ID: 323781
Sample Name: Direct Deposit.xlsx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 14:45:42
Date: 27/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

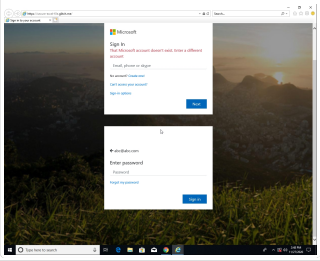
Analysis Report Direct Deposit.xlsx

Overview

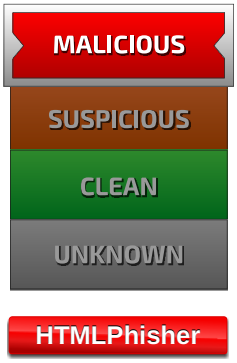
General Information

Sample Name:	Direct Deposit.xlsx
Analysis ID:	323781
MD5:	69e51c55e817ad..
SHA1:	0385a74d84fbf89..
SHA256:	c38e8675fe9efcc...
Tags:	xlsx

Most interesting Screenshot:



Detection

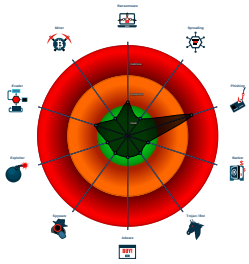


Score:	56
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Yara detected HtmlPhish_10
- IP address seen in connection with o...
- JA3 SSL client fingerprint seen in co...

Classification



Startup

- **System is w10x64**
- EXCEL.EXE (PID: 6684 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
- iexplore.exe (PID: 4900 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 4280 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4900 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 7040 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4900 CREDAT:17414 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

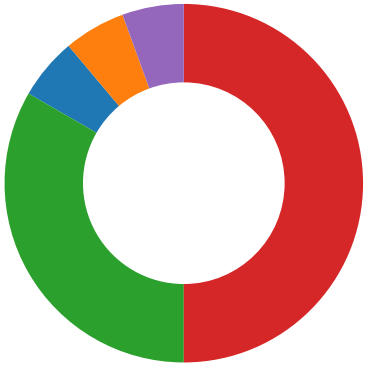
Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\5O11KYTY.htm	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Phishing
- Networking
- System Summary
- Hooking and other Techniques for Hiding and Protection

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

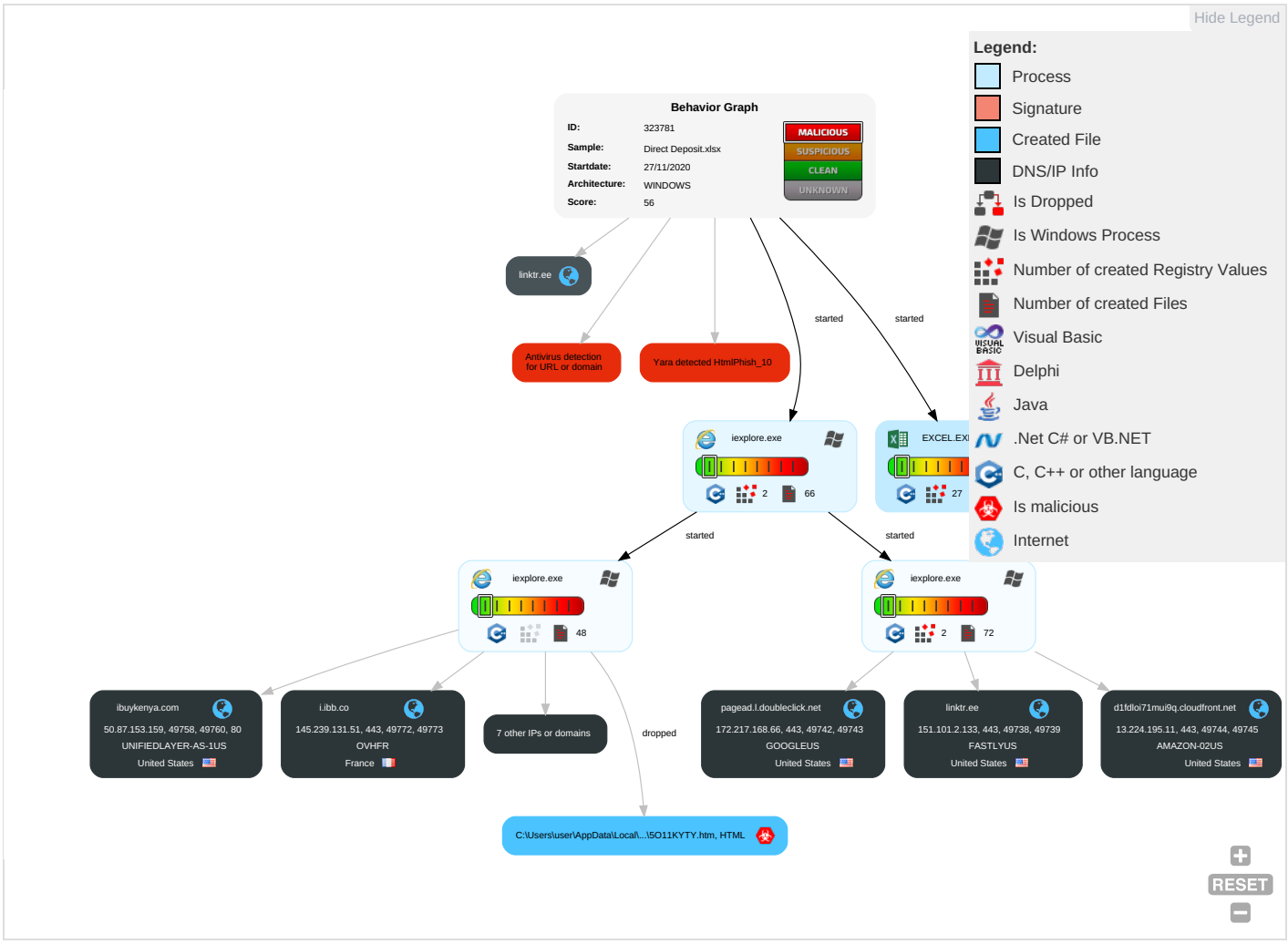
Phishing:

Yara detected HtmlPhish_10

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	Impa
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 Partit
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	System Information Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 2	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Devic Lock
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 3	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delet Devic Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Ingress Tool Transfer 1	SIM Card Swap		Carri Billin Fraud

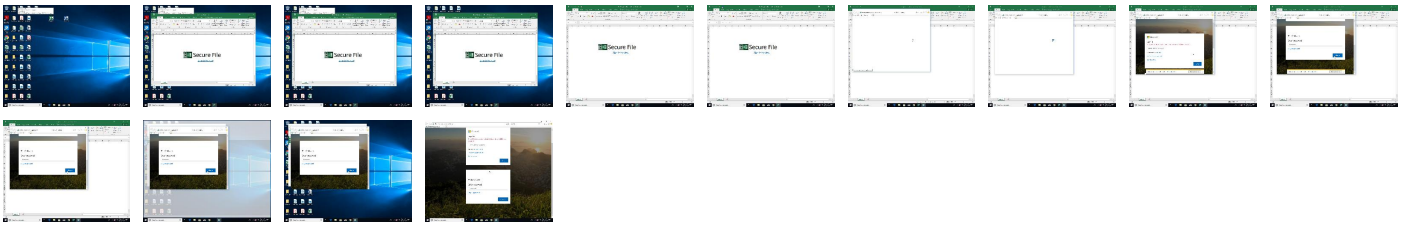
Behavior Graph

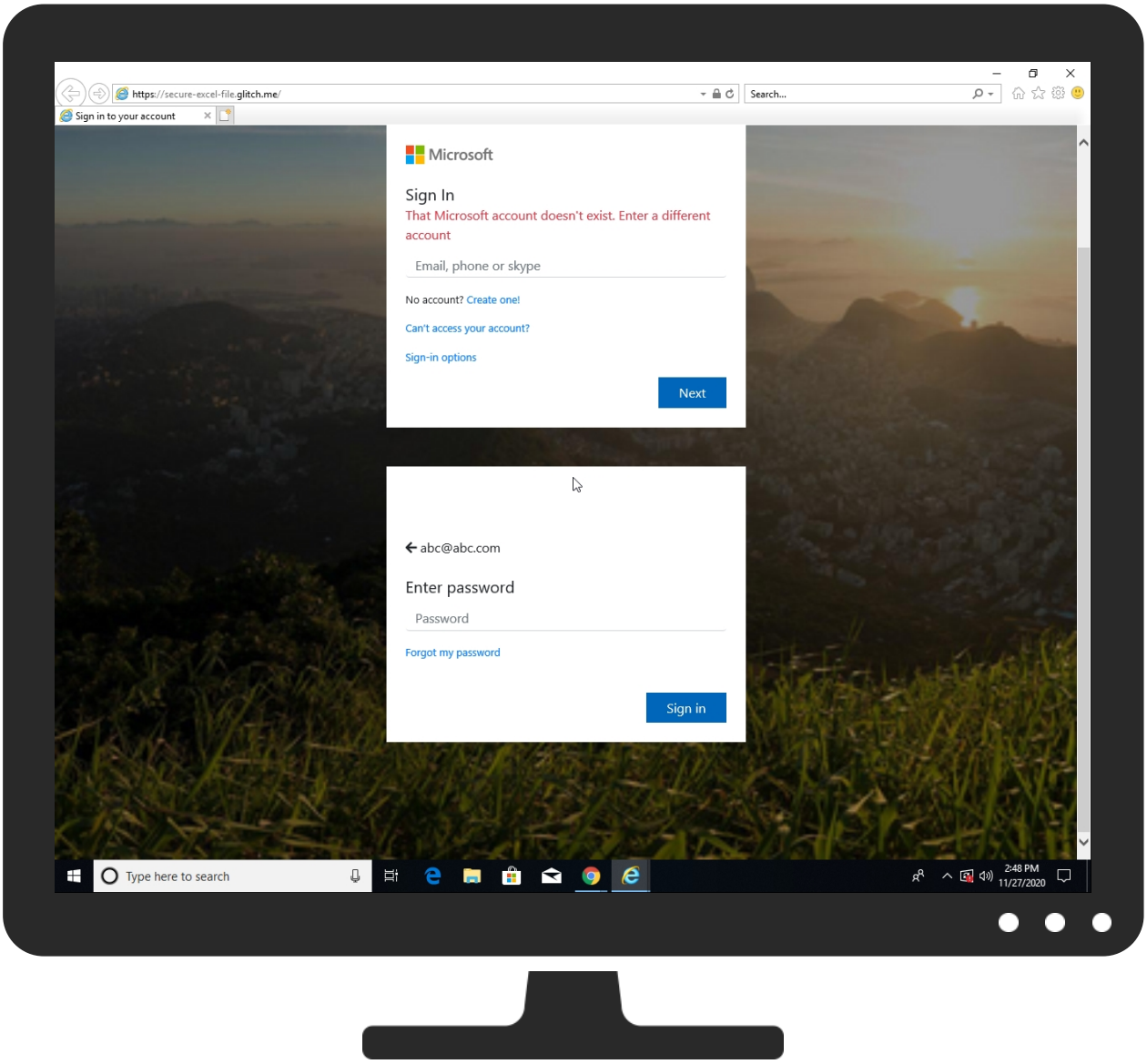


Screenshots

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
Direct Deposit.xlsx	0%	Virustotal		Browse
Direct Deposit.xlsx	0%	ReversingLabs		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
ibuykenya.com	1%	Virustotal		Browse
secure.aadcdn.microsoftonline-p.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link

