T.....:EJ.4"..X.....<\|.pgkk+....>~.....pju1i"b.J.&!.!...=T....k..D7.....O.<.?}...../..(.`0..!.C..'.?..e..~.....l6...._.x1rmR...$|E...l.WKDH...f..... ...Y.0R....>...{...-..o.....,...E../....._....eM.Q....@Q...w sp5.9..l.W)...Pq... .]..B..).../M.G.g....].V...5$<.....Eb.9.....>LYAk.Z.k..b..]N%>}4a....4!S...t..d..<.8AH+.../r...._...!qt.:q..fR.:..KW.._...T...5..>.0!.hq.rbND\...XR.,2.uX..Q.b...wQ.....g..X...F...~.....ikZE...UA....V.I!..]..Mm..R.....~k.VC.n..V.*B#W...\..yI.3.....2.....6c....2J....,g..5O1.s.4V2.....f..K..Obf\....;.w...\.F>F>6_z..P.dU<.wVV.....?.q.?&.....O.>....l.S.upp....59.C_.....fJ.M.={v,.....]Y_....n.?UF....v<.$..AD...p.....:$r =p...C.k.3....n.v..~.TGd!...l.W...s..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\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:	A10AD32428C2BF3A815C5F594C390812CA8FF9B7FAE49591CB9D2DBC7BDBEF70199808B69687A259F785DA80C9D49EE8E2FB300BE63B837ACBBA133D4DFD251B
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)||Object.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=Object.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\CS6IXJW6\preview-components~shared-file.ad8a132249[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\preview-components~shared-file.ad8a132249[1].js	
Size (bytes):	31371
Entropy (8bit):	5.4035622030959445
Encrypted:	false
SSDEEP:	768:1bufLTkkqKC/ugPK9QZWvB7mgI44id5qeVyRwI:h0PPC/W95v424idcwI
MD5:	F35FB7D310F85C009F4B837D2DCC5231
SHA1:	09D5D06C9C102CE7E9817B61BCD59182D8E75DFC
SHA-256:	CA4E12743A15E6864CDA722F1876332CE98542FB9FE53076C44865D528B2BAA1
SHA-512:	E9707EE08F26108C82808AEADEA698A92747FDD5618E78FE1E6A80ACBA3242510A9EA0D597041F05FB0AC110E253B2251896560566A830F3F14B1FC70D0108D8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn01.boxcdn.net/enduser/preview-components~shared-file.ad8a132249.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("BBtKKuFpl S"),p=n("1En/ASmD05"),f=n("0sbS2nMEFU"),w=n("wnhEk9N3Ty");function v(){return(v=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 b(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\CS6IXJW6\preview[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	64927
Entropy (8bit):	5.032389860121013
Encrypted:	false
SSDEEP:	768:SSl0/vylihw5Q136bUEcDefZYMki45g4vcqK7KOdUy7:BqhwE36gETZV4RK7KOd3
MD5:	724192BFC7925D7B33264393D94DB843
SHA1:	29EAC6C7B94690494179FFE9C8CEEB30CA38C2B9
SHA-256:	BE95FEA6E8E76B03B2C42821E5EC0E0D5BC64326E54DA731D61AF786AE2A2BDE
SHA-512:	BB0CBFA992CB6BEF9BFE92CECB1B21D181785A674BA80B4EBCC69B79D1FFB12F70E0D96AA1F98F6B89C484CC6745DBB94995A14D446FB0C8D0218E5A9F602 E0C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn01.boxcdn.net/platform/preview/2.69.0/en-US/preview.css
Preview:	/*!. * Box Content Preview. * . * Copyright 2019 Box, Inc. All rights reserved.. * . * This product includes software developed by Box, Inc. ("Box"). * (http://www.box.com). * . * ALL BOX SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESS OR IMPLIED. * WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF. * MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.. * IN NO EVENT SHALL BOX BE LIABLE FOR ANY DIRECT, I NDIRECT, INCIDENTAL,. * SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT. * LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE,. * DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY. * THEORY OF LIABILITY, W HETHER IN CONTRACT, STRICT LIABILITY, OR TORT. * (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE. * OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.. * . * See the Box license for the specific language governing permissions. * and limitations under the licen

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\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):	704488
Entropy (8bit):	5.356171646521712
Encrypted:	false
SSDEEP:	6144:z5wwJaP2dbt8oBoKjxAOfBUTY7Cx8RPvpeTZzMD2NQVGGbOm:uHYn37Cx8RPv4VMD2N0n
MD5:	A3FC1662F91C7B0F7BD1BA50479E5D68
SHA1:	6386DECA083D82061FEC29E476ECDD3F9F5AC96C
SHA-256:	E041549E4A937EE01627A0D6F9EB1D50F264E74170EA3FBA40ACD87735E5E1A8
SHA-512:	0E173467B16DC4BBFE6C136E0651F120D1E32C37F485B3DDA6C626F6B648465208B03C48BADCF5AF6566E9F4693793CD4A149F27E7672DE99DFEC109AA4202B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn01.boxcdn.net/platform/preview/2.69.0/en-US/preview.js
Preview:	/*!. * Box Content Preview. * . * Copyright 2019 Box, Inc. All rights reserved.. * . * This product includes software developed by Box, Inc. ("Box"). * (http://www.box.com). * . * ALL BOX SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESS OR IMPLIED. * WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF. * MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.. * IN NO EVENT SHALL BOX BE LIABLE FOR ANY DIRECT, 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\CS6IXJW6\share-point[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	15526
Entropy (8bit):	5.721275823828831
Encrypted:	false
SSDEEP:	384:Ox5T7PuUyxgg2Ctjo/kohz2YDDD1fSCRdVl37Sm9:OjT7GDxgg2GE/kohz2YDDD1fS8oh9
MD5:	63DF83784CADD3A339B776520600C21A
SHA1:	69BB829612F3E3CB2F521323945C9284A2B0DCDE
SHA-256:	2EE69AEF3AFB10B368BDE9FEA7E97CC75C030C890E3D2B8DC4AD19D498234DBF
SHA-512:	FC1C4F31A0817471D1D2CA8ADEA7F3C39B67B0EA688CC58EB4F6C68F5F6558E236B9D3D2D8BA95EE296CFBF3C0197CE54DFECADBCCCE1B7497542FEE2914 1D5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://erffggf.cf/jd/sharepoint-0/css/share-point.css
Preview:	html {...line-height: 1.15;...-ms-text-size-adjust: 100%;...-webkit-text-size-adjust: 100%..}..body {...height: 100%;...margin: 0..}..article, aside, footer, header, nav, section { ...display: block..}..h1 {...font-size: 2em;...margin: .67em 0..}..figcaption, figure, main {...display: block..}..figure {...margin: 1em 40px..}..hr {...box-sizing: content-box;.. .height: 0;...overflow: visible..}..pre {...font-family: monospace, monospace;...font-size: 1em..}..a {...background-color: transparent;...-webkit-text-decoration-skip: objects..}. .abbr[title] {...border-bottom: none;...text-decoration: underline;...text-decoration: underline dotted..}..b, strong {...font-weight: inherit..}..b, strong {...font-weight: bolder ..}..code, kbd, samp {...font-family: monospace, monospace;...font-size: 1em..}..dfn {...font-style: italic..}..mark {...background-color: #ff0;...color: #000..}..small {...font-size: 80%..}..sub, sup {...font-size: 75%;...line-height: 0;...position: relative;...vertical-align: b

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\vendors~app.1978418f74[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	1094388
Entropy (8bit):	5.439011389373188