Source	Detection	Scanner	Label	Link
http://https://secure-excel-file.glitch.me/	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://https://secure-excel-file.glitch.me/	100%	UrlScan	phishing brand: generic microsoft	Browse
http://ibuykenya.com/vendor/doctrine/styles.css	1%	Virustotal		Browse
http://ibuykenya.com/vendor/doctrine/styles.css	0%	Avira URL Cloud	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://fontawesome.comhttps://fontawesome.comFont	0%	Avira URL Cloud	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	Avira URL Cloud	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://promisesaplus.com/#point-59	0%	URL Reputation	safe	
http://https://promisesaplus.com/#point-59	0%	URL Reputation	safe	
http://https://promisesaplus.com/#point-59	0%	URL Reputation	safe	
http://https://promisesaplus.com/#point-57	0%	URL Reputation	safe	
http://https://promisesaplus.com/#point-57	0%	URL Reputation	safe	
http://https://promisesaplus.com/#point-57	0%	URL Reputation	safe	
http://https://promisesaplus.com/#point-54	0%	URL Reputation	safe	
http://https://promisesaplus.com/#point-54	0%	URL Reputation	safe	
http://https://promisesaplus.com/#point-54	0%	URL Reputation	safe	
http://https://secure.aadcdn.microsoftonline-p.com/ests/2.1.8576.13/content/images/microsoft_logo_ee5c8d9fb	0%	Avira URL Cloud	safe	
http://https://getbootstrap.com)	0%	Avira URL Cloud	safe	
http://https://promisesaplus.com/#point-48	0%	URL Reputation	safe	
http://https://promisesaplus.com/#point-48	0%	URL Reputation	safe	
http://https://promisesaplus.com/#point-48	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
linktr.ee	151.101.2.133	true	false		high
ibuykenya.com	50.87.153.159	true	false	• 1%, Virustotal, Browse	unknown
secure-excel-file.glitch.me	34.231.129.212	true	false		high
pagead.l.doubleclick.net	172.217.168.66	true	false		high
cdnjs.cloudflare.com	104.16.19.94	true	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
d1fdloi71mui9q.cloudfront.net	13.224.195.11	true	false		high
i.ibb.co	145.239.131.51	true	false		high
secure.aadcdn.microsoftonline-p.com	unknown	unknown	false	• 0%, Virustotal, Browse	unknown
ka-f.fontawesome.com	unknown	unknown	false		high
code.jquery.com	unknown	unknown	false		high
kit.fontawesome.com	unknown	unknown	false		high
maxcdn.bootstrapcdn.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://ibuykenya.com/vendor/doctrine/styles.css	false	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://secure-excel-file.glitch.me/	false	• 100%, UrlScan, Browse • SlashNext: Fake Login Page type: Phishing & Social Engineering	high

URLs from Memory and Binaries

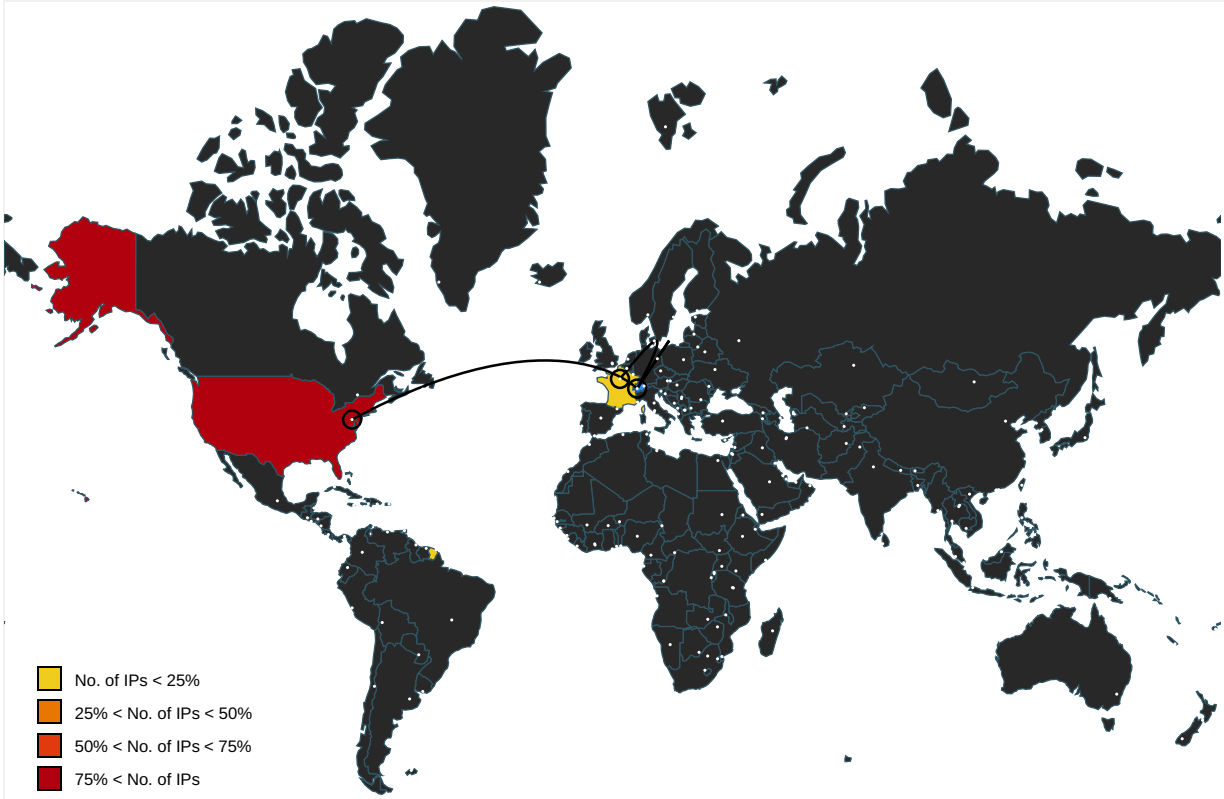
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://shell.suite.office.com:1443	1ED43371-383F-4AFE-8A72-9D45E7252268.0.dr	false		high
http://https://code.jquery.com/jquery-3.2.1.slim.min.js	5O11KYTY.htm.20.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	1ED43371-383F-4AFE-8A72-9D45E7252268.0.dr	false		high
http://https://cdn.entity.	1ED43371-383F-4AFE-8A72-9D45E7252268.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	1ED43371-383F-4AFE-8A72-9D45E7252268.0.dr	false		high
http://https://web.archive.org/web/20100324014747/blindsignals.com/index.php/2009/07/jquery-delay/	jquery-3.3.1[1].js.20.dr	false		high
http://https://rpsticket.partnerservices.getmicrosoftkey.com	1ED43371-383F-4AFE-8A72-9D45E7252268.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	1ED43371-383F-4AFE-8A72-9D45E7252268.0.dr	false		high
http://https://fontawesome.comhttps://fontawesome.comFont	free-fa-regular-400[1].eot.20.dr, free-fa-solid-900[1].eot.20.dr	false	• Avira URL Cloud: safe	unknown
http://https://html.spec.whatwg.org/multipage/forms.html#concept-fe-disabled	jquery-3.3.1[1].js.20.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	1ED43371-383F-4AFE-8A72-9D45E7252268.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	1ED43371-383F-4AFE-8A72-9D45E7252268.0.dr	false		high
http://https://api.aadrm.com/	1ED43371-383F-4AFE-8A72-9D45E7252268.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://infra.spec.whatwg.org/#strip-and-collapse-ascii-whitespace	jquery-3.3.1[1].js.20.dr	false		high
http://https://fontawesome.com	free-fa-regular-400[1].eot.20.dr, free-v4-shims.min[1].css.20.dr	false		high
http://https://github.com/twbs/bootstrap/graphs/contributors)	bootstrap.min[1].js.20.dr	false		high
http://https://github.com/jrburke/requirejs/wiki/Updating-existing-libraries#wiki-anon	jquery-3.3.1[1].js.20.dr	false		high
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	1ED43371-383F-4AFE-8A72-9D45E7252268.0.dr	false		high
http://https://api.microsoftstream.com/api/	1ED43371-383F-4AFE-8A72-9D45E7252268.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	1ED43371-383F-4AFE-8A72-9D45E7252268.0.dr	false		high
http://https://cr.office.com	1ED43371-383F-4AFE-8A72-9D45E7252268.0.dr	false		high
http://https://bugzilla.mozilla.org/show_bug.cgi?id=687787	jquery-3.3.1[1].js.20.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://bugs.chromium.org/p/chromium/issues/detail?id=470258	jquery-3.3.1[1].js.20.dr	false		high
http://https://kit.fontawesome.com/585b051251.js	5O11KYTY.htm.20.dr	false		high
http://https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/js/bootstrap.min.js	5O11KYTY.htm.20.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	1ED43371-383F-4AFE-8A72-9D45E7252268.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	1ED43371-383F-4AFE-8A72-9D45E7252268.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	1ED43371-383F-4AFE-8A72-9D45E7252268.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://store.office.cn/addinstemplate	1ED43371-383F-4AFE-8A72-9D45E7252268.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://wus2-000.pagecontentsync.	1ED43371-383F-4AFE-8A72-9D45E7252268.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	1ED43371-383F-4AFE-8A72-9D45E7252268.0.dr	false		high
http://https://www.odwebp.svc.ms	1ED43371-383F-4AFE-8A72-9D45E7252268.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://jsperf.com/getall-vs-sizzle/2	jquery-3.3.1[1].js.20.dr	false		high
http://https://api.powerbi.com/v1.0/myorg/groups	1ED43371-383F-4AFE-8A72-9D45E7252268.0.dr	false		high
http://https://web.microsoftstream.com/video/	1ED43371-383F-4AFE-8A72-9D45E7252268.0.dr	false		high
http://https://graph.windows.net	1ED43371-383F-4AFE-8A72-9D45E7252268.0.dr	false		high
http://https://linktr.ee/static/favicon.png.	imagestore.dat.19.dr	false		high
http://https://www.office.com/?auth=2	5O11KYTY.htm.20.dr	false		high
http://https://jquery.com/	jquery-3.3.1[1].js.20.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	1ED43371-383F-4AFE-8A72-9D45E7252268.0.dr	false		high
http://https://linktr.ee/excel.O365.securefile	{886E4481-3102-11EB-90E4-ECF4BB862DED}.dat.18.dr	false		high
http://https://github.com/twbs/bootstrap/blob/master/LICENSE)	bootstrap.min[1].css.20.dr, bootstrap.min[1].js.20.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	1ED43371-383F-4AFE-8A72-9D45E7252268.0.dr	false		high
http://weather.service.msn.com/data.aspx	1ED43371-383F-4AFE-8A72-9D45E7252268.0.dr	false		high
http://https://sizzlejs.com/	jquery-3.3.1[1].js.20.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	1ED43371-383F-4AFE-8A72-9D45E7252268.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	1ED43371-383F-4AFE-8A72-9D45E7252268.0.dr	false		high
http://www.imagemagick.org	imagestore.dat.19.dr	false		high
http://https://secure-excel-file.glitch.me/.Sign	{886E4483-3102-11EB-90E4-ECF4BB862DED}.dat.18.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	1ED43371-383F-4AFE-8A72-9D45E7252268.0.dr	false		high
http://https://ka-f.fontawesome.com	585b051251[1].js.20.dr	false		high
http://https://linktr.ee/excel.O365.securefile6Excel	{886E4481-3102-11EB-90E4-ECF4BB862DED}.dat.18.dr	false		high
http://https://bugs.jquery.com/ticket/12359	jquery-3.3.1[1].js.20.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	1ED43371-383F-4AFE-8A72-9D45E7252268.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	1ED43371-383F-4AFE-8A72-9D45E7252268.0.dr	false		high
http://https://d1fdloi71mui9q.cloudfront.net/YS99cwPS1yJGdXcJU31Y_62xa7aqirVCeh6yn);background-image:url(ht	excel.O365[1].htm.19.dr	false		high
http://https://linktr.ee/excel.O365.securefileRoot	{886E4481-3102-11EB-90E4-ECF4BB862DED}.dat.18.dr	false		high
http://https://secure-excel-file.glitch.me/	{886E4483-3102-11EB-90E4-ECF4BB862DED}.dat.18.dr	false	• 100%, UrlScan, Browse • SlashNext: Fake Login Page type: Phishing & Social Engineering	high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://clients.config.office.net/user/v1.0/android/policies	1ED43371-383F-4AFE-8A72-9D45E7252268.0.dr	false		high
http://https://entitlement.diagnostics.office.com	1ED43371-383F-4AFE-8A72-9D45E7252268.0.dr	false		high
http://https://linktr.ee/excel.O365.securefile6Excell.O365.securefileRoot	{886E4481-3102-11EB-90E4-ECF4BB862DED}.dat.18.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	1ED43371-383F-4AFE-8A72-9D45E7252268.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	1ED43371-383F-4AFE-8A72-9D45E7252268.0.dr	false		high
http://https://fontawesome.com/license/free	free-v4-shims.min[1].css.20.dr	false		high
http://https://github.com/jquery/jquery/pull/557)	jquery-3.3.1[1].js.20.dr	false		high
http://https://bugs.chromium.org/p/chromium/issues/detail?id=378607	jquery-3.3.1[1].js.20.dr	false		high
http://https://secure-excel-file.glitch.me/Root	{886E4483-3102-11EB-90E4-ECF4BB862DED}.dat.18.dr	false		high
http://https://graph.windows.net/	1ED43371-383F-4AFE-8A72-9D45E7252268.0.dr	false		high
http://https://devnull.onenote.com	1ED43371-383F-4AFE-8A72-9D45E7252268.0.dr	false		high
http://https://messaging.office.com/	1ED43371-383F-4AFE-8A72-9D45E7252268.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	1ED43371-383F-4AFE-8A72-9D45E7252268.0.dr	false		high
http://https://skyapi.live.net/Activity/	1ED43371-383F-4AFE-8A72-9D45E7252268.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://drafts.csswg.org/cssom/#resolved-values	jquery-3.3.1[1].js.20.dr	false		high
http://https://bugs.chromium.org/p/chromium/issues/detail?id=589347	jquery-3.3.1[1].js.20.dr	false		high
http://https://visio.uservoice.com/forums/368202-visio-on-devices	1ED43371-383F-4AFE-8A72-9D45E7252268.0.dr	false		high
http://https://code.jquery.com/jquery-3.1.1.min.js	5O11KYTY.htm.20.dr	false		high
http://https://onedrive.live.com/embed?	1ED43371-383F-4AFE-8A72-9D45E7252268.0.dr	false		high
http://https://augloop.office.com	1ED43371-383F-4AFE-8A72-9D45E7252268.0.dr	false		high
http://https://html.spec.whatwg.org/multipage/syntax.html#attributes-2	jquery-3.3.1[1].js.20.dr	false		high
http://https://promisesaplus.com/#point-59	jquery-3.3.1[1].js.20.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://promisesaplus.com/#point-57	jquery-3.3.1[1].js.20.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://github.com/eslint/eslint/issues/3229	jquery-3.3.1[1].js.20.dr	false		high
http://https://promisesaplus.com/#point-54	jquery-3.3.1[1].js.20.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://code.jquery.com/jquery-3.3.1.js	5O11KYTY.htm.20.dr	false		high
http://https://secure.aadcdn.microsoftonline-p.com/ests/2.1.8576.13/content/images/microsoft_logo_ee5c8d9fb	5O11KYTY.htm.20.dr	false	• Avira URL Cloud: safe	unknown
http://https://html.spec.whatwg.org/multipage/scripting.html#selector-disabled	jquery-3.3.1[1].js.20.dr	false		high
http://https://api.diagnostics.office.com	1ED43371-383F-4AFE-8A72-9D45E7252268.0.dr	false		high
http://https://jquery.org/license	jquery-3.3.1[1].js.20.dr	false		high
http://https://store.office.de/addinstemplate	1ED43371-383F-4AFE-8A72-9D45E7252268.0.dr	false		high
http://https://getbootstrap.com)	bootstrap.min[1].css.20.dr, bootstrap.min[1].js.20.dr	false	• Avira URL Cloud: safe	low
http://https://api.powerbi.com/v1.0/myorg/datasets	1ED43371-383F-4AFE-8A72-9D45E7252268.0.dr	false		high
http://https://bugs.webkit.org/show_bug.cgi?id=137337	jquery-3.3.1[1].js.20.dr	false		high
http://https://html.spec.whatwg.org/multipage/scripting.html#selector-enabled	jquery-3.3.1[1].js.20.dr	false		high
http://https://promisesaplus.com/#point-48	jquery-3.3.1[1].js.20.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://logo.clearbit.com/	5O11KYTY.htm.20.dr	false		high
http://https://secure-excel-file.glitch.me/erop4294967295	~DFA61C54DA1C9AEE49.TMP.18.dr	false		high
http://https://api.diagnosticssdf.office.com	1ED43371-383F-4AFE-8A72-9D45E7252268.0.dr	false		high
http://https://login.microsoftonline.com/	1ED43371-383F-4AFE-8A72-9D45E7252268.0.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
34.231.129.212	unknown	United States		14618	AMAZON-AESUS	false
145.239.131.51	unknown	France		16276	OVHFR	false
50.87.153.159	unknown	United States		46606	UNIFIEDLAYER-AS-1US	false
151.101.2.133	unknown	United States		54113	FASTLYUS	false
172.217.168.66	unknown	United States		15169	GOOGLEUS	false
13.224.195.11	unknown	United States		16509	AMAZON-02US	false
104.16.19.94	unknown	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	323781
Start date:	27.11.2020
Start time:	14:45:42
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 36s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Direct Deposit.xlsx
Cookbook file name:	defaultwindowsofficecookbook.jbs