Encrypted:	false
SSDEEP:	6144:iFAk2GFOjBGbdvd778oTx9ZMKTTaJF2MKYTdjwmdLlyfLplkWmAYTdjjv4i5pvYY:UrjOj8hFTTB6lKFmH5pQ45CfHnrs
MD5:	7C0EAC129EFCA3017C9B49934D95E781
SHA1:	32718812DCB6E0D24F79F1062B78EADC06F1E602
SHA-256:	7CE5AD473F7F68D1C2847009FDC3F1468CCF9157E86D386FE5FCCEE3ECF1720F
SHA-512:	9C9C921B3C7FA9E118E601020C3811887745BDDEEFA33F3E93E701D798177603A4704728FC9005686C3126E360CE448520F09BB9AD69D5B8991B9BD8DDE32EA(
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn01.boxcdn.net/enduser/vendors~app.1978418f74.js
Preview:	/*! For license information please see vendors~app.1978418f74.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"),a=n("t2Dn8l5vat"),i=n("cq/+ZHEllX"),o=n("T1AVtgJeLR"),s=n("GoyQGQ25b1"),u=n("mTTRHTH0TC"),c=n("itsjJeh/nX");e.exports=function e (t,n,l,f,d){t!==n&&i(n,(function(i,u){if(d||(d=new r),s(i))o(t,n,u,l,e,f,d);else{var p=f?f(c(t,u),i,u+"",t,n,d):void 0;void 0===p&&(p=i),a(t,u,p)}}),u)}},"+c4WVrHK/K":function(e,t,n) {var r=n("711d4qXG

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\as-security~change-current-user-role-modal~collaborators~collection-detail-page~content-explorer-mod~2da256af.a0db8de5f2[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):	5.495168521800379
Encrypted:	false
SSDEEP:	384:p/CXDeUxEk4s4xb268LYhyqYvfGTW8QWoK7aHFlXZhq4f/RW94sPRugXhkUF5no7:pK6ls4xi6CcQ5SPq2iCBS3HTC
MD5:	A0A0AD79772308D2FA9C7FEB0D365E27
SHA1:	B6D6AD65CDE92616D62EB1593ED804FE9671ED48
SHA-256:	8F27FA13A51FAF0B5264DCCA894F10471640F4BC6DE092DB4D54137635308312
SHA-512:	68FE411A6FF74D2DB8BB44BF8274CCE0481CC4A22569636E3F49B706295CCE0064A0CB169D945B7EF851873393561EA2195D155A0D88B14F759C81D0D230146C
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~2da256af.a0db8de5f2.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\as-security~change-current-user-role-modal~collaborators~collection-detail-page~content-explorer-mod~2da256af.a0db8de5f2[1].js

Preview:


```
(window.webpackJsonp=window.webpackJsonp||[]).push([["as-security~change-current-user-role-modal~collaborators~collection-detail-page~content-explorer-mod~2da25
6af","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},"+plKfkdWim":function(t,e,n){n("ApPDsGgrfM"),t.exports=n("WEpklf3dyC").Object.getPrototypeOf},"0HdwK5vH5Z":function(t,e){t.exports=function(t){return
t&&t.__esModule?t:{default:t}}
```


C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\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, 1024x1024, frames 3
Category:	downloaded
Size (bytes):	60846
Entropy (8bit):	6.888247639055118
Encrypted:	false
SSDEEP:	768:FbV+wCUE0R2leBd9brQj06x0ekhbh5s5BHVyBKFSSd1GMhl0OmiPOjRmJ:C3eBdZrwubLsHHVH9ZamJ
MD5:	12E19BE7F23232BF4851B60FAA4FAB70
SHA1:	216FBE74D066A63FF51C34AF13ED9DCF339CD579
SHA-256:	E6315F6A423FA162F2C9C6E8B56EF9A6B4DD1A1AEDA076285A1C120FFBCA4DD3
SHA-512:	4D32E25A75DAD38812A50A76AA52E37162CC83F18EC2E834BB3ED9715C53DE1F16B13AA24DBE9B2F360EA658906D6976B0EBADBFF343260C169028B268FB741 1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://public.boxcloud.com/api/2.0/internal_files/797531939634/versions/852889767234/representations/jpg_1024x1024/content/?access_token=1!njIT8VPswMD6-FhGnf5Sg6ngjcePllMVMXIPJUNrryKT4ZNkRGP1ZYvo8zmSD2Wb9HLZWwAnxH6oWoNy4ykuINGq8tdQ8lOJN9YhCnvMR8Ci-uYg1gNBsgGJ6rqR3YdeF8m4oqN0wctIFTh1wA5nK8fsGju46kXVYFyNKDOM-uvN2gAvgMs3vPB9mM4kRDJqz-CXYWV0svEJgVfdIuB3wjwPXAa7xDTqhiMqVdm7NL6fUDWZbG3KI_A4Vzpprmpq8b2X9vItlOix0nlw585BgrVaJcwuJCBnAYyfuHAugr7JvyI3fp9_KixGam8CoqpCuqdKTxhio7q3E5ufZDQbdWcF4TZ582duJtOcxKee86bFkx1yg-mdvG64ZNNIoVbhXmnvf1iifI2Xi1_TeT6ebsj9FJGMuu7G9ZvRupcvH-IUh-ktpgL6A9WP5I5FF4ZcGm_aftk5Uufzv7cOAllz2U3bBGuTAtoSgniy1WjeDb5tKGEnncq_CpUtXf4EaxdXXmKLI6-J3xHAAvb6baEziMEUBVn8WSKIsAbx66mkjxeLodF0ywL5DWbKVhY4Elc.&shared_link=https%3A%2F%2Fapp.box.com%2Fs%2Fldmpej4bczs3ra2es3qlr0qrqifh99wc&box_client_name=box-content-preview&box_client_version=2.69.0

Preview:


```
......JFIF.............Exif..MM.*................J..........R.(.......................i........Z.............................0232..................9...........0100...............ASCII...pdfWidth:504.00pts,pdfHeig
ht:504.00pts,numPages:1....C...................................................................C.........................................................................................................h.......................
....!.1.."AQ.2a....#RVq.....3BS...$48CTUbrtv..79...&6c.....DEFWw...dfsu.......................................H......................!..1a...AQSq........2RT...."34r..$5B#b%C.....s...........?..S..
...............................................................................................................................................................................................................................
.....................................................................
```


C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\favicon-32x32-VwW37b[1].png

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 32 x 32, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	1157
Entropy (8bit):	7.424718197664869
Encrypted:	false
SSDEEP:	24:hMkjvNSTHDyCbibxDx4fZ9qMfhkbOTKBN:hdjvA3bc9ENhkbb
MD5:	86AEDF25C0B3AE1224D92E32D80FFEF8
SHA1:	D75B54256BC48B27E6D7DF1C2A6F4635DE2FE5EE
SHA-256:	D1A4A65AC84A381199843B9722E6470470C8093885CF2A6481C2FF0DEF618C64
SHA-512:	13C4E0AF14577A4858D6E85D93E399186FD5F4AD4A836FA014D89C79673FF7E53EE9B06DE271374C70B3B15F72250075CB8F20E690AAAEE93C6698ABF7D6898
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn01.boxcdn.net/_assets/img/favicons/favicon-32x32-VwW37b.png

Preview:


```
.PNG........IHDR... ... .....D.......gAMA......a.....sRGB........ cHRM..z&.............u0...`..:....p..Q<....PLTE....a..a..a..a..a..a..a..a..a..a..a..a..a..a..a..a..a..a..a..a..a..a..a..a..a..a..a..a..a..a
..`.._.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\OR0WKIO1\li6orbsabcm5o36s3wlba8p8[1].htm

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text
Category:	downloaded
Size (bytes):	4306
Entropy (8bit):	5.189381735103431
Encrypted:	false
SSDEEP:	96:IusujH4WP0Yanwtwioywe4/JS3ejrw+ti7twzd7+uM:TH4WPDanwtwi5we4vrw+tqtwzlM
MD5:	86D9014D5BA2388806BA47FD139587E6

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\li6orbsabcm5o36s3wlba8p8[1].htm	
SHA1:	77C730A19F1F4FA067F7B390D09FA93A634B9439
SHA-256:	0AC4641C1120D7591AF50D7EDFC1687D08E0D8E3FBA0EECC3EA3A12FB1492030
SHA-512:	07098D31126B8AF3406ACE36CED2B22199C8B64312FF3D195205BB33CB3AAF9A5D002EA9294B83E59DDCB5B96B7B13AF424E01697379F2403623A51CB7E956F