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
Run name:	Potential for more IOCs and behavior
Number of analysed new started processes analysed:	27
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 • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal56.phis.winXLSX@6/65@12/7
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsx • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Browse link: https://linktr.ee/excel.O365.securefile • Scroll down • Close Viewer • Browsing link: https://secure-excel-file.glitch.me/

Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 52.255.188.83, 104.43.139.144, 204.79.197.200, 13.107.21.200, 52.109.88.177, 52.109.88.38, 52.109.12.21, 51.11.168.160, 104.43.193.48, 92.122.213.194, 92.122.213.247, 23.210.248.85, 13.64.90.137, 20.54.26.129, 51.104.139.180, 104.108.39.131, 216.58.215.234, 172.217.168.8, 172.217.168.3, 209.197.3.24, 209.197.3.15, 104.18.22.52, 104.18.23.52, 92.122.39.6, 172.64.203.28, 172.64.202.28, 152.199.19.161 • Excluded domains from analysis (whitelisted): gstaticadssl.l.google.com, cds.s5x3j6q5.hwcdn.net, prod-w.nexus.live.com.akadns.net, arc.msn.com.nsatc.net, www.googleadservices.com, ka-f.fontawesome.com.cdn.cloudflare.net, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, go.microsoft.com, www.googletagmanager.com, www-bing-com.dual-a-0001.a-msedge.net, e13761.dscg.akamaiedge.net, nexus.officeapps.live.com, officeclient.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, www.bing.com, kit.fontawesome.com.cdn.cloudflare.net, skypedataprdcolwus17.cloudapp.net, fonts.googleapis.com, fs.microsoft.com, dual-a-0001.a-msedge.net, fonts.gstatic.com, ajax.googleapis.com, ie9comview.vo.msecnd.net, prod.configsvc1.live.com.akadns.net, db3p-ris-pf-prod-atm.trafficmanager.net, www-googletagmanager.l.google.com, secure.aadcdn.microsoftonline-p.com.edgekey.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, skypedataprdcolcus16.cloudapp.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, config.officeapps.live.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, cds.j3z9t3p6.hwcdn.net, europe.configsvc1.live.com.akadns.net, cs9.wpc.v0cdn.net • Report size getting too big, too many NtDeviceIoControlFile calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
34.231.129.212	http://https://www.change.org/p/retire-dogs-cats-monkeys-from-u-s-government-labs-givethemback/u/24450590?cs_tk=Aq3W7_HddGjbN9snv1wAAXicyyvNyQEABF8BvKhdVW63xQ22RV7AG4rJi7k%3D&utm_campaign=65ff8cc89eba417b9042eb54db31169d&utm_medium=email&utm_source=petition_update&utm_term=cs	Get hash	malicious	Browse	
50.87.153.159	Direct Deposit.xlsx	Get hash	malicious	Browse	• ibuykenya.com/vendor/doctrine/styles.css
	Cleared_Payment_Notification_1588-5755.HTml	Get hash	malicious	Browse	• ibuykenya.com/vendor/doctrine/styles.css
	Outward_Swift_Confirmation_1503.htML	Get hash	malicious	Browse	• ibuykenya.com/vendor/doctrine/styles.css
	Cleared_Order_Notification_natwest.HTML	Get hash	malicious	Browse	• ibuykenya.com/vendor/doctrine/styles.css
	Swift_Payment_Notification_9530-008_.Html	Get hash	malicious	Browse	• ibuykenya.com/vendor/doctrine/styles.css
	http://https://u4718414.ct.sendgrid.net/ls/click?upn=Z1kQAFopiApyAMkH2FlexXDA-2BLE-2BiMfN-2B6WYbaQXXU5ne-2BFVeSiBTVuWH5JgyQxoc_ge_fgghTLC1drLvtu2vN8DyOA2wcBtMZDKgrNNYfnOK1M-2F2sJcIWacwxf41PdlltZuKCDTDX9lriBog1LoLAGz59LzA-2BLetPJGVwgaPwPI1mVsMYvlORvTrEjTxbJlktGedna45JgjD-2FSysb5lide33oA7YC0mDPDeGx7yS0FrMuEypMV0hvS9KRJ9jdgyGjl1lTLbBGoxLfEKn5xKBHJg5hSX-2BRJlyfA86CPkDhkUTTBg-3D	Get hash	malicious	Browse	• ibuykenya.com/vendor/doctrine/styles.css
	Remittance_Advice_00124452.html	Get hash	malicious	Browse	• ibuykenya.com/vendor/doctrine/styles.css
	Swift_Payment_Notification_4418-567_.Html	Get hash	malicious	Browse	• ibuykenya.com/vendor/doctrine/styles.css
	Cleared_Payment_Notification_1930-2989-223_.Html	Get hash	malicious	Browse	• ibuykenya.com/vendor/doctrine/styles.css
	Cleared_Payment_Notification_8175-7991-6045_.Html	Get hash	malicious	Browse	• ibuykenya.com/vendor/doctrine/styles.css
	Outward_Swift_Confirmation_7404-6045_.Html	Get hash	malicious	Browse	• ibuykenya.com/vendor/doctrine/styles.css
	Swift_pdf.htML	Get hash	malicious	Browse	• ibuykenya.com/vendor/doctrine/styles.css
	Aggiornamento_su_pagamento_90344_pdf.htML	Get hash	malicious	Browse	• ibuykenya.com/vendor/doctrine/styles.css
	http://jeevanmate.com/assets/plugins/bootstrap-modal/img/_vti_cnf/CO7221619133069235401.zip	Get hash	malicious	Browse	• jeevanmate.com/assets/plugins/bootstrap-modal/img/_vti_cnf/CO7221619133069235401.zip
151.101.2.133	http://resources.digital-cloud.medallia.ca	Get hash	malicious	Browse	• resources.digital-cloud.medallia.ca/
	http://assertoolersa.tk	Get hash	malicious	Browse	• secure2.alphassl.com/cacert/gsalphasha2g2r1.crt

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://tedia.com/laboratory/global-research-part1/feature-article-73/index.html	Get hash	malicious	Browse	• secure2.alphassl.com/cacert/gsalphasha2g2r1.crt

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ibuykenya.com	Direct Deposit.xlsx	Get hash	malicious	Browse	• 50.87.153.159
	Cleared_Payment_Notification_1588-5755.HTml	Get hash	malicious	Browse	• 50.87.153.159
	Outward_Swift_Confirmation_1503.htML	Get hash	malicious	Browse	• 50.87.153.159
	Cleared_Order_Notification_natwest.HTML	Get hash	malicious	Browse	• 50.87.153.159
	Swift_Payment_Notification_9530-008_.Html	Get hash	malicious	Browse	• 50.87.153.159
	http://https://u4718414.ct.sendgrid.net/ls/click?upn=Z1kQAFopiApyAMkH2FlexXDA-2BLE-2BiMfN-2B6WYbaQXXU5ne-2BFVeSiBTVuWH5JgyQxoc_ge_fgghTLC1drLvtu2vN8DyOA2wcBtMZDKgrNNYfnOK1M-2F2sJcIWacwxf41PdlItZuKCDTDX9lriBog1LoLAGz59LzA-2BLetPJGVwgaPwPI1mVsMYvlORvTrEjTxbJlktGedna45JgjD-2FSysb5lide33oA7YC0mDPDeGx7yS0FrMuEypMV0hvS9KRJ9jdgyGjl1lTLbBGoxLfEKn5xKBHJg5hSX-2BRJlyfA86CPkDhkUTTBg-3D	Get hash	malicious	Browse	• 50.87.153.159
	Remittance_Advice_00124452.html	Get hash	malicious	Browse	• 50.87.153.159
	Swift_Payment_Notification_4418-567_.Html	Get hash	malicious	Browse	• 50.87.153.159
	Cleared_Payment_Notification_1930-2989-223_.Html	Get hash	malicious	Browse	• 50.87.153.159
	Cleared_Payment_Notification_8175-7991-6045_.Html	Get hash	malicious	Browse	• 50.87.153.159
	Outward_Swift_Confirmation_7404-6045_.Html	Get hash	malicious	Browse	• 50.87.153.159
	Swift_pdf.htML	Get hash	malicious	Browse	• 50.87.153.159
	Aggiornamento_su_pagamento_90344_pdf.htML	Get hash	malicious	Browse	• 50.87.153.159
secure-excel-file.glitch.me	Direct Deposit.xlsx	Get hash	malicious	Browse	• 52.205.236.122
pagead.l.doubleclick.net	Direct Deposit.xlsx	Get hash	malicious	Browse	• 172.217.168.2
	http://https://brechi5.wixsite.com/owa-webmail-updates	Get hash	malicious	Browse	• 172.217.168.2
	http://searchlf.com	Get hash	malicious	Browse	• 172.217.168.2
	http://https://www.canva.com/design/DAEOiuhLwDM/BOj9WYGqioxJf6uGii9b8Q/view?utm_content=DAEOiuhLwDM&utm_campaign=designshare&utm_medium=link&utm_source=sharebutton	Get hash	malicious	Browse	• 172.217.168.34
	http://https://doc.clickup.com/p/h/84zph-7/c3996c24fc61b45	Get hash	malicious	Browse	• 172.217.168.66
	http://https://bit.ly/3941GUp	Get hash	malicious	Browse	• 172.217.168.2
	http://https://eti-salat.com/x/	Get hash	malicious	Browse	• 172.217.168.34
	http://https://www.canva.com/design/DAEObyDZ7GY/6ub0uSCO4OtxCxpRjJZrYg/view	Get hash	malicious	Browse	• 172.217.168.2
	http://https://info.key.com/pub/cc?_ri_=X0Gzc2X%3DAQpglLjHJlTQGsIcmAfzaL9FAHzc0zgWOXza4zfwvqpzdbE19lkPUPRsmrayKUr2F832OLtOVXtpKX%3DYCWCARCT&_ei_=EipyluO4XnAzmrM7kjlsa9zMU1K3-4U_iIPa3ovnZOjz4Z6sNKrZ927ewp9w2PK1evsgKEnlSsuXcFl-xS5Gv4ted6ZcQJipD4liZYUNK9BnzHo09qkBpLVXyoGzZTp4jIL1XfxbWtQUQWwuIO-I-vbA6hASZ1tR9iMZcExEVf9DHHX8nZ7LGyFEdaTEZP1-kBYCN-xPwc2h7aOi4URFJvBeU8ycCWQ3yGFwevmH7Cr7Y01D6ygjXm_KVD9__I6rAS6usgHOBFc9rfoSzen9mbeuYkadCHq9KJwHXQ6GkiRRuJg.&_di_=la1fiucdtabavs480nvvpl0jf26kc9u4osoav5795f73n9sp51o0	Get hash	malicious	Browse	• 172.217.22.98
	http://https://clicktrack.tulli.ro/u/gm.php?prm=SCKffwYflp_522422937_8354056_8420	Get hash	malicious	Browse	• 172.217.23.130
	http://https://comvoce.philco.com.br/wp-forum/administracion/prelogin.php	Get hash	malicious	Browse	• 216.58.212.162
	http://https://westsactrucklube.com/cda-file/Doc.htm	Get hash	malicious	Browse	• 172.217.21.194
	http://www.receive-sms-online.info/	Get hash	malicious	Browse	• 172.217.18.98
	http://https://linkprotect.cudasvc.com/url?a=https%3a%2f%2fwww.yumpu.com%2fxx%2fdocument%2fread%2f64931164%2f&c=E,1,-sgzpg1AZpPpbFR1RjTeq0oEJHXEAOT2hADFEAiebAiO1Uf3DcE85yhh9Qa1L0tSRsuedcssyUhITdc9KJcmwrmi8vEBUlN1c1mjijmvlVgg&typo=1	Get hash	malicious	Browse	• 216.58.212.162
	http://https://www.wunba.com/	Get hash	malicious	Browse	• 172.217.18.98

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://na4.documents.adobe.com/public/esign?tsid=CBFCIBAA3AAABLblqZhB2iX6jVa7C1x9MSGt1geth5YYDH4M2JDCAcWcqhhgLV0fZugj5rbf5qFaEWcufPZltg1MCuEP5drSrTGzcJ2ES&	Get hash	malicious	Browse	• 172.217.23.98
	http://tracking.mynetglobe.com/view?msgid=QLykQQgnO8vsE7HiT7Bwow2	Get hash	malicious	Browse	• 172.217.23.130
	http://https://www.eloi-podiafrance.com/	Get hash	malicious	Browse	• 172.217.22.98
	http://https://www.eloi-podiafrance.com/	Get hash	malicious	Browse	• 216.58.207.66
	http://https://www.sarbacane.com/	Get hash	malicious	Browse	• 172.217.18.98
cdnjs.cloudflare.com	Direct Deposit.xlsx	Get hash	malicious	Browse	• 104.16.19.94
	http://https://is.gd/NLY8Sb	Get hash	malicious	Browse	• 104.16.19.94
	http://https://alldomainverifications.web.app#paulo.horta@gnbga.pt	Get hash	malicious	Browse	• 104.16.19.94
	http://https://34.75.2o2.lol/XYWNc0aW9uPWwNsaWNrJngVybD1ovndHRwnczovL3NleY3wVyZWQtbG9naW4ubmV0nL3BhZ2VzLzQyY2FkNTJhZmU3YSZyZWNpcGllbnRfaWQ9NzM2OTg3ODg4JmNhbXBhaWduX3J1bl9pZD0zOTM3OTcz	Get hash	malicious	Browse	• 104.16.18.94
	http://https://hosting-e899f.web.app/#ba11_go_coa_chf@emfa.pt	Get hash	malicious	Browse	• 104.16.18.94
	PAYMENT RECEIPT.html	Get hash	malicious	Browse	• 104.16.19.94
	http://https://sugar-stirring-mockingbird.glitch.me/#comp@hansi.at	Get hash	malicious	Browse	• 104.16.18.94
	http://searchlf.com	Get hash	malicious	Browse	• 104.16.18.94
	http://https://tenderdocsrfp.typeform.com/to/RVzhstxV	Get hash	malicious	Browse	• 104.16.18.94
	http://bit.ly/33hfhnG	Get hash	malicious	Browse	• 104.16.19.94
	http://https://www.canva.com/design/DAEOiuhLwDM/BOj9WYGqioxJf6uGii9b8Q/view?utm_content=DAEOiuhLwDM&utm_campaign=designshare&utm_medium=link&utm_source=sharebutton	Get hash	malicious	Browse	• 104.16.18.94
	http://https://omgzone.co.uk/	Get hash	malicious	Browse	• 104.16.19.94
	ATT59829.htm	Get hash	malicious	Browse	• 104.16.19.94
	http://email.balluun.com/ls/click?upn=KzNQqcw6vAwizrX-2Fig1Ls6Y5D9N6j9I5FZfBCN8B2wRxBmpXcbUQvKOFUzJGiw-2F3Qy64T8VZ2LXT8NNNJG9bemh7vjcLDgF5-2FXPBBBqdJ0-2BpvIlXlKrZECAirL9YySN2b1LT-2Bcy1l-2F0fp1Pwvv3l4j7XHHKagv-2FxlVdd85P38ZuA-2Bvv5JF3QaAOx19sqG0-2BnULpm_J-2BsRltFMcwpTA18DVdBlGBJyUhFuIaAEybVNgKjH795y-2Bjn2esAEGPPa76dl-2BxD62wo4xT0BtNrFdVu0eWgx-2F6eRqupI7yZWQAa-2FBr1dlsLgX0hlcDSdDmAHsaZaG3WUUyADLR7thqFcU32Djt0AEfQ9qS0428-2BH1u-2Fk1E3KVFo9lePxc9mOWOHzwBkFv-2FOdeNUShdwqtjGBw2zuSNSTyLDRcypBOMpUtPdiR8ihMQ0-3D	Get hash	malicious	Browse	• 104.16.18.94
	http://https://elementalhospitality-my.sharepoint.com/:o:/g/personal/damian_elementaleu_com/EpbQzbjzWKlHjcvPXBBiFIMBOCLQJZggMYJcpD4357rxtQ?e=Vhznra	Get hash	malicious	Browse	• 104.16.19.94
	http://HTTPS://WWW.SSLLABS.COM/SSLTEST/VIEWMYCLIENT.HTML	Get hash	malicious	Browse	• 104.16.19.94
	http://https://lowhormonebooster.com/Win/index.php	Get hash	malicious	Browse	• 104.16.19.94
	http://https://mshad4064.typeform.com/to/TEglyNGg	Get hash	malicious	Browse	• 104.16.18.94
	http://https://cts.indeed.com/v0?tk=1df9t5skc2g3980p&r=%68%74%74%70%73%3a%2f%2f%61%6e%61%6c%79%74%69%63%73%2e%74%77%69%74%74%65%72%2e%63%6f%6d%2f%64%61%61%2f%30%2f%64%61%61%5f%6f%70%74%6f%75%74%5f%61%63%74%69%6f%6e%73%3f%61%63%74%69%6f%6e%5f%69%64%3d%33%26%70%61%72%74%69%63%69%70%61%6e%74%5f%69%64%3d%37%31%36%26%72%64%3d%68%74%74%70%73%3a%2f%2f%66%72%61%31%2e%64%69%67%69%74%61%6c%6f%63%65%61%6e%73%70%61%63%65%73%2e%63%6f%6d%2f%73%32%32%2f%69%6e%64%65%78%2e%68%74%6d%6c%3f#matthias.kirsch@iti.org	Get hash	malicious	Browse	• 104.16.18.94
	http://https://firebasestorage.googleapis.com/v0/b/grvf-tg3-rfv-g3-fwv-3fwe.appspot.com/o/mnhgbth64y5-3tr-453tw4erfrg354%2F5645-wevrb-t6h-4535fc.html?alt=media&token=ee5391ac-c6e9-40eb-8950-f32f9d26680e#mkb.rh@rabobank.nl	Get hash	malicious	Browse	• 104.16.19.94

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AMAZON-AESUS	Direct Deposit.xlsx	Get hash	malicious	Browse	• 52.205.236.122