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_10, Description: Yara detected HtmlPhish_10, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\li6orbsabcm5o36s3wlba8p8[1].htm, Author: Joe Security
Reputation:	low
IE Cache URL:	http://https://erffggf.cf/jd/sharepoint-0/li6orbsabcm5o36s3wlba8p8.php?rand=13InboxLightaspxn.1774256418&fid&1252899642&fid.1&fav.1&email=
Preview:	<!doctype html>.<html>..<head>..<meta charset="UTF-8" name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, minimum-scale=1.0, user-scalable=no">..<title>Sharing Link Validation</title>..<link rel='stylesheet prefetch' href='https://fonts.googleapis.com/css?family=Open+Sans:600'>..<link rel="stylesheet" href="css/share-point.css">.</head>..<body>.. ... . SharePoint.... ... ...<img class="microsoft-logo" src="img/logo.png" alt="">.... ....<span style="font-family: 'Segoe UI Web (West European)','Segoe UI',-apple-system,BlinkMacSystemFon

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\preview-components.a5aea5c3e0[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):	21786
Entropy (8bit):	5.025510764924365
Encrypted:	false
SSDEEP:	384:jvVY2bm2cD2cI252TTc//T4/fnsWsgeWegnWngwWwhsQsGeQeGnQnGwQwrE07Sg9:jvTorMuHY6mD2RhO6rFZU
MD5:	4CCC39E80CC569305D87B440DEF31D65
SHA1:	2C75DDBA7DDC53EE2F2BB80867ADC8264F054CAC
SHA-256:	37B047678243379CF8ECAAE2E6E4EC028AEB21B9F8BD13183F4A5C69945FCD77
SHA-512:	6574756A4E219B8ABFEE90F232A53106AFA887D7AD6CB51BB99E70F71CDAE45187D302382ACFCA33FF7FEDB0258C6DDE8D29A6A1B386E61948953B7B96C393 1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn01.boxcdn.net/enduser/preview-components.a5aea5c3e0.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\OR0WKIO1\preview-components~shared-file.4fbef49e0d[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:	C6A43F897F882A6DAC9585E2C66A1F3BF68012BE1E8870F5E9295B17877AC46751D23ADC9DC02828B837EDDFD28E74D46B6CDD3AE916CF25C72BA7D3AAF89 35
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn01.boxcdn.net/enduser/preview-components~shared-file.4fbef49e0d.css
Preview:	.MaliciousBanner .icon-alert-circle{margin-right:5px}.EditClassificationButton,.EditClassificationButton:hover{margin-left:6px}@media (max-width:849px){.EditClassificationButton{display:none}}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\promise[1].js	
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\OR0WKIO1\runtime.989e647586[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):	45981
Entropy (8bit):	4.911671958491008
Encrypted:	false
SSDEEP:	768:PLeRnRMGVoxdDta9Uvxt6z/qNQJ3JnNIa2dq20qHGeRnRMGVoxdDta9Uvxt6z/qY:QRyxsz/qN43JardqV9sRyxsz/qQnI3GZ
MD5:	7BA2B159D69A6BE5E5D6E455B1535C76
SHA1:	99C65A5065EEB4FDFD3323CE057D9D5EE93F1F2C
SHA-256:	E7FA097600C81B07A2ECBCD4680E2DA6783733804559C8C491C06E27F00DDAB8
SHA-512:	28F6255E794D809E0D2CA9AA3B3E720A39A1D45EFABB38229D63CB4F0368C4B92256D43518F8DDA6C20953A7505C417ACF81DE3C23E891A3AE645F5393E4443
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn01.boxcdn.net/enduser/runtime.989e647586.js
Preview:	!function(e){function a(a){for(var t,l,d=a[0],i=a[1],r=a[2],c=0,f=[];c<d.length;c++)l=d[c],Object.prototype.hasOwnProperty.call(n,l)&&n[l]&&f.push(n[l][0]),n[l]=0;for(t in i)Object .prototype.hasOwnProperty.call(i,t)&&(e[t]=i[t]);for(m&&m(a);f.length;)f.shift()();return s.push.apply(s,r||[]),o()}function o(){for(var e,a=0;a<s.length;a++){for(var o=s[a],t=!0,l =1;l<o.length;l++){var i=o[l];0!==n[i]&&(t=!1)}t&&(s.splice(a--,1),e=d(d.s=o[0]))}return e}var t={},l={runtime:0},n={runtime:0},s=[];function d(a){if(t[a])return t[a].exports;var o =t[a]={i:a,l:!1,exports:{}};return e[a].call(o.exports,o,o.exports,d),o.l=!0,o.exports}d.e=function(e){var a=[];l[e]?a.push(l[e]):0!==l[e]&&{"access-stats-export-modal~activity-sidebar~as-account~as-diagnostics~as-integrations~as-notification~56206fd7":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\shared-file.058946a378[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):	13528
Entropy (8bit):	5.272249940260548
Encrypted:	false
SSDEEP:	192:SnwXvKIorujBkyyolc49/4TfiFSr5fkro0O9VDqyY5F7rfJcyFocuVy6:ms8u2gltAiFYIpO9VevJcyFej
MD5:	6CC8350017812880D8515965592F6AFE
SHA1:	4FCAF5D1BEE80FB89920FEE501AC0B89279BC4E4
SHA-256:	CCA8DE909FDA557182FA587E7FB924F5C24423D3EFD54A57FDD803B2EC080EE5
SHA-512:	D9101C87857AAB489D60314BF868EBCEDBB05400B2FA5C2926E576EDEA550697096EF2BBC8096BF4F46C104DFBDAF4A54DEE5D97DD758DB0DD0B5B0D261C2 C57
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn01.boxcdn.net/enduser/shared-file.058946a378.js
Preview:	(window.webpackJsonp=window.webpackJsonp||[]).push([["shared-file"],{"8bPKGyOoiP":function(e,t,n){},"9Nyd+vSxbR":function(e,t,n){},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(O bject.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])})):Ob ject.getOwnPropertyDescriptors?Object.defineProperties(e,Object.getOwnPropertyDescriptors(n)):u(Object(n)).forEach((function(t){Object.defineProperty(e,t,Object .getOwnPropertyDescr

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\shared-file.f1f6d40967[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\OR0WKIO1\shared-file.f1f6d40967[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.f1f6d40967.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\Temp\dat8C00.tmp	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 119132, version 1.0
Category:	dropped
Size (bytes):	119132
Entropy (8bit):	**7.991532245734968**
Encrypted:	**true**
SSDEEP:	3072:pECjkMzGFzkgGdoAiZzixFwotRAE9urcBQbtF0roFS:pECjVzIGYZ4Fpx9urUQbtFeoFS
MD5:	3E4A4FC6317C4C2CF35D7C77EC1789C3
SHA1:	40EA0D8678B92988824193587F707E3AEDC4591F
SHA-256:	607EC0A4A29F6A4607F6E0A3CF486E50322DDF66F1F1870150CB69A7061E978D
SHA-512:	F7D639520F4C3A3539AD7506EC1CEBED8107C2A264316FE0E98A15132ACCFE6212A22391F4A7203B6D8304B3222B603F0137BA9ACAC7478F217363EEF4556DE
Malicious:	false
Reputation:	low
Preview:	wOFF.....\.....FFTM.....p.\MGDEF.....7...8.x..GPOS.....z...b...GSUB...x...,...FA..sOS/2....._...`i...cmap.....x.!>cvt .....r....?9..fpgm...T..... ..gasp.....glyf.....a..?.head.....1...6..qfhhea.....!...$....hmtx.....C.2loca.....-&maxp..... ... .L..name.....hpost.....'....)prep.....o.i:webf...T... .....`.V.....=.....y.....x.c`d``..b...`b`e`dj..f.6.f.v.o.F..._.&.?.^.F...*..i..C.x...|M.....!.<.fEI.USS\TcVUTT.E.UUu.RUUWCM5W.U5....Ap".H"b.I.'!..j..g.....o_..Yg...z.z...Jv\..!<. .p..{_....cG.....h1..q.E'.B.!..!...I.s.....W.).T.....a.7QO4...x.-D[.Y....`1B....1M...1v...;E.D;..c.....b.....;.....v^..^...M..&.F.f...u.]Eo..$....7.Vi...&W9]..au}F].T....[>.t.....+..F j.X.^U...jzu}.._W...OS.....M.;.].k.fQ..../.K.h.f..\.vr..... ..#]G..s..:.u.k..\.E..]W..s...u..!.c..\3]s\.\.....r.....-.-..[...n....w.....n...p.....nS..