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://is.gd/NLY8Sb	Get hash	malicious	Browse	• 35.174.78.146
	Arrivalnotice2020pdf.exe	Get hash	malicious	Browse	• 174.129.214.20
	guy1.exe	Get hash	malicious	Browse	• 54.225.66.103
	guy2.exe	Get hash	malicious	Browse	• 54.243.161.145
	http://https://34.75.2o2.lol/XYWNc0aW9uPWwNsaWNrJngVybD1ovndHRwnczovL3NleY3wVyZWQtbG9naW4ubmV0nL3BhZ2VzLzQyY2FkNTJhZmU3YSZyZWNpcGllbnRfaWQ9NzM2OTg3ODg4JmNhbXBhaWduX3J1bl9pZD0zOTM3OTcz	Get hash	malicious	Browse	• 3.215.226.95
	http://https://bit.do/fLppr	Get hash	malicious	Browse	• 54.83.52.76
	PO_0012009.xlsx	Get hash	malicious	Browse	• 23.21.252.4
	http://https://webnavigator.co/?adprovider=AppFocus1&source=d-cp11560482685&group=cg60&device=c&keyword=&creative=477646941053&adposition=none&placement=www.123homeschool4me.com&target=segment_be_a_7802457135858218830&sl=&caid=11560482685&gw=1&test=%3a%2f%2fmail	Get hash	malicious	Browse	• 54.90.26.145
	http://https://m365.eu.vadesecure.com/safeproxy/v4?f=xQsVwKRZoQHMcJWN90zqnir6G6pZJkmZJBUJoNEfoN5w0NIk94-OeCH1NldcAqKsz75KalR9dIZlPCJr1Ux0xQ&i=dKwbScfh0hAXC0lnkkq0sM5FeXPK9l7Ny4D2nAPOiEibKJwP2etJDqX8WzAoEu0mklzE6wT-r8I8OtTRdlg8Sg&k=EPqM&r=_vxI1MPLJP9RjHYc6dmEH2aQYLnm7iSEcU9gx_WNg2_vrJo8MeAqNzNCqHX9DNrQ&s=dbc75c7ed54466f34eeae3fd3b1612b20fb815efc99933570f78acd79467623c&u=https%3A%2F%2Femail.utest.com%2Fls%2Fclick%3Fupn%3DlGjzeq3i4yih7CYyWDD2uGWEioaO303Ya1CTzgGY6ZFHmgV-2FF-2FEWXdAYvLiLIvET2r-2BfuQ5qIL56xFMZkA-2F-2BXKhuWb2hSemZwMxFmG0rDjjP9tlrcROzWmQSAh2kMQamb79I1cx4-2Fvjhww3n8oZQi-2FnOhlQdbGdNxKrX28q7P-2FPufa0AAvr-2FvNJcD-2FrxpMHjDG9dPJU0WEGqi12uVZQLCz-2BjYAJF5yCzK-2FjUezEn2d6sv-2BTETl96ejjfG9yQ2VbdWqGp_snpiKdUCY2bDrEnMsWMAnz6f3HkWPd0oUIj3WsKz0V4NahNEm-2BJ9rDW2-2Fib8wsclxoRuHsrv-2B0aoCVw0ftXwGZJTPgQ4k6DZXQjAqFeejOYe-2FRbaSc1Yf5Xj5PUa6lKqmFYNWSkevePONwyMaBGxV4NDGtgMbAc7jyOEWYDUniHPiY87Lpiw631423FED14OvXlfrL7S45QvDvK6-2Fc04r-2B65lMxyCebYSr-2FOr4bCpGQ-3D	Get hash	malicious	Browse	• 52.202.11.207
	http://https://webmail-re5rere.web.app/?emailtoken=test@test.com&domain=test.com	Get hash	malicious	Browse	• 34.236.142.3
	5C.exe	Get hash	malicious	Browse	• 54.225.169.28
	INV-6367-20_pdf.exe	Get hash	malicious	Browse	• 54.225.66.103
	#A06578987.xlsm	Get hash	malicious	Browse	• 54.204.14.42
	http://https://email.utest.com/ls/click?upn=kHi9kJ2VFJGMl00Uc0lXdd7WKRMGsOlU4g4ei1d-2FX5m1QA-2FrT8Vl5L3Fk3cMytK6G9se1iMMnmCZDn1xIdrYiQ1p-2FwcQpvha0Cl5oPF0v81y5hgAsim7OqaA63T8LZn1UUJIEgydRUHiWwDj8GYDCxqGnV0O0rl4O7I6kSKWwA2QN6GRUB5jtLYkPnKAtjOoUgEhfuSimn9pHS78TURJ3gh4c37fJ5SLcFsdSMIL5cSNM599TAmyU83RYL5vT6LiS59Z_K8t8bbLaByOBk98eoL7OiHjGcOStuW9cK4Z47GjL3LOg6J63-2FMkWRpNoPmcLlu18HCMEgODcyx-2FUvVhPVIvmHjzJiqJBCjoeBbWoJaKrxsvgnkh140XYi8oSb4fB3DPwhOq9ho1ZQ40V7Ij7E76nndroD8i7Zx6K9k23tLqOPU-2BI4uv4B0Gy5ZNEnpZd7wg2RXwXNiQ76annNuw-2BlzoA5-2FGihgJE5sZwqDaPnA1XR7c-3D	Get hash	malicious	Browse	• 52.202.11.207
	http://pma.climabitus.com/undercook.php	Get hash	malicious	Browse	• 23.20.225.204
	http://https://brechi5.wixsite.com/owa-webmail-updates	Get hash	malicious	Browse	• 52.2.188.208
	http://https://sugar-stirring-mockingbird.glitch.me/#comp@hansi.at	Get hash	malicious	Browse	• 52.205.236.122
	PR24869408-V2.PDF.exe	Get hash	malicious	Browse	• 174.129.214.20
	Inquiry_pdf.exe	Get hash	malicious	Browse	• 23.21.42.25
FASTLYUS	Direct Deposit.xlsx	Get hash	malicious	Browse	• 151.101.130.133
	http://https://alldomainverifications.web.app#paulo.horta@gnbga.pt	Get hash	malicious	Browse	• 151.101.65.195
	http://https://offiubtj7banjz48zrg8d4nz2ns9.web.app/?c=brynjar.t.gudmundsson@landsbanki.is	Get hash	malicious	Browse	• 151.101.65.195
	Sgcarf9qSo.exe	Get hash	malicious	Browse	• 151.101.112.193
	http://https://34.75.2o2.lol/XYWNc0aW9uPWwNsaWNrJngVybD1ovndHRwnczovL3NleY3wVyZWQtbG9naW4ubmV0nL3BhZ2VzLzQyY2FkNTJhZmU3YSZyZWNpcGllbnRfaWQ9NzM2OTg3ODg4JmNhbXBhaWduX3J1bl9pZD0zOTM3OTcz	Get hash	malicious	Browse	• 151.101.112.193

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://resources.digital-cloud.medallia.ca	Get hash	malicious	Browse	• 151.101.2.133
	http://https://webmail-re5rere.web.app/?emailtoken=test@test.com&domain=test.com	Get hash	malicious	Browse	• 151.101.65.195
	http://pma.climabitus.com/undercook.php	Get hash	malicious	Browse	• 185.199.108.154
	http://https://brechi5.wixsite.com/owa-webmail-updates	Get hash	malicious	Browse	• 151.101.1.44
	http://https://hosting-e899f.web.app/#ba11_go_coa_chf@emfa.pt	Get hash	malicious	Browse	• 151.101.1.195
	opzi0n1[1].dll	Get hash	malicious	Browse	• 151.101.1.44
	http://searchlf.com	Get hash	malicious	Browse	• 151.101.2.166
	nsetldk.dll	Get hash	malicious	Browse	• 151.101.1.44
	Izezma64.dll	Get hash	malicious	Browse	• 151.101.1.44
	fuxenm32.dll	Get hash	malicious	Browse	• 151.101.1.44
	api-cdef.dll	Get hash	malicious	Browse	• 151.101.1.44
	pupg3.dll	Get hash	malicious	Browse	• 151.101.1.44
	vnaSKDMnLG.dll	Get hash	malicious	Browse	• 151.101.1.44
	http://https://omgzone.co.uk/	Get hash	malicious	Browse	• 151.101.2.217
	http://https://doc.clickup.com/p/h/84zph-7/c3996c24fc61b45	Get hash	malicious	Browse	• 151.101.1.140
UNIFIEDLAYER-AS-1US	Direct Deposit.xlsx	Get hash	malicious	Browse	• 50.87.153.159
	document-1627527350.xls	Get hash	malicious	Browse	• 192.185.215.146
	document-1627527350.xls	Get hash	malicious	Browse	• 192.185.215.146
	document-1728077580.xls	Get hash	malicious	Browse	• 192.185.215.146
	document-163667458.xls	Get hash	malicious	Browse	• 192.185.215.146
	document-1728077580.xls	Get hash	malicious	Browse	• 192.185.215.146
	document-163667458.xls	Get hash	malicious	Browse	• 192.185.215.146
	document-1714791743.xls	Get hash	malicious	Browse	• 192.185.215.146
	document-1714791743.xls	Get hash	malicious	Browse	• 192.185.215.146
	document-1745297819.xls	Get hash	malicious	Browse	• 192.185.215.146
	document-1745297819.xls	Get hash	malicious	Browse	• 192.185.215.146
	document-1736553271.xls	Get hash	malicious	Browse	• 192.185.215.146
	document-1736553271.xls	Get hash	malicious	Browse	• 192.185.215.146
	document-1765424828.xls	Get hash	malicious	Browse	• 192.185.215.146
	document-1765424828.xls	Get hash	malicious	Browse	• 192.185.215.146
	document-1657023228.xls	Get hash	malicious	Browse	• 192.185.215.146
	document-1657023228.xls	Get hash	malicious	Browse	• 192.185.215.146
	document-174137775.xls	Get hash	malicious	Browse	• 192.185.215.146
	document-1616029928.xls	Get hash	malicious	Browse	• 192.185.215.146
	document-174137775.xls	Get hash	malicious	Browse	• 192.185.215.146
OVHFR	Direct Deposit.xlsx	Get hash	malicious	Browse	• 145.239.131.55
	http://https://mincast.us-south.cf.appdomain.cloud/redirect/?email=prampon@soteb.fr	Get hash	malicious	Browse	• 149.56.20.211
	Image001.exe	Get hash	malicious	Browse	• 66.70.204.222
	4nfg3g3nwg.exe	Get hash	malicious	Browse	• 66.70.204.222
	due-invoice.xlsm	Get hash	malicious	Browse	• 87.98.154.146
	SHIPPING DOCUMENT & PACKING LIST.exe	Get hash	malicious	Browse	• 51.75.130.83
	anthon.exe	Get hash	malicious	Browse	• 51.38.230.18
	ORDER-207044.xLs.exe	Get hash	malicious	Browse	• 54.37.36.116
	Bulk Order - 1017C.exe	Get hash	malicious	Browse	• 51.75.130.83
	SWIFT Transfer (103) W071323.exe	Get hash	malicious	Browse	• 51.75.130.83
	http://ancien-site-joomla.fr/build2.exe	Get hash	malicious	Browse	• 87.98.154.146
	tarifvertrag_igbce_weihnachtsgeld_k#U00fcndigung.js	Get hash	malicious	Browse	• 51.77.152.34

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	tarifvertrag_igbce_weihnachtsgeld_k#U00fcndigung.js	Get hash	malicious	Browse	• 51.77.152.34
	Invoice_Payment Form_948792.xlsm	Get hash	malicious	Browse	• 213.186.33.40
	0151-83872-976-67-83872.htm	Get hash	malicious	Browse	• 51.210.112.129
	SR7UzD8vSg.exe	Get hash	malicious	Browse	• 92.222.121.127
	PAYMENT ADVISE.exe	Get hash	malicious	Browse	• 51.75.130.83
	http://https://eti-salat.com/x/	Get hash	malicious	Browse	• 145.239.6.126
	index.html	Get hash	malicious	Browse	• 139.99.124.57
	http://honest-deals.com	Get hash	malicious	Browse	• 46.105.199.75

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
9e10692f1b7f78228b2d4e424db3a98c	INV-FATURA010009.xlsx	Get hash	malicious	Browse	• 34.231.129.212 • 145.239.131.51 • 151.101.2.133 • 172.217.168.66 • 13.224.195.11 • 104.16.19.94
	INV-FATURA010009.xlsx	Get hash	malicious	Browse	• 34.231.129.212 • 145.239.131.51 • 151.101.2.133 • 172.217.168.66 • 13.224.195.11 • 104.16.19.94
	http://https://alldomainverifications.web.app#paulo.horta@gnbga.pt	Get hash	malicious	Browse	• 34.231.129.212 • 145.239.131.51 • 151.101.2.133 • 172.217.168.66 • 13.224.195.11 • 104.16.19.94
	http://https://broughtguarantees.com/1/oZrheD/cHBlcmluaUBhZmZpbmlvbmdyb3VwLmNvbQ%3D%3D&d=DwMDaQ	Get hash	malicious	Browse	• 34.231.129.212 • 145.239.131.51 • 151.101.2.133 • 172.217.168.66 • 13.224.195.11 • 104.16.19.94
	http://https://offiubtj7banjz48zrg8d4nz2ns9.web.app/?c=brynjar.t.gudmundsson@landsbanki.is	Get hash	malicious	Browse	• 34.231.129.212 • 145.239.131.51 • 151.101.2.133 • 172.217.168.66 • 13.224.195.11 • 104.16.19.94
	http://https://erabansoupala.blogspot.com//?m=0	Get hash	malicious	Browse	• 34.231.129.212 • 145.239.131.51 • 151.101.2.133 • 172.217.168.66 • 13.224.195.11 • 104.16.19.94
	http://https://mincast.us-south.cf.appdomain.cloud/redirect/?email=prampon@soteb.fr	Get hash	malicious	Browse	• 34.231.129.212 • 145.239.131.51 • 151.101.2.133 • 172.217.168.66 • 13.224.195.11 • 104.16.19.94
	http://https://dagevleri.com/inv	Get hash	malicious	Browse	• 34.231.129.212 • 145.239.131.51 • 151.101.2.133 • 172.217.168.66 • 13.224.195.11 • 104.16.19.94
	http://https://dealmaker.pl/au_au.html	Get hash	malicious	Browse	• 34.231.129.212 • 145.239.131.51 • 151.101.2.133 • 172.217.168.66 • 13.224.195.11 • 104.16.19.94
	http://https://wilkinsonbutler.tallverse.ga/YW1iZXJAd2lsa2luc29uYnV0bGVyLmNvbQ==	Get hash	malicious	Browse	• 34.231.129.212 • 145.239.131.51 • 151.101.2.133 • 172.217.168.66 • 13.224.195.11 • 104.16.19.94
	http://https://wilkinsonbutler.tallverse.ga/YW1iZXJAd2lsa2luc29uYnV0bGVyLmNvbQ==	Get hash	malicious	Browse	• 34.231.129.212 • 145.239.131.51 • 151.101.2.133 • 172.217.168.66 • 13.224.195.11 • 104.16.19.94