C:\Users\user\AppData\Local\Temp\dat8C8E.tmp	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format (Version 2), TrueType, length 84396, version 2.983
Category:	dropped
Size (bytes):	84396
Entropy (8bit):	**7.996116383259223**
Encrypted:	**true**
SSDEEP:	1536:lhWk7aeOTww2X4owbcnRqvjFkw8cyW/fTJnh2r667bZ3fTyG/q+TBpMLB:lHdOk9ojj2a//rFoeutTyG/ZBC
MD5:	8A54EA1AEB67D07C751BD5F03068317B
SHA1:	CFBEE4F2FD7F359A2A60648BB6797CAC1FD4DA3E
SHA-256:	4230A20B841519BDBE4B0C154BAD414E017CF80B3918127D45C4F907EEA07280
SHA-512:	A3CA9E052DBB81A20C71DDD24962CE57E842134A8B30842328410DF3FCF76EED4367C3A5A1148DD11092CF0CF3E29B57040CF79D40AC6450D8234F27204D47E
Malicious:	false
Reputation:	low
Preview:	wOF2.....I.....m...I;.....?FFTM..8...>..F.`.. ..j.....|.6.$..$..(.. ..Z.....9?webf.[/0..B%.^..m.m..[..F...&...v....!.....i.V]\.I....b.a..96....H.....J...../....3.H...X.g.** .j.....v.!p4.-.I....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\datA806.tmp	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	OpenType font data
Category:	dropped
Size (bytes):	1120
Entropy (8bit):	3.252203479159748
Encrypted:	false
SSDEEP:	12:+5Pc921oNY0p9b1IfSly/VAAc5EK/HU1qsG1bhCEo8+R5+ddmq0/gNV11Mp1VjED:+S9fuUx1IfSljAP3G6M3B8PwQAo/K
MD5:	2B87BDC9369E256C61872AA2A2B51C9D
SHA1:	5373C688D8DE2AB2EA0142A58D6DB9D9AE2EAF94

C:\Users\user\AppData\Local\Temp\datA806.tmp	
SHA-256:	0F989EC9456A15AC03963AA23BD73F1FD7BB9A02C3AD360983AF0EAEF81C329A
SHA-512:	709897B78A667F915BE2DD81E9A961ACD4B61C1C6C6EF85EFEB107CC842F4A1FD8C3E3B90DA4A60A248CCE6DCBC0B8E8B8CCEF953EEB813CC2964B158D02F94
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....!.....|..... !XXXlt16179900159200XXXXXXXX

C:\Users\user\AppData\Local\Temp\datA874.tmp	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	OpenType font data
Category:	dropped
Size (bytes):	1120
Entropy (8bit):	3.2450606220168914
Encrypted:	false
SSDEEP:	12:+5br921oNY0p9b1IfSly/VAAc5EK/HU1qsG1bhCEo8+R5+ddmq0/gNV11Mp1VjXh:+Rr9fuUx1IfSljAP3G6M3B8PrCAo/K
MD5:	E1C4F2715CC2DC892147D166D44E0C05
SHA1:	E43CEFA29EBE0DA6C6B855AC263B8DD53BE2E98A
SHA-256:	D9BC6A022BE33B5502940A81D9235252A8B616779EE6609D696A638388FF9C9E
SHA-512:	7779A2D5BDD2D03D4B9141B51938DEA92B01222A06F775225ECE6E0E18388C6CB6AF93B925648175EAD4CD45C21D832BC13A7B52E3898D26CA4C68C009F7DC7
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....!.....|..... !XXXlt16179900160261XXXXXXXX

C:\Users\user\AppData\Local\Temp\datA911.tmp	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	OpenType font data
Category:	dropped
Size (bytes):	1120
Entropy (8bit):	3.2493952228849925
Encrypted:	false
SSDEEP:	12:+5eR921oNY0p9b1IfSly/VAAc5EK/HU1qsG1bhCEo8+R5+ddmq0/gNV11Mp1Vjra:+oR9fuUx1IfSljAP3G6M3B8P3Ao/K
MD5:	54124C1DC7524719CC83DA42A757F67C
SHA1:	96F63F92A6485249222047 96FF1D5FDCDCDF0EF5
SHA-256:	09F15D443AE33D998AE652C7BEF41BAF1108B5BE29B798EFF9A7FAFB3BF54E00
SHA-512:	93B7727A25879284F833BD37EC7FE69D417DE35B7134559041345B9445716FC0859B8E9C7CEB8913937E96A782DEFAC30E706DE975E6F46355A8A68D21E41474
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....!.....|..... !XXXlt16179900161672XXXXXXXX

C:\Users\user\AppData\Local\Temp\datA961.tmp	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	TrueType Font data, 13 tables, 1st "OS/2", 20 names, Macintosh, \251 2018 Microsoft Corporation. All Rights Reserved.
Category:	dropped
Size (bytes):	82268
Entropy (8bit):	5.144804657433481
Encrypted:	false
SSDEEP:	768:0suVhMTXKNDmWI4CAPHSEeToYGXFUBRbU40qVcXpJrB5svFS3dCC:4Yb4xPyhKeRb2XpJrzVd
MD5:	338090212C9A8635572AC20DE9D48C75
SHA1:	8FF5C895B6169F8354CCE22AE34583F76698CD80
SHA-256:	22134C4719323D485AE28D5DA9F03E4F6CBE0ABC4EAA4ABBF9847E3AD3091DC1
SHA-512:	5D565642172A900F2243DEEA048F2FD4130E2F52583D00556602D447DE2D6B6731D674D09921A1705E06899890122EB5014F556A3FA1A7DEFF75466C74FDD876
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\datA961.tmp	
Preview:	..........POS/2..9).....`cmap...T...<...vcvt ?.X.....fpgm..B....<....glyf.W>....P..r.head.|y.....6hhea.....$hmtx..$^...,..i.loca.B./.....6Xmaxp(.....$4... nameV....$T....post.....*X... prep.@.s..*x.....J.....3.....3.....${.....MS . .....& ..... .....j.....$.....J...X.D.E.....&.,.D.E.K.W.d.z.....(.P.Z.].o.u.v.}... .....`.....).....m.....&.....&.....?..... 6.....p.r.u.x.y.z.{.}.~..... .....

C:\Users\user\AppData\Local\Temp\datA990.tmp	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	TrueType Font data, 13 tables, 1st "OS/2", 20 names, Macintosh, \251 2018 Microsoft Corporation. All Rights Reserved.
Category:	dropped
Size (bytes):	82448
Entropy (8bit):	5.150566447385317
Encrypted:	false
SSDEEP:	768:osuVhMTXKNDmWI4CAPHSEeToYGXFUBRbU40qVcXpJrB5svFS3dCC:8Yb4xPyhKeRb2XpJrzVd
MD5:	AD4439CA330A2B3A389ABDC9AE8F3B77
SHA1:	3FF6B45EC83D5E965EFA4AD4BCB7C705379867FA
SHA-256:	8A38BD1F0BA3DF1C23A412C60B9C020A6A5769F83062CCAA78ED388F1B2DF828
SHA-512:	D388C94B4AAC45D935A2C59EC07A5EAB0B60F443B1AFBD6157BEF2A2330746DE2711437D2902A87B59A220F11D8C4CB479B9E72F3410B5C611FA8E6A1250082
Malicious:	false
Reputation:	low
Preview:	..........POS/2..9).....`cmap.-r....<...*cvt ?.X....h.....fpgm..B.....glyf.W>.....r.head.|y.....6hhea.....$hmtx..$^.....i.loca.B./.....6Xmaxp(.....$.... nameV....%.....post.....+.... prep.@.s..+,.....J.....3.....3.....${.....MS . .....& ....~.....*.....&.,.D.E.K.W.d.z.....(.+.,.-...8.G.K.L.O.P.U.Z.].f.o.u.v.}.....%.&.J.Q.X.....D.E.W.....!.&.'.(.).-.2.....`.....).. .....m.....&.....&.....?....6.....p.r.u.x.y.z.{.}.~..... .....