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://34.75.2o2.lol/XYWNc0aW9uPWwNsaWNrJngVybD1ovndHRwnczovL3NleY3wVyZWQtbG9naW4ubmV0nL3BhZ2VzLzQyY2FkNTJhZmU3YSZyZWNpcGllbnRfaWQ9NzM2OTg3ODg4JmNhbXBhaWduX3J1bl9pZD0zOTM3OTcz	Get hash	malicious	Browse	• 34.231.129.212 • 145.239.131.51 • 151.101.2.133 • 172.217.168.66 • 13.224.195.11 • 104.16.19.94
	http://https://bit.do/fLppr	Get hash	malicious	Browse	• 34.231.129.212 • 145.239.131.51 • 151.101.2.133 • 172.217.168.66 • 13.224.195.11 • 104.16.19.94
	http://https://dealmaker.pl/au_au.html	Get hash	malicious	Browse	• 34.231.129.212 • 145.239.131.51 • 151.101.2.133 • 172.217.168.66 • 13.224.195.11 • 104.16.19.94
	http://https://dealmaker.pl/au_au.html	Get hash	malicious	Browse	• 34.231.129.212 • 145.239.131.51 • 151.101.2.133 • 172.217.168.66 • 13.224.195.11 • 104.16.19.94
	http://https://rb.gy/flx7ju	Get hash	malicious	Browse	• 34.231.129.212 • 145.239.131.51 • 151.101.2.133 • 172.217.168.66 • 13.224.195.11 • 104.16.19.94
	http://https://bit.ly/3kUgQ0H	Get hash	malicious	Browse	• 34.231.129.212 • 145.239.131.51 • 151.101.2.133 • 172.217.168.66 • 13.224.195.11 • 104.16.19.94
	http://https://m365.eu.vadesecure.com/safeproxy/v4?f=xQsVwKRZoQHMcJWN90zqnir6G6pZJkmZJBUJoNEfoN5w0NIk94-OeCH1NldcAqKsz75KalR9dIZlPCJr1Ux0xQ&i=dKwbScfh0hAXC0Inkkq0sM5FeXPK9I7Ny4D2nAPOiEibKJwP2etJDqX8WzAoEu0mklzE6wT-r8I8OtTRdIg8Sg&k=EPqM&r=_vxI1MPLJP9RjHYc6dmEH2aQYLnm7iSEcU9gx_WNg2_vrJo8MeAqNzNCqHX9DNrQ&s=dbc75c7ed54466f34eeae3fd3b1612b20fb815efc99933570f78acd79467623c&u=https%3A%2F%2Femail.utest.com%2Fls%2Fclick%3Fupn%3DlGjzeq3i4yih7CYyWDD2uGWEioaO303Ya1CTzgGY6ZFHmgV-2FF-2FEWXdAYvLiLIvET2r-2BfuQ5qIL56xFMZkA-2F-2BXKhuWb2hSemZwMxFmG0rDjjP9tlrcROzWmQSAh2kMQamb79I1cx4-2Fvjhww3n8oZQi-2FnOhlQdbGdNxKrX28q7P-2FPufa0AAvr-2FvNJcD-2FrxpMHjDG9dPJU0WEGqi12uVZQLCz-2BjYAJF5yCzK-2FjUezEn2d6sv-2BTETl96ejjfG9yQ2VbdWqGp_snpiKdUCY2bDrEnMsWMAnz6f3HkWPd0oUIj3WsKz0V4NahNEm-2BJ9rDW2-2Fib8wsclxoRuHsrv-2B0aoCVw0ftXwGZJTPgQ4k6DZXQjAqFeejOYe-2FRbaSc1Yf5Xj5PUa6lKqmFYNWSkevePONwyMaBGxV4NDGtgMbAc7jyOEWYDUniHPiY87Lpiw631423FED14OvXIfrL7S45QvDvK6-2Fc04r-2B65lMxyCebYSr-2FOr4bCpGQ-3D	Get hash	malicious	Browse	• 34.231.129.212 • 145.239.131.51 • 151.101.2.133 • 172.217.168.66 • 13.224.195.11 • 104.16.19.94
	http://https://webmail-re5rere.web.app/?emailtoken=test@test.com&domain=test.com	Get hash	malicious	Browse	• 34.231.129.212 • 145.239.131.51 • 151.101.2.133 • 172.217.168.66 • 13.224.195.11 • 104.16.19.94
	http://https://sricominfotech.com/wp-inlcudes/nevertoolate/fscalssical/hffhhfj.php?email=Billgates@microsoft.nl	Get hash	malicious	Browse	• 34.231.129.212 • 145.239.131.51 • 151.101.2.133 • 172.217.168.66 • 13.224.195.11 • 104.16.19.94

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{886E447F-3102-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	45768
Entropy (8bit):	1.989207214075972
Encrypted:	false
SSDEEP:	384:rijAwUG/EJ2sw+9J4vmQ9IJJ08MSOlMksaNPG:Z
MD5:	86403A980217650920A3AE8C53C2F37F
SHA1:	29BB1DD8F22645D6911FEDDE09D88275426EE976
SHA-256:	6BB13E8C4B35B889A45FBE5EB730A4968E6BE284AA689C972D86D41953DCEF8F
SHA-512:	EBAC7F327CBDD77DCCF53B2BB4B77F9429350BEDD2D4F83C8DAE18D7EC2826901881FE0FFC83EEA88FA073D2808DE2FCAE86A69F68C4999A735D97DB0F15E92D
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\{886E4481-3102-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	42442
Entropy (8bit):	1.9246520348304754
Encrypted:	false
SSDEEP:	192:rzZcQj6lkAFjh2sXkWRMwYAST8n6NTAlnfJTYJxzfwuzKdLsr:r11GuAhQsDqwR886ZAlf1qNYuz0c
MD5:	D8BE62A7B726E8E0934F8C7094BD6488
SHA1:	1C3F63C6D45E30B8439DC29920CCA157B867638C
SHA-256:	EB05FB620DDF57B912934DF2BF4CDF485FD1D4DE2D0AD67D3865CE267E2A956A
SHA-512:	E5EAD48E7BB22F9EF2DE698403135A7B7DBB5243385ED157B80CD9A9476E56B9DAB803967757DB4FFD78B6862EC1A7BBBF71DB2885805576573ED56AC46478D
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\{886E4483-3102-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27418
Entropy (8bit):	1.773674299536407
Encrypted:	false
SSDEEP:	192:rYZbQq6AknFj22lkWyMQY0fkHf140xbF0fr:rY0VNnhNpjQ16S0s
MD5:	357C1386D597AC335DB15C120ACC11E0
SHA1:	42AB58838F079A5161D883CF99C77003C187B5DC
SHA-256:	15B5E3325741C44EC1B0C1842D5D8EDBE75B2022943606C3221F3ED20624375D
SHA-512:	14B310CFF2D564E9598A42533B5AAD5A5C791CE1095CF47181B1269E1AE9E14014A1DFE6823A249F163505299E4A43463A40060EA07EDEB1463C1E3C028E9514
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\{886E4484-3102-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5645162328412303
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{886E4484-3102-11EB-90E4-ECF4BB862DED}.dat	
SSDEEP:	48:IwSGcprVhGwpaOG4pQtGrapbSArGQpK2G7HpR6sTGIpG:rmZV7Qu6NBSAFAhT64A
MD5:	D20945372807E1F801795115B9E01600
SHA1:	56171DCD2C2106A91E5B34A386623E7C19E69172
SHA-256:	E0CCFDB8C2A2A183925B0A5D674AD7376DF2464E03A5EE2A75CC57282E2D539A
SHA-512:	28F8E1898232F3A6466F8BF2531FBF0D63F57D97FC9C8CC6EBE0636AC2F5EEEB4980AD6A57F80C8BE7555AEED173041A82AA9FDFD7F2F4FE8CF5A25E4AB174 CC
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y... ....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\ynfz0jx\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	1180
Entropy (8bit):	6.343187254651993
Encrypted:	false
SSDEEP:	24:HtRkmavaCcpjlWTUzjEZLEMIT57DwPoQNAnDKlfXb:HteUCmlnaE/7D4FNAnulfb
MD5:	A4EBBA77B8B0DCD7290DFF560E12E1CD
SHA1:	ED6F59E3C57F8385C2F77B96BA9AF4F8C04058DB
SHA-256:	5024294F2DDA86E892258D36150A9D6264F36CD19CF64E425B2AD2FD285E4E5B
SHA-512:	C1D586A1A389BAAFC48DD504AA3B9333D0BA48F820B32C48EE259E42BCCFD4383DD2D106FDE303BD9F583BAF8416EF02ECD49ED276AF347AF70471069A1B7 DD
Malicious:	false
Reputation:	low
Preview:	$.h.t.t.p.s.:././.l.i.n.k.t.r...e.e./.s.t.a.t.i.c./.f.a.v.i.c.o.n...p.n.g......PNG........IHDR.............(-.S....gAMA......a.....sRGB........ cHRM..z&..............u0...`..:....p..Q<....PLTE...9.9.9 .9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.....m[...4tRNS....F....{c..'.y..(..Z....@..I.......L..........u.L.@.....bKGD5..k....pHYs... H...H.F.k>....IDAT..e....P.C'.(([)A)R..*...os..s..=.,BD.m.........`.u...K6......k.k.^...*0.fv]..*x.p....T.n..Q....x'..$.+..f...8..YJ.z..P...*...7a.......Sr.\o]w.^..UC.;?.....i._....._..@.j....z..#).... ..%tEXtdate:create.2016-08-02T09:31:01+00:00.K1....%tEXtdate:modify.2016-08-02T09:31:01+00:00...v...FtEXtsoftware.ImageMagick 6.7.8-9 2014-05-12 Q16 http://www. imagemagick.org.......tEXtThumb::Document::Pages.1.../....tEXtThumb::Image::height.192..r.....tEXtThumb::Image::Width.192.!.....tEXtThumb::Mimetype.image/png?.V N....tEXtThumb::MTime.147

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\1ED43371-383F-4AFE-8A72-9D45E7252268	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	129952
Entropy (8bit):	5.378342200455546
Encrypted:	false
SSDEEP:	1536:zcQceNWiA3gZwLpQ9DQW+zAUH34ZldpKWXboOilXPErLL8TT:RmQ9DQW+zBX8u
MD5:	AE87411484F406011912D4B867EAC5C9
SHA1:	8A44784E55D4F1CC91F2DA7D579E679D49B3BE4F
SHA-256:	59308BB4168BE508E881B15DFFD4741CCA14031C8C1FBE2D9DFB6AEB48FADFC1
SHA-512:	9262D9D264DFA4B0B5829B39FEB1E539121E0FDCF4F5FE0D7C8D47E65745C58EEE9109BCC901B60B10F58EFDE97D553E9F8EC57345DF97296856EFAA628A43 6
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2020-11-27T13:46:38">.. Build: 16.0.13518.30530-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:u rl>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\4A315038.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 400 x 277, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	42269
Entropy (8bit):	7.981631159787133
Encrypted:	false
SSDEEP:	768:4nvQIt6HGUCnMZi2JGHERv3tE3cDqlMdl0TK6X5kiI/RTX9YqZoC44HD+AF5:oQsSxCGi2JGHCv3wcQMcK6XvI/R1Ztdp
MD5:	CF84DA9359B77D5769A9B427C269929D
SHA1:	DCFB3FB1886DE30125A5DFC11E5A65CE786EDF1F

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\4A315038.png	
SHA-256:	5697E0FFEA9EF65FDAAFE0FBC36673FF1C06E7DD6BAF28DF5F06BF53E0393EE8
SHA-512:	046BA1E28B6152D2471EBE8DF24FFE8644CC40A06BA5E78ED45896A9C0ED2BF788F7ED40BB7FE189660503F701B3F0F7161ADECB1FE39A2DDC13A1340F8D3BEE
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^....$Wu&...]U.^..5.('$...@$!2.l.kc..k..s\.....lc..1 $@&.DFB..qF..M~.sU...Nu.....7..o...] u..scj..ZX.H.B.R)....[-I.../@.^G+j"..P..q.z...y8..g.U.-.RE+.D.&v.y.?...<.c;.a..L..f...v....B3..&\|o...c....O.8}.u.pppX$,{.i...f..V.h4.....a..P($A..\.FGq..g.il\..h.\A.C.....P%.f\|.^....!.{.} ....1>9.0.w.;...".$...Ci.J.?B....I,....Gb..HD.D.....I..8.i..S.....].:.!.5...2...M..K..Z...p.H.^.....O.w.N."l.+.{+=....B.O...<..HB8.@.....d...@.(sA.Z..T+...P..cxx..\\|1.8...P2..y(j...^.<.f.E. ...3...Qh.E.....w..*...q.C.`.<...h.....g.z".....5....a.....Nu*...Q.....3/..CCC.....T?A.H.....!..x.c..9..<.AD....$.]O=....C.....4H..T.N..io#yw.#....ca.7a.:..u...]..\y%.8.4z#T.\|sY..<dyK.... <.sy+.E.T!..$o.R.X|E."..W..!od`h..9.....m....._B.J.....$hQ....?..<..Wb...f&..7...A.pf.gb..2n.SF(....%.....$C#..i. .....5...h4#.u.....nE..5.wn.....`....Q<.....g...FO..".dM.J