C:\Users\user\AppData\Local\Temp\datE68B.tmp	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 2532, version 2.24904
Category:	modified
Size (bytes):	2532
Entropy (8bit):	7.627755614174705
Encrypted:	false
SSDEEP:	48:WGMiY6eIlk7QuaqrjRh4pi6j4fN6+XRsnBBpr+bes:WRBLIloQuHfRh4pi6sfPGnDFs
MD5:	10600F6B3D9C9BE2D2B2CE58D2C6508B
SHA1:	421CA4369738433E33348785FE776A0C839605D5
SHA-256:	29B7A9358ABDC68C51DB5A5AF4A4F4E2E041A67527ADEE2366B1F84F116FE9A5
SHA-512:	B6C04F3068EB7DAC8F782BDED0FE815B4FE5A9BECCF0B561D6CEAEAA7365919A39710B2D1AD58D252330476AA836629B3C62C84FABFA6DC4BCF1C8F055D66 C1C
Malicious:	false
Reputation:	low
Preview:	wOFF.....aH.....OS/2...D...H...`1Wp.cmap.....l...b..ocvt ..... ...*....fpgm.....Y...gasp.....glyf.....Whead.....2...6.tJ.hhea.....$....hmtx..... .....loca.....X.hmaxp...,..... .y..name...L.....Mpost...D..... .Q.}prep...X.....x...x.c`aog.....:....Q.B3_dHc..`e.bdb... .`@..`.....,9.\|...V...)00...C..x.c```f.`..F.....\|... ..... .\..K..n.,..g`@.I\|.8"vYl.....p...0.....x.c.b.e(`h`X.....x.....x.]..N.@..s$..'@:!.u*C....K$.%%...J.....n..b.....\|.s...\|v..G*)V.7.....!O.6eaL.yV.e.j..kN..M.h....Lm....-b....p.N.m. v.....U<..#...O.}.K..,V..&...^...L.c.x.....?ug..l9e..Ns.D....D...K.....m..A.M....a.....g.P..`....d.....x..R.K.1...$....g-.B.Vq..m..Z..T..@\t.E...7X...:.).c... ].{.Q.[7'...`.^...&....{y<..N. ....t...6..f....\.K1..Z}{.eA-..x.{....0P7p.....l.....E...r....EVQ.....Q_.4.A.Z..;...PGs.o..Eo...{t...a.P.~...b,Dz.}.OXdp."d4."C.X..&,u.g.....r.c..j

C:\Users\user\AppData\Local\Temp\~DF1D930BD22B0D5A83.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	46929
Entropy (8bit):	0.8163984837384177
Encrypted:	false
SSDEEP:	384:kBqoxKAuqR+RP98fm1KjW1KAvljRBvJv1kvukvkkv1kv:RjXJhCr9m
MD5:	F10A0B07EBEFD964CE6C6E5812CD9448
SHA1:	DC6A28A2D678FAAAB39F21F8959BFBB5CDFC3211
SHA-256:	AD5751191C55FA0097928C431680AF036373CB065C138154B305842648675DF9
SHA-512:	D12CC10BC26FC4988BAAC985E056E9325101F191F6456639A9791BD037F56C851BCF783E3CB181C50152FDAE38A08CE7B77F7AA5B253403CFC12F0403CA85F2
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF4580B808E1CFC63F.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.27918767598683664
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laA:kBqoxxJhHWSVSEab
MD5:	AB889A32AB9ACD33E816C2422337C69A
SHA1:	1190C6B34DED2D295827C2A88310D10A8B90B59B
SHA-256:	4D6EC54B8D244E63B0F04FBE2B97402A3DF722560AD12F218665BA440F4CEFDA
SHA-512:	BD250855747BB4CEC61814D0E44F810156D390E3E9F120A12935EFDF80ACA33C4777AD66257CCA4E4003FEF0741692894980B9298F01C4CDD2D8A9C7BB522FB
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF999979F56005C7E8.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.4781946887148703
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lol9loF9lW9TqIOqa:kBqoIOwlqDqa
MD5:	161819C33711A456036264626B40D392
SHA1:	CB5E419D5D2547ED8538E1CE2F6D12506522062D
SHA-256:	B85D3C0DE56485273CE5BE82EC379690FDA77C67806C9ED7F6DC7CBB2F19FAE7
SHA-512:	05F4F106D17D1BE2B657912C9504CF087F2090D2E266FB3A1BAD475DAEB8765F4D8BF164975E4FA7FB547F526DB601D8C49E9471A0AAA80948DC8919B8714EE
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

Total Packets: 107

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 9, 2021 19:40:08.698887110 CEST	49738	443	192.168.2.4	185.235.236.201
Apr 9, 2021 19:40:08.700051069 CEST	49739	443	192.168.2.4	185.235.236.201
Apr 9, 2021 19:40:08.716732979 CEST	443	49738	185.235.236.201	192.168.2.4
Apr 9, 2021 19:40:08.716842890 CEST	49738	443	192.168.2.4	185.235.236.201
Apr 9, 2021 19:40:08.718766928 CEST	443	49739	185.235.236.201	192.168.2.4
Apr 9, 2021 19:40:08.718929052 CEST	49739	443	192.168.2.4	185.235.236.201
Apr 9, 2021 19:40:08.728879929 CEST	49739	443	192.168.2.4	185.235.236.201
Apr 9, 2021 19:40:08.729167938 CEST	49738	443	192.168.2.4	185.235.236.201
Apr 9, 2021 19:40:08.746560097 CEST	443	49739	185.235.236.201	192.168.2.4
Apr 9, 2021 19:40:08.746588945 CEST	443	49738	185.235.236.201	192.168.2.4
Apr 9, 2021 19:40:08.747698069 CEST	443	49739	185.235.236.201	192.168.2.4
Apr 9, 2021 19:40:08.747725964 CEST	443	49739	185.235.236.201	192.168.2.4
Apr 9, 2021 19:40:08.747746944 CEST	443	49739	185.235.236.201	192.168.2.4
Apr 9, 2021 19:40:08.747778893 CEST	443	49738	185.235.236.201	192.168.2.4
Apr 9, 2021 19:40:08.747797966 CEST	49739	443	192.168.2.4	185.235.236.201
Apr 9, 2021 19:40:08.747807980 CEST	443	49738	185.235.236.201	192.168.2.4
Apr 9, 2021 19:40:08.747829914 CEST	443	49738	185.235.236.201	192.168.2.4
Apr 9, 2021 19:40:08.747852087 CEST	49739	443	192.168.2.4	185.235.236.201
Apr 9, 2021 19:40:08.747859001 CEST	49739	443	192.168.2.4	185.235.236.201
Apr 9, 2021 19:40:08.747895956 CEST	49738	443	192.168.2.4	185.235.236.201
Apr 9, 2021 19:40:08.747915983 CEST	49738	443	192.168.2.4	185.235.236.201
Apr 9, 2021 19:40:08.789563894 CEST	49739	443	192.168.2.4	185.235.236.201
Apr 9, 2021 19:40:08.790915966 CEST	49738	443	192.168.2.4	185.235.236.201
Apr 9, 2021 19:40:08.795468092 CEST	49739	443	192.168.2.4	185.235.236.201
Apr 9, 2021 19:40:08.809607983 CEST	443	49739	185.235.236.201	192.168.2.4
Apr 9, 2021 19:40:08.809740067 CEST	49739	443	192.168.2.4	185.235.236.201
Apr 9, 2021 19:40:08.811553955 CEST	443	49738	185.235.236.201	192.168.2.4
Apr 9, 2021 19:40:08.811655998 CEST	49738	443	192.168.2.4	185.235.236.201
Apr 9, 2021 19:40:08.856940985 CEST	443	49739	185.235.236.201	192.168.2.4
Apr 9, 2021 19:40:09.133900881 CEST	443	49739	185.235.236.201	192.168.2.4
Apr 9, 2021 19:40:09.133940935 CEST	443	49739	185.235.236.201	192.168.2.4
Apr 9, 2021 19:40:09.134018898 CEST	49739	443	192.168.2.4	185.235.236.201
Apr 9, 2021 19:40:09.134418011 CEST	49739	443	192.168.2.4	185.235.236.201
Apr 9, 2021 19:40:09.320306063 CEST	443	49739	185.235.236.201	192.168.2.4