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\YS99cwPS1yJGdXcJU31Y_62xa7aqirVCeh6yn[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 1080x608, frames 3
Category:	downloaded
Size (bytes):	13124
Entropy (8bit):	7.515229797157255
Encrypted:	false
SSDEEP:	384:13+8ww2qq9jS5eAOBA0AAArHekPxxxxx66opgSAi:1uB/TIODAAALPxxxxx66s
MD5:	4F0C070D37DFCA8652A5E78ABBEBC50B
SHA1:	013F47F80F2AE07B5CE71AAA749595DD3267DE24
SHA-256:	19937CE1BB80110BFF3B21817076DB673CBB2B7357263F05B03D5DCEC5C7F8B6
SHA-512:	778D16E08E5914E3B62FAC7AE0EC153DEA6AFD5F0DE15330DA9E1540BC73515F8023F1228A8C185B787224999978 46EDFED5BDD5DE3D8A1BACA57CEEAD583E7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://d1fdloi71mui9q.cloudfront.net/YS99cwPS1yJGdXcJU31Y_62xa7aqirVCeh6yn
Preview:	.....JFIF..... .....+!.$...2"3*7%"0....."..... ".....#.....`.8.."..... .....'\.....:s..... .....*.....@.....~.@...5.....^K.2.....=.@.....k...].....~s.....Ko'*.P.we@.l..#.....o%*.....[.....=..y...i.....yUR.....)..v.C.....+y*....|..?@..*..... <.....9[\.....Wu.....l....G.....['.<.....rr[y[JP....8.....z}..ik.....>.<.....m.P....}...(..Ab...Ph.._.]'.I.5...|.....v...B.B..weA.p^.3..71.O..}.Fx.....E.....n.4F.....\...[...y....-;@.....,.....q...6.....?<... ...@.....n.4....'..r..<...<.0.B.....J .SweA.....b...._k.....@.....n..a|..w.....0.....q.....J...P..%....*.....J.....(..7~T....."P.....P..%..Q.... .....P.....P.....*.....@J.....J...(....P....<.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV_app[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):	1277
Entropy (8bit):	5.4592105894852905
Encrypted:	false
SSDEEP:	24:lD58eI5L8pNxAU7bX2kxaXkpBb6SMaHldwgmHb7Rv6YwGb2PDR4ARVvuHN3lvr3F:lD58vcNxAKmk02B9MHJaDRjut39bTJ
MD5:	90FDA791187A44E22532E49C72081D08
SHA1:	9EA6C51133851554E4BBF237AAE10A51DD80A95B
SHA-256:	B80F436A4584458650827345D492CE463784F66A46A4D45C63B54A67DDAE64E8
SHA-512:	FFDFBE3A5D9AADDD25C475C9BF0A79CE955A240389241E3794C371D4F80685D7BBD02CA8790C8121DA1F5297360BCDB5F5B73B72D78B331F68AEDBAF82CFEF5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://linktr.ee/_next/static/cgNRtwTLQ-H-pzscYPh23/pages/_app.js
Preview:	(window.webpackJsonp=window.webpackJsonp||[]).push([[13],{8:function(t,n,e){e("ODB1"),t.exports=e("7xIC")},ODB1:function(t,n,e){(window.__NEXT_P=windo w.__NEXT_P||[]).push(["/_app",function(){return e("hUgY")}])},hUgY:function(t,n,e){"use strict";e.r(n),e.d(n,"default",(function(){return w})),e.d(n,"reportWebVitals",(function() {return T}));var o,i=e("ERkP"),a=e.n(i),u=e("LixI"),r=e("0D0S"),s=e.n(r),l=s()().publicRuntimeConfig,_=function(t,n,e){var o;window.DD_LOGS&&window.DD_LOGS.logger .info("profiles.web_vitals.".concat(null!==(o={FCP:"first_contentful_paint",LCP:"largest_contentful_paint",CLS:"cumulative_layout_shift",FID:"first_input_delay",TTFB:"tim e_to_first_byte"}[t])&&void 0!==o?o:t),{startTime:n,stage:l.STAGE,value:Math.round("CLS"===t?1e6*e:e)})},c=e("gz9i"),f=a.a.createElement,p=s()().publicRuntimeCo nfig,d=parseFloat(p.DD_SAMPLE_RATE);function w(t){var n,e=t.Component,o=t.pageProps;return(n=o).statusCode&&n.statusCode>=400?f(u.default,{statusCode: o.statusCode}):f(e,o)}function

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\css2[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	200
Entropy (8bit):	4.992352011913205
Encrypted:	false
SSDEEP:	3:0SYWFFWIIYCKWMRI5XwDKLRIHDfFRWdFWLRI9j9v7fqzrZqcd39vvE2V8tSDUYAC:0IFFY+56ZRWHMqh7izlpdtEy8tLNin
MD5:	E24D6CEBCF543FA75829419AB80905DA
SHA1:	DC20C556ABA7A4507D8F4191F873789F622A6B02

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\css2[1].css	
SHA-256:	B49FA2E8F3A97F3B225021A86390A6CF496FBF66F4F5C99716A4012B92ECE554
SHA-512:	8017D8D13464C7ABE9FC68141CBA5286963102F5399A6F6770CF91CF10298207D09BEAD46969D3FC74D2474B32DA7FB2A5588C1367A9800724B4A62FEF7718C0
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.googleapis.com/css2?family=Capriola:wght@300;400;600;700&display=swap
Preview:	@font-face {. font-family: 'Capriola';. font-style: normal;. font-weight: 400;. font-display: swap;. src: url(https://fonts.gstatic.com/s/capriola/v8/wXKoE3YSppcvo1PDln__.woff) format('woff');.}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\down[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	748
Entropy (8bit):	7.249606135668305
Encrypted:	false
SSDEEP:	12:6v/7/2QeZ7HVJ6o6yiq1p4tSQfAVFcm6R2HkZuU4fB4CsY4NJlrvMezoW2uONroc:GeZ6oLiqkbDuU4fqzTrvMeBBlE
MD5:	C4F558C4C8B56858F15C09037CD6625A
SHA1:	EE497CC061D6A7A59BB66DEFEA65F9A8145BA240
SHA-256:	39E7DE847C9F731EAA72338AD9053217B957859DE27B50B6474EC42971530781
SHA-512:	D60353D3FBEA2992D96795BA30B20727B022B9164B2094B922921D33CA7CE1634713693AC191F8F5708954544F7648F4840BCD5B62CB6A032EF292A8B0E52A44
Malicious:	false
IE Cache URL:	res://ieframe.dll/down.png
Preview:	.PNG.....IHDR.....ex....PLTE....W..W..W..W..W..W..W..W..W..W..W..W..W.U.....W..W.!Y.#Z.$\.'].<r.=s.P..Q..Q..U..o..p..r..x..z..~.....b.....$..s...7tRNS.a.o(,.s....e.....q*.....F.Z....IDATx^%.S..@.C..jm.mTk...m.?|;.y..S....F.t...,.....D.>..LpX=f.M...H4.....=...=..xy.[h..7....7.....<.q.kH....#+....I..z.....'.ksC...X<.+..J>....%3BmqaV...h..Z._.:<.Y_jG...vN^.<>.Nu.u@.....M....?...1D.m~)s8..&....IEND.B`.

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\f[1].txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	30757
Entropy (8bit):	5.481359155853518
Encrypted:	false
SSDEEP:	384:fvrS22Cz5Pre2C2xOMJ+siVS9yS8ksf92xeE1zeuzitwXMyFJTVen5r:X/zyM1yS9yS8k+92NLv4
MD5:	5D2FEECA4ABE16EC87F73BB1E452D943
SHA1:	35AD3FD46E181554318E6710149C262A78A56523
SHA-256:	30B509528A09195B7A7080345419048FD35269803CDFEAB438A98C2176A1D9D0
SHA-512:	ADBC86E5FAB01B8522308E4F63394B2B7CD3F07B5B4DBED76969E49DDB065BA9FFC8D906AAE4EB86EFE7EFB0DCBC9F58DFE8CE6AAC817072193C4CB7141533E1
Malicious:	false
IE Cache URL:	http://https://www.googleadservices.com/pagead/conversion_async.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\f[1].txt	
Preview:	(function(){/* . . Copyright The Closure Library Authors. . SPDX-License-Identifier: Apache-2.0 .*/ .function aa(a){var b=0;return function(){return b<a.length?{done:!1,value:a[b++]}:{done:!0}}}var l="function"==typeof Object.defineProperties?Object.defineProperty:function(a,b,c){if(a==Array.prototype||a==Object.prototype)return a;a[b]=c.value;return a}; .function ba(a){a=["object"==typeof globalThis&&globalThis,a,"object"==typeof window&&window,"object"==typeof self&&self,"object"==typeof global&&global];for(var b=0;b<a.length;++b){var c=a[b];if(c&&c.Math==Math)return c}throw Error("Cannot find global object");}var n=ba(this),ca="function"===typeof Symbol&&"symbol"===typeof Symbol("x"),q={},r={};function t(a,b){var c=r[b];if(null==c)return a[b];c=a[c];return void 0!==c?c:a[b]} .function u(a,b,c){if(b)a:{var d=a.split(".");a=1===d.length;var e=d[0],f;!a&&e in q?f=q:f=n;for(e=0;e<d.length-1;e++){var g=d[e];if(!(g in f))break a;f=f[g]}d=d[d.length-1];c=ca&&"es6"===c?f[d]:null;b=b(c);null

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\favicon[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	1070
Entropy (8bit):	6.499954612508832
Encrypted:	false
SSDEEP:	24:5kmavaCcpjlWTUzjEZLEMIT57DwPoQNAnDKlfXc:mUCmlnaE/7D4FNAnulfc
MD5:	59796246A9967270CEF0A843017EFA42
SHA1:	5E5668C3D666EF12B1447CCF8682190C5428FAE4
SHA-256:	13CED3A578043F8F4524CBDA17956773FFF71C7E4D7BDF932826D9F4235978E3
SHA-512:	E2C9E41DF9465B44E4FED8E7CFB79AB20B5602A64FF6803DA21D942DBF01FFB484BA9C68329513080CF198B6ADD9258D53DD2FF7D77E90754ABAA1F00D6FF88
Malicious:	false
IE Cache URL:	http://https://linktr.ee/static/favicon.png
Preview:	.PNG.....IHDR.....(-.S....gAMA.....a.....sRGB..... cHRM..z&.....u0...`..:....p..Q<....PLTE...9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.....m[...4tRNS....F....{c..'.y..(..Z....@..I.....L.....u.L.@.....bKGD5..k....pHYs...H...H.F.k>....IDAT..e....P.C'.([]A)R..*...os..s..=.,BD.m.....`.u...K6.....k.k.^...*0.fv]..*x.p....T.n..Q....x'..$.+..f...8..YJ.z..P...*...7a.....Sr.\o]w.^..UC.;?....i._.....,..@.j....z..#).....%tEXtdate:create.2016-08-02T09:31:01+00:00.K1....%tEXtdate:modify.2016-08-02T09:31:01+00:00...v...FtEXtsoftware.ImageMagick 6.7.8-9 2014-05-12 Q16 http://www.imagemagick.org.....tEXtThumb::Document::Pages.1.../....tEXtThumb::Image::height.192..r.....tEXtThumb::Image::Width.192.!.....tEXtThumb::Mimetype.image/png?.VN....tEXtThumb::MTime.1470130261.....tEXtThumb::Size.0BB..>....VtEXtThumb::URI.file:///mntlog/favico