Apr 9, 2021 19:40:09.320333004 CEST	443	49739	185.235.236.201	192.168.2.4
Apr 9, 2021 19:40:09.320369005 CEST	49739	443	192.168.2.4	185.235.236.201
Apr 9, 2021 19:40:09.320398092 CEST	49739	443	192.168.2.4	185.235.236.201
Apr 9, 2021 19:40:09.381652117 CEST	443	49739	185.235.236.201	192.168.2.4
Apr 9, 2021 19:40:09.381665945 CEST	443	49739	185.235.236.201	192.168.2.4
Apr 9, 2021 19:40:09.381717920 CEST	49739	443	192.168.2.4	185.235.236.201
Apr 9, 2021 19:40:09.381752968 CEST	49739	443	192.168.2.4	185.235.236.201
Apr 9, 2021 19:40:11.032999992 CEST	49739	443	192.168.2.4	185.235.236.201
Apr 9, 2021 19:40:11.050554037 CEST	443	49739	185.235.236.201	192.168.2.4
Apr 9, 2021 19:40:11.622287989 CEST	443	49739	185.235.236.201	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 9, 2021 19:40:11.622334957 CEST	443	49739	185.235.236.201	192.168.2.4
Apr 9, 2021 19:40:11.622410059 CEST	49739	443	192.168.2.4	185.235.236.201
Apr 9, 2021 19:40:11.622488976 CEST	49739	443	192.168.2.4	185.235.236.201
Apr 9, 2021 19:40:13.072390079 CEST	49739	443	192.168.2.4	185.235.236.201
Apr 9, 2021 19:40:13.077361107 CEST	49738	443	192.168.2.4	185.235.236.201
Apr 9, 2021 19:40:13.081935883 CEST	49739	443	192.168.2.4	185.235.236.201
Apr 9, 2021 19:40:13.090195894 CEST	443	49739	185.235.236.201	192.168.2.4
Apr 9, 2021 19:40:13.095066071 CEST	443	49738	185.235.236.201	192.168.2.4
Apr 9, 2021 19:40:13.099560022 CEST	443	49739	185.235.236.201	192.168.2.4
Apr 9, 2021 19:40:13.261368990 CEST	443	49738	185.235.236.201	192.168.2.4
Apr 9, 2021 19:40:13.261512995 CEST	49738	443	192.168.2.4	185.235.236.201
Apr 9, 2021 19:40:13.306564093 CEST	443	49739	185.235.236.201	192.168.2.4
Apr 9, 2021 19:40:13.306612968 CEST	443	49739	185.235.236.201	192.168.2.4
Apr 9, 2021 19:40:13.306709051 CEST	49739	443	192.168.2.4	185.235.236.201
Apr 9, 2021 19:40:13.306771040 CEST	49739	443	192.168.2.4	185.235.236.201
Apr 9, 2021 19:40:13.487991095 CEST	49746	443	192.168.2.4	185.235.236.197
Apr 9, 2021 19:40:13.487992048 CEST	49745	443	192.168.2.4	185.235.236.197
Apr 9, 2021 19:40:13.507533073 CEST	443	49746	185.235.236.197	192.168.2.4
Apr 9, 2021 19:40:13.507579088 CEST	443	49745	185.235.236.197	192.168.2.4
Apr 9, 2021 19:40:13.507647038 CEST	49746	443	192.168.2.4	185.235.236.197
Apr 9, 2021 19:40:13.507683992 CEST	49745	443	192.168.2.4	185.235.236.197
Apr 9, 2021 19:40:13.509135008 CEST	49746	443	192.168.2.4	185.235.236.197
Apr 9, 2021 19:40:13.509174109 CEST	49745	443	192.168.2.4	185.235.236.197
Apr 9, 2021 19:40:13.529141903 CEST	443	49746	185.235.236.197	192.168.2.4
Apr 9, 2021 19:40:13.529172897 CEST	443	49745	185.235.236.197	192.168.2.4
Apr 9, 2021 19:40:13.529211998 CEST	443	49746	185.235.236.197	192.168.2.4
Apr 9, 2021 19:40:13.529247999 CEST	443	49746	185.235.236.197	192.168.2.4
Apr 9, 2021 19:40:13.529279947 CEST	443	49746	185.235.236.197	192.168.2.4
Apr 9, 2021 19:40:13.529310942 CEST	49746	443	192.168.2.4	185.235.236.197
Apr 9, 2021 19:40:13.529314995 CEST	443	49745	185.235.236.197	192.168.2.4
Apr 9, 2021 19:40:13.529325962 CEST	49746	443	192.168.2.4	185.235.236.197
Apr 9, 2021 19:40:13.529361963 CEST	443	49745	185.235.236.197	192.168.2.4
Apr 9, 2021 19:40:13.529376030 CEST	49746	443	192.168.2.4	185.235.236.197
Apr 9, 2021 19:40:13.529439926 CEST	443	49745	185.235.236.197	192.168.2.4
Apr 9, 2021 19:40:13.529475927 CEST	49745	443	192.168.2.4	185.235.236.197
Apr 9, 2021 19:40:13.529510975 CEST	49745	443	192.168.2.4	185.235.236.197
Apr 9, 2021 19:40:13.529520035 CEST	49745	443	192.168.2.4	185.235.236.197
Apr 9, 2021 19:40:13.532749891 CEST	49745	443	192.168.2.4	185.235.236.197
Apr 9, 2021 19:40:13.532799006 CEST	49746	443	192.168.2.4	185.235.236.197
Apr 9, 2021 19:40:13.533411980 CEST	49746	443	192.168.2.4	185.235.236.197
Apr 9, 2021 19:40:13.553581953 CEST	443	49746	185.235.236.197	192.168.2.4
Apr 9, 2021 19:40:13.553633928 CEST	443	49745	185.235.236.197	192.168.2.4
Apr 9, 2021 19:40:13.553704977 CEST	49745	443	192.168.2.4	185.235.236.197
Apr 9, 2021 19:40:13.553723097 CEST	49746	443	192.168.2.4	185.235.236.197
Apr 9, 2021 19:40:13.592164040 CEST	443	49746	185.235.236.197	192.168.2.4
Apr 9, 2021 19:40:13.700006008 CEST	443	49746	185.235.236.197	192.168.2.4
Apr 9, 2021 19:40:13.700103045 CEST	49746	443	192.168.2.4	185.235.236.197
Apr 9, 2021 19:40:13.702545881 CEST	49746	443	192.168.2.4	185.235.236.197
Apr 9, 2021 19:40:13.719907999 CEST	443	49746	185.235.236.197	192.168.2.4
Apr 9, 2021 19:40:13.719927073 CEST	443	49746	185.235.236.197	192.168.2.4
Apr 9, 2021 19:40:14.001027107 CEST	443	49746	185.235.236.197	192.168.2.4
Apr 9, 2021 19:40:14.001044035 CEST	443	49746	185.235.236.197	192.168.2.4
Apr 9, 2021 19:40:14.001148939 CEST	49746	443	192.168.2.4	185.235.236.197
Apr 9, 2021 19:40:14.001183987 CEST	49746	443	192.168.2.4	185.235.236.197
Apr 9, 2021 19:40:14.477513075 CEST	49748	443	192.168.2.4	185.235.236.200
Apr 9, 2021 19:40:14.478152990 CEST	49749	443	192.168.2.4	185.235.236.200

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 9, 2021 19:40:00.264616966 CEST	54531	53	192.168.2.4	8.8.8.8
Apr 9, 2021 19:40:00.277681112 CEST	53	54531	8.8.8.8	192.168.2.4
Apr 9, 2021 19:40:01.245932102 CEST	49714	53	192.168.2.4	8.8.8.8
Apr 9, 2021 19:40:01.259212971 CEST	53	49714	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 9, 2021 19:40:02.261037111 CEST	58028	53	192.168.2.4	8.8.8.8
Apr 9, 2021 19:40:02.271034002 CEST	53097	53	192.168.2.4	8.8.8.8
Apr 9, 2021 19:40:02.273721933 CEST	53	58028	8.8.8.8	192.168.2.4
Apr 9, 2021 19:40:02.291922092 CEST	53	53097	8.8.8.8	192.168.2.4
Apr 9, 2021 19:40:02.906789064 CEST	49257	53	192.168.2.4	8.8.8.8
Apr 9, 2021 19:40:02.920991898 CEST	53	49257	8.8.8.8	192.168.2.4
Apr 9, 2021 19:40:03.731709003 CEST	62389	53	192.168.2.4	8.8.8.8
Apr 9, 2021 19:40:03.745975018 CEST	53	62389	8.8.8.8	192.168.2.4
Apr 9, 2021 19:40:05.100671053 CEST	49910	53	192.168.2.4	8.8.8.8
Apr 9, 2021 19:40:05.114511967 CEST	53	49910	8.8.8.8	192.168.2.4
Apr 9, 2021 19:40:06.242120981 CEST	55854	53	192.168.2.4	8.8.8.8
Apr 9, 2021 19:40:06.254987001 CEST	53	55854	8.8.8.8	192.168.2.4
Apr 9, 2021 19:40:07.347959042 CEST	64549	53	192.168.2.4	8.8.8.8
Apr 9, 2021 19:40:07.361588001 CEST	53	64549	8.8.8.8	192.168.2.4
Apr 9, 2021 19:40:07.613732100 CEST	63153	53	192.168.2.4	8.8.8.8
Apr 9, 2021 19:40:07.632381916 CEST	53	63153	8.8.8.8	192.168.2.4
Apr 9, 2021 19:40:08.014081001 CEST	52991	53	192.168.2.4	8.8.8.8
Apr 9, 2021 19:40:08.029352903 CEST	53	52991	8.8.8.8	192.168.2.4
Apr 9, 2021 19:40:08.661225080 CEST	53700	53	192.168.2.4	8.8.8.8
Apr 9, 2021 19:40:08.682404995 CEST	53	53700	8.8.8.8	192.168.2.4
Apr 9, 2021 19:40:08.940548897 CEST	51726	53	192.168.2.4	8.8.8.8
Apr 9, 2021 19:40:08.954715014 CEST	53	51726	8.8.8.8	192.168.2.4
Apr 9, 2021 19:40:09.197120905 CEST	56794	53	192.168.2.4	8.8.8.8
Apr 9, 2021 19:40:09.219883919 CEST	53	56794	8.8.8.8	192.168.2.4
Apr 9, 2021 19:40:12.013125896 CEST	56534	53	192.168.2.4	8.8.8.8
Apr 9, 2021 19:40:12.025569916 CEST	53	56534	8.8.8.8	192.168.2.4
Apr 9, 2021 19:40:13.155064106 CEST	56627	53	192.168.2.4	8.8.8.8
Apr 9, 2021 19:40:13.168973923 CEST	53	56627	8.8.8.8	192.168.2.4
Apr 9, 2021 19:40:13.459388971 CEST	56621	53	192.168.2.4	8.8.8.8
Apr 9, 2021 19:40:13.486084938 CEST	53	56621	8.8.8.8	192.168.2.4
Apr 9, 2021 19:40:14.343380928 CEST	63116	53	192.168.2.4	8.8.8.8
Apr 9, 2021 19:40:14.357645988 CEST	53	63116	8.8.8.8	192.168.2.4
Apr 9, 2021 19:40:14.441097021 CEST	64078	53	192.168.2.4	8.8.8.8
Apr 9, 2021 19:40:14.468913078 CEST	53	64078	8.8.8.8	192.168.2.4
Apr 9, 2021 19:40:17.056035042 CEST	64801	53	192.168.2.4	8.8.8.8
Apr 9, 2021 19:40:17.068676949 CEST	53	64801	8.8.8.8	192.168.2.4
Apr 9, 2021 19:40:17.809616089 CEST	61721	53	192.168.2.4	8.8.8.8
Apr 9, 2021 19:40:17.823206902 CEST	53	61721	8.8.8.8	192.168.2.4
Apr 9, 2021 19:40:18.546160936 CEST	51255	53	192.168.2.4	8.8.8.8
Apr 9, 2021 19:40:18.558936119 CEST	53	51255	8.8.8.8	192.168.2.4
Apr 9, 2021 19:40:19.399782896 CEST	61522	53	192.168.2.4	8.8.8.8
Apr 9, 2021 19:40:19.417651892 CEST	53	61522	8.8.8.8	192.168.2.4
Apr 9, 2021 19:40:20.354120016 CEST	52337	53	192.168.2.4	8.8.8.8
Apr 9, 2021 19:40:20.372322083 CEST	53	52337	8.8.8.8	192.168.2.4
Apr 9, 2021 19:40:21.009419918 CEST	55046	53	192.168.2.4	8.8.8.8
Apr 9, 2021 19:40:21.024245977 CEST	53	55046	8.8.8.8	192.168.2.4
Apr 9, 2021 19:40:25.773560047 CEST	49612	53	192.168.2.4	8.8.8.8
Apr 9, 2021 19:40:25.788463116 CEST	53	49612	8.8.8.8	192.168.2.4
Apr 9, 2021 19:40:29.673434019 CEST	49285	53	192.168.2.4	8.8.8.8
Apr 9, 2021 19:40:29.686013937 CEST	53	49285	8.8.8.8	192.168.2.4
Apr 9, 2021 19:40:30.826956034 CEST	50601	53	192.168.2.4	8.8.8.8
Apr 9, 2021 19:40:30.901876926 CEST	53	50601	8.8.8.8	192.168.2.4
Apr 9, 2021 19:40:31.301104069 CEST	60875	53	192.168.2.4	8.8.8.8
Apr 9, 2021 19:40:31.344579935 CEST	53	60875	8.8.8.8	192.168.2.4
Apr 9, 2021 19:40:32.189842939 CEST	56448	53	192.168.2.4	8.8.8.8
Apr 9, 2021 19:40:32.205826044 CEST	53	56448	8.8.8.8	192.168.2.4
Apr 9, 2021 19:40:36.030066013 CEST	59172	53	192.168.2.4	8.8.8.8
Apr 9, 2021 19:40:36.048909903 CEST	53	59172	8.8.8.8	192.168.2.4
Apr 9, 2021 19:40:37.599287033 CEST	62420	53	192.168.2.4	8.8.8.8
Apr 9, 2021 19:40:37.612315893 CEST	53	62420	8.8.8.8	192.168.2.4
Apr 9, 2021 19:40:38.258934975 CEST	60579	53	192.168.2.4	8.8.8.8
Apr 9, 2021 19:40:38.271790981 CEST	53	60579	8.8.8.8	192.168.2.4
Apr 9, 2021 19:40:38.612457037 CEST	62420	53	192.168.2.4	8.8.8.8
Apr 9, 2021 19:40:38.626830101 CEST	53	62420	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 9, 2021 19:40:39.267400026 CEST	60579	53	192.168.2.4	8.8.8.8
Apr 9, 2021 19:40:39.282589912 CEST	53	60579	8.8.8.8	192.168.2.4
Apr 9, 2021 19:40:39.627219915 CEST	62420	53	192.168.2.4	8.8.8.8
Apr 9, 2021 19:40:39.639832973 CEST	53	62420	8.8.8.8	192.168.2.4
Apr 9, 2021 19:40:40.318718910 CEST	60579	53	192.168.2.4	8.8.8.8
Apr 9, 2021 19:40:40.332087994 CEST	53	60579	8.8.8.8	192.168.2.4
Apr 9, 2021 19:40:41.642400026 CEST	62420	53	192.168.2.4	8.8.8.8
Apr 9, 2021 19:40:41.655910015 CEST	53	62420	8.8.8.8	192.168.2.4
Apr 9, 2021 19:40:42.314651012 CEST	60579	53	192.168.2.4	8.8.8.8
Apr 9, 2021 19:40:42.327291012 CEST	53	60579	8.8.8.8	192.168.2.4
Apr 9, 2021 19:40:45.658334017 CEST	62420	53	192.168.2.4	8.8.8.8
Apr 9, 2021 19:40:45.671049118 CEST	53	62420	8.8.8.8	192.168.2.4
Apr 9, 2021 19:40:46.330313921 CEST	60579	53	192.168.2.4	8.8.8.8
Apr 9, 2021 19:40:46.344769955 CEST	53	60579	8.8.8.8	192.168.2.4
Apr 9, 2021 19:40:47.598186970 CEST	50183	53	192.168.2.4	8.8.8.8
Apr 9, 2021 19:40:47.611006021 CEST	53	50183	8.8.8.8	192.168.2.4
Apr 9, 2021 19:40:48.028372049 CEST	61531	53	192.168.2.4	8.8.8.8
Apr 9, 2021 19:40:48.041064978 CEST	53	61531	8.8.8.8	192.168.2.4
Apr 9, 2021 19:40:48.514560938 CEST	49228	53	192.168.2.4	8.8.8.8
Apr 9, 2021 19:40:48.527401924 CEST	53	49228	8.8.8.8	192.168.2.4
Apr 9, 2021 19:40:48.854758024 CEST	59794	53	192.168.2.4	8.8.8.8
Apr 9, 2021 19:40:48.867476940 CEST	53	59794	8.8.8.8	192.168.2.4
Apr 9, 2021 19:40:48.889524937 CEST	55916	53	192.168.2.4	8.8.8.8
Apr 9, 2021 19:40:48.902061939 CEST	53	55916	8.8.8.8	192.168.2.4
Apr 9, 2021 19:40:49.311681032 CEST	52752	53	192.168.2.4	8.8.8.8
Apr 9, 2021 19:40:49.325030088 CEST	53	52752	8.8.8.8	192.168.2.4
Apr 9, 2021 19:40:49.758795023 CEST	60542	53	192.168.2.4	8.8.8.8
Apr 9, 2021 19:40:49.771728039 CEST	53	60542	8.8.8.8	192.168.2.4
Apr 9, 2021 19:40:50.203191996 CEST	60689	53	192.168.2.4	8.8.8.8
Apr 9, 2021 19:40:50.215749979 CEST	53	60689	8.8.8.8	192.168.2.4
Apr 9, 2021 19:40:50.789213896 CEST	64206	53	192.168.2.4	8.8.8.8
Apr 9, 2021 19:40:50.804688931 CEST	53	64206	8.8.8.8	192.168.2.4
Apr 9, 2021 19:40:51.492253065 CEST	50904	53	192.168.2.4	8.8.8.8
Apr 9, 2021 19:40:51.507811069 CEST	53	50904	8.8.8.8	192.168.2.4
Apr 9, 2021 19:40:52.003351927 CEST	57525	53	192.168.2.4	8.8.8.8
Apr 9, 2021 19:40:52.016809940 CEST	53	57525	8.8.8.8	192.168.2.4
Apr 9, 2021 19:40:56.224081039 CEST	53814	53	192.168.2.4	8.8.8.8
Apr 9, 2021 19:40:56.237498045 CEST	53	53814	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 9, 2021 19:40:08.661225080 CEST	192.168.2.4	8.8.8.8	0x97da	Standard query (0)	app.box.com	A (IP address)	IN (0x0001)
Apr 9, 2021 19:40:09.197120905 CEST	192.168.2.4	8.8.8.8	0xeda	Standard query (0)	cdn01.boxcdn.net	A (IP address)	IN (0x0001)
Apr 9, 2021 19:40:13.459388971 CEST	192.168.2.4	8.8.8.8	0x8f46	Standard query (0)	api.box.com	A (IP address)	IN (0x0001)
Apr 9, 2021 19:40:14.441097021 CEST	192.168.2.4	8.8.8.8	0x3557	Standard query (0)	public.box cloud.com	A (IP address)	IN (0x0001)
Apr 9, 2021 19:40:25.773560047 CEST	192.168.2.4	8.8.8.8	0x1889	Standard query (0)	cdn01.boxcdn.net	A (IP address)	IN (0x0001)
Apr 9, 2021 19:40:30.826956034 CEST	192.168.2.4	8.8.8.8	0xbf05	Standard query (0)	955b0f04ec 1842b79e67 27b6d5210d e0.svc.dyn amics.com	A (IP address)	IN (0x0001)
Apr 9, 2021 19:40:31.301104069 CEST	192.168.2.4	8.8.8.8	0x9b5e	Standard query (0)	erffggf.cf	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 9, 2021 19:40:08.682404995 CEST	8.8.8.8	192.168.2.4	0x97da	No error (0)	app.box.com		185.235.236.201	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 9, 2021 19:40:09.219883919 CEST	8.8.8.8	192.168.2.4	0xeda	No error (0)	cdn01.boxcdn.net	cdn01.boxcdn.net.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Apr 9, 2021 19:40:13.486084938 CEST	8.8.8.8	192.168.2.4	0x8f46	No error (0)	api.box.com		185.235.236.197	A (IP address)	IN (0x0001)
Apr 9, 2021 19:40:14.468913078 CEST	8.8.8.8	192.168.2.4	0x3557	No error (0)	public.boxcloud.com		185.235.236.200	A (IP address)	IN (0x0001)
Apr 9, 2021 19:40:25.788463116 CEST	8.8.8.8	192.168.2.4	0x1889	No error (0)	cdn01.boxcdn.net	cdn01.boxcdn.net.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Apr 9, 2021 19:40:30.901876926 CEST	8.8.8.8	192.168.2.4	0xbf05	No error (0)	955b0f04ec1842b79e6727b6d5210de0.svc.dynamics.com	mktsvcp102ne001.svc.dynamics.com		CNAME (Canonical name)	IN (0x0001)
Apr 9, 2021 19:40:30.901876926 CEST	8.8.8.8	192.168.2.4	0xbf05	No error (0)	mktsvcp102ne001.svc.dynamics.com	mktsvcp102ne001.northeurope.cloudapp.azure.com		CNAME (Canonical name)	IN (0x0001)
Apr 9, 2021 19:40:31.344579935 CEST	8.8.8.8	192.168.2.4	0x9b5e	No error (0)	erffggf.cf		198.54.125.84	A (IP address)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 9, 2021 19:40:08.747746944 CEST	185.235.236.201	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	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	Fri Jan 15 01:00:00 CET 2021	Fri Jan 14 00:59:59 CET 2022	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=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		
Apr 9, 2021 19:40:08.747829914 CEST	185.235.236.201	443	192.168.2.4	49738	CN=box.com, O="Box, Inc.", L=Redwood City, ST=California, C=US CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Jan 15 01:00:00 CET 2021	Fri Jan 14 00:59:59 CET 2022	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=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		
Apr 9, 2021 19:40:13.529279947 CEST	185.235.236.197	443	192.168.2.4	49746	CN=box.com, O="Box, Inc.", L=Redwood City, ST=California, C=US CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Jan 15 01:00:00 CET 2021	Fri Jan 14 00:59:59 CET 2022	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=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
Apr 9, 2021 19:40:13.529439926 CEST	185.235.236.197	443	192.168.2.4	49745	CN=box.com, O="Box, Inc.", L=Redwood City, ST=California, C=US CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Jan 15 01:00:00 CET 2021 Mon Nov 06 13:23:45 CET 2017	Fri Jan 14 00:59:59 CET 2022 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		
Apr 9, 2021 19:40:14.519754887 CEST	185.235.236.200	443	192.168.2.4	49748	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	Thu Feb 18 01:00:00 CET 2021 Mon Nov 06 13:23:45 CET 2017	Thu Feb 17 00:59:59 CET 2022 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		
Apr 9, 2021 19:40:14.521554947 CEST	185.235.236.200	443	192.168.2.4	49749	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	Thu Feb 18 01:00:00 CET 2021 Mon Nov 06 13:23:45 CET 2017	Thu Feb 17 00:59:59 CET 2022 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		
Apr 9, 2021 19:40:31.700187922 CEST	198.54.125.84	443	192.168.2.4	49763	CN=erffggf.cf CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Fri Apr 09 02:00:00 CEST 2021 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Sun Apr 10 01:59:59 CEST 2022 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 9, 2021 19:40:31.703378916 CEST	198.54.125.84	443	192.168.2.4	49762	CN=erffggf.cf CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Fri Apr 09 02:00:00 CEST 2021 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Sun Apr 10 01:59:59 CEST 2022 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 6644 Parent PID: 800

General

Start time:	19:40:06
Start date:	09/04/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false

Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff7c5250000
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: 6752 Parent PID: 6644

General

Start time:	19:40:07
Start date:	09/04/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6644 CREDAT:17410 /prefetch:2
Imagebase:	0x12f0000
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