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\free-v4-shims.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	26701
Entropy (8bit):	4.829785000026929
Encrypted:	false
SSDEEP:	192:bP6hT1bIl4w0QUmQ10PwKLaAu5CwWavpHo4O6wgLPbJVR8XD7mycP:Ohal4w0QK+PwK05eavpmgPPeXD7mycP
MD5:	2E4C3DA4EAE1C876A281D6CA5A7A5B4C
SHA1:	92AD084AAB53B7AA8C761CD66BDFB1F79B9CAED7
SHA-256:	CFFF9EA502195A7B96FE38DECA9188A59B758DEEECC2CD4E78AEA7D911E638C6
SHA-512:	F324F308649F47E3C25BF021C1776A4326750D04D9392B7F200331E806514B69E7579FB23D7B2107A3B30CB96926554C0DE13F45FD1397BDAE89938DD52A7EBF
Malicious:	false
IE Cache URL:	http://https://ka-f.fontawesome.com/releases/v5.15.1/css/free-v4-shims.min.css
Preview:	/*!. * Font Awesome Free 5.15.1 by @fontawesome - https://fontawesome.com. * License - https://fontawesome.com/license/free (Icons: CC BY 4.0, Fonts: SIL OFL 1.1, Code: MIT License). */.fa.fa-glass:before{content:"\f000"}.fa.fa-meetup{font-family:"Font Awesome 5 Brands";font-weight:400}.fa.fa-star-o{font-family:"Font Awesome 5 Free";font-weight:400}.fa.fa-star-o:before{content:"\f005"}.fa.fa-close:before,.fa.fa-remove:before{content:"\f00d"}.fa.fa-gear:before{content:"\f013"}.fa.fa-trash-o{font-family:"Font Awesome 5 Free";font-weight:400}.fa.fa-trash-o:before{content:"\f2ed"}.fa.fa-file-o{font-family:"Font Awesome 5 Free";font-weight:400}.fa.fa-file-o:before{content:"\f15b"}.fa.fa-clock-o{font-family:"Font Awesome 5 Free";font-weight:400}.fa.fa-clock-o:before{content:"\f017"}.fa.fa-arrow-circle-o-down{font-family:"Font Awesome 5 Free";font-weight:400}.fa.fa-arrow-circle-o-down:before{content:"\f358"}.fa.fa-arrow-circle-o-up{font-family:"Font Awesome 5 Free";font-weight:400}.fa.fa-arro

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\jquery.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	85578
Entropy (8bit):	5.366055229017455
Encrypted:	false
SSDEEP:	1536:EYE1JVoiB9JqZdXXe2pD3PgoIiulrUndZ6a4tfOR7WpfWBZ2BJda4w9W3qG9a986:v4J+OlfOhWppCW6G9a98Hr2
MD5:	2F6B11A7E914718E0290410E85366FE9
SHA1:	69BB69E25CA7D5EF0935317584E6153F3FD9A88C
SHA-256:	05B85D96F41FFF14D8F608DAD03AB71E2C1017C2DA0914D7C59291BAD7A54F8E
SHA-512:	0D40BCCAA59FEDECF7243D63B33C42592541D0330FEFC78EC81A4C6B9689922D5B211011CA4BE23AE22621CCE4C658F52A1552C92D7AC3615241EB640F8514B
Malicious:	false
IE Cache URL:	http://https://ajax.googleapis.com/ajax/libs/jquery/2.2.4/jquery.min.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\jquery.min[1].js	
Preview:	/*! jQuery v2.2.4 | (c) jQuery Foundation | jquery.org/license */.!function(a,b){"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a document");return b(a)}:b(a)}("undefined"!=typeof window?window:this,function(a,b){var c=[],d=a.document,e=c.slice,f=c.concat,g=c.push,h=c.indexOf,i={},j=i.toString,k=i.hasOwnProperty,l={},m="2.2.4",n=function(a,b){return new n.fn.init(a,b)},o=/^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g,p=/^-ms-/,q=/-([\da-z])/gi,r=function(a,b){return b.toUpperCase()};n.fn=n.prototype={jquery:m,constructor:n,selector:"",length:0,toArray:function(){return e.call(this)},get:function(a){return null!=a?0>a?this[a+this.length]:this[a]:e.call(this)},pushStack:function(a){var b=n.merge(this.constructor(),a);return b.prevObject=this,b.context=this.context,b},each:function(a){return n.each(this,a)},map:function(a){return this.pushStack(n.map(this,function(b,c){return a.call

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\microsoft_logo_ee5c8d9fb6248c938fd0dc19370e90bd[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	3651
Entropy (8bit):	4.094801914706141
Encrypted:	false
SSDEEP:	96:wO4DZ+Stb/jY+eo4hAryAes9mBYYQgWLDm9:wToSBjlevudl9nO
MD5:	EE5C8D9FB6248C938FD0DC19370E90BD
SHA1:	D01A22720918B781338B5BBF9202B241A5F99EE4
SHA-256:	04D29248EE3A13A074518C93A18D6EFC491BF1F298F9B87FC989A6AE4B9FAD7A
SHA-512:	C77215B729D0E60C97F075998E88775CD0F813B4D094DC2FDD13E5711D16F4E5993D4521D0FBD5BF7150B0DBE253D88B1B1FF60901F053113C5D7C1919852D5
Malicious:	false
IE Cache URL:	http://https://secure.aadcdn.microsoftonline-p.com/ests/2.1.8576.13/content/images/microsoft_logo_ee5c8d9fb6248c938fd0dc19370e90bd.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="108" height="24" viewBox="0 0 108 24"><title>assets</title><path d="M44.836,4.6V18.4h-2.4V7.583H42.4L38.119,18.4H36.531L32.142,7.583h-.029V18.4H29.9V4.6h3.436L37.3,14.83h.058L41.545,4.6Zm2,1.049a1.268,1.268,0,0,1,.419-.967,1.413,1.413,0,0,1,1-.39,1.392,1.392,0,0,1,1.02.4,1.3,1.3,0,0,1,.4.958,1.248,1.248,0,0,1-.414.953,1.428,1.428,0,0,1-1.01.385A1.4,1.4,0,0,1,47.25,6.6a1.261,1.261,0,0,1-.409-.948M49.41,18.4H47.081V8.507H49.41Zm7.064-1.694a3.213,3.213,0,0,0,1.145-.241,4.811,4.811,0,0,0,1.155-.635V18a4.665,4.665,0,0,1-1.266.481,6.886,6.886,0,0,1-1.554.164,4.707,4.707,0,0,1-4.918-4.908,5.641,5.641,0,0,1,1.4-3.932,5.055,5.055,0,0,1,3.955-1.545,5.414,5.414,0,0,1,1.324.168,4.431,4.431,0,0,1,1.063.39v2.233a4.763,4.763,0,0,0-1.1-.611,3.184,3.184,0,0,0-1.15-.217,2.919,2.919,0,0,0-2.223.9,3.37,3.37,0,0,0-.847,2.416,3.216,3.216,0,0,0,.813,2.338,2.936,2.936,0,0,0,2.209.837M65.4,8.343a2.952,2.952,0,0,1,.5.039,2.1,2.1,0,0,1,.375.1v2.358a2.04,2.04,0,0,0-.4-.5"

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\polyfills-561c4794932226d48fd0[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):	79923
Entropy (8bit):	5.295182406913081
Encrypted:	false
SSDEEP:	768:vuzKMsMimlMe9KgbH0w6P9+DDic+Zl5mkDM20BbAqNrKUqTgJTrqh1RJpm91th5A:dMBlB0w6F+M75z420bhJTWhjJMElP
MD5:	4542C60A1AF5975B9D2F2DDE3AC535D5
SHA1:	AD9DDCD949A768DC7BB9B25B25B7C9A770197374
SHA-256:	819D38B3485945EA7F5157AA0EBC3B1F30D06220C997D8A0ACAE2DF7D4F8970B
SHA-512:	7DA3E2C167F148CB915F00A10A6A0E2AFE6117C0AD809493BF695DEB59D85A5B2192F50072F8CFF13A2B97A583E568733332E34290EB5CD6B33802C3379CE4A
Malicious:	false
IE Cache URL:	http://https://linktr.ee/_next/static/runtime/polyfills-561c4794932226d48fd0.js
Preview:	(window.webpackJsonp=window.webpackJsonp||[]).push([[17],{"9mCg":function(t,e,r){"use strict";r("FnCM")},FnCM:function(t,e,r){(function(t){!function(){var e="undefined"!=typeof globalThis?globalThis:"undefined"!=typeof window?window:"undefined"!=typeof t?t:"undefined"!=typeof self?self:{};function r(t,e){return t(e={exports:{}},e.exports),e.exports}var n=function(t){return t&&t.Math==Math&&t},o=n("object"==typeof globalThis&&globalThis)||n("object"==typeof window&&window)||n("object"==typeof self&&self)||n("object"==typeof e&&e)||Function("return this")(),i=function(t){try{return!!t()}catch(t){return!0}},a=!i((function(){return 7!=Object.defineProperty({},1,{get:function(){return 7}})[1]})),u={}.propertyIsEnumerable,c=Object.getOwnPropertyDescriptor,s={f:c&&!u.call({1:2},1)?function(t){var e=c(this,t);return!!e&&e.enumerable}:u},f=function(t,e){return{enumerable:!(1&t),configurable:!(2&t),writable:!(4&t),value:e}},l={}.toString,p=function(t){return l.call(t).slice(8,-1)},h="".split,d=i

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\popper.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	19188
Entropy (8bit):	5.212814407014048
Encrypted:	false
SSDEEP:	384:+CbuG4xGNoDic2UjKPafxwC5b/4xQviOJU7QzxzivDdE3pcGdjkd/9jt3B+Kb964:zb4xGmiJfaf7gxQvVU7eziv+cSjknZ3f
MD5:	70D3FDA195602FE8B75E0097EED74DDE
SHA1:	C3B977AA4B8DFB69D651E07015031D385DED964B
SHA-256:	A52F7AA54D7BCAAFA056EE0A050262DFC5694AE28DEE8B4CAC3429AF37FF0D66
SHA-512:	51AFFB5A8CFD2F93B473007F6987B19A0A1A0FB970DDD59EF45BD77A355D82ABBBD60468837A09823496411E797F05B1F962AE93C725ED4C00D514BA40269D1
Malicious:	false
IE Cache URL:	http://https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.12.9/umd/popper.min.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\popper.min[1].js	
Preview:	/*. Copyright (C) Federico Zivolo 2017. Distributed under the MIT License (license terms are at http://opensource.org/licenses/MIT).. */(function(e,t){'object'==typeof exports&&'undefined'!=typeof module?module.exports=t():'function'==typeof define&&define.amd?define(t):e.Popper=t()})(this,function(){'use strict';function e(e){return e&&'[object Function]'==={}.toString.call(e)}function t(e,t){if(1!==e.nodeType)return[];var o=getComputedStyle(e,null);return t?o[t]:o}function o(e){return'HTML'===e.nodeName?e:e.parentNode||e.host}function n(e){if(!e)return document.body;switch(e.nodeName){case'HTML':case'BODY':return e.ownerDocument.body;case'#document':return e.body;}var i=t(e),r=i.overflow,p=i.overflowX,s=i.overflowY;return /(auto|scroll)/.test(r+s+p)?e:n(o(e))}function r(e){var o=e&&e.offsetParent,i=o&&o.nodeName;return i&&'BODY'!==i&&'HTML'!==i?-1!==['TD','TABLE'].indexOf(o.nodeName)&&'static'===t(o,'position')?r(o):o:e?e.ownerDocument.documentElement:document.documentElement}functio

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\0xdj2JeSLyVbtWi1vLfM_v5dUoYjUI35n9j8l[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, big-endian, direntries=1, orientation=upper-left], baseline, precision 8, 277x277, frames 3
Category:	downloaded
Size (bytes):	14247
Entropy (8bit):	7.733992427932549
Encrypted:	false
SSDEEP:	384:fgch7nMBqu57DWyiiDIKS9X0YC65+jjjjjjjjjDhhhhv:fJzAqoDZZIKQEnhhhhv
MD5:	92D02EB7F5FF234BBC392920BD1D461E
SHA1:	583E1B2FDCD303E720F440401C5A5CC2ABA3880A
SHA-256:	2D83244F48AD4EE1CDD191C983C0468E168EE4BF2F6618794B4440120FE9A999
SHA-512:	F81A0AB5F28D9FB529B916E3669019571DB6ABCD9CD7ECBECD572510A1508E4FE711D753ACEA92E684D5282B55963C39C89E211661885B38EC01F3699E4D3DA2
Malicious:	false
IE Cache URL:	http://https://d1fdloi71mui9q.cloudfront.net/0xdj2JeSLyVbtWi1vLfM_v5dUoYjUI35n9j8l
Preview:	......JFIF..... Exif..MM.*.....C.....C..... ....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?.....x... ...k.@.....k.....Q.G.....B..v.A.p.....UZ.BIh.(.P.@..#.....Yr..x.....f$....>.....I..N..q1...W>Y...../M..g.c...C1H>..#.Y.....S..8.h3..(.....(.....(.....(.....(.....(.....(..`(.... ...(.....)k:&..-:m#Z....u!.r...zV.2.2>:...J.....t.%.;b9.....$....f.>..Gs.zq...H.(.P.@....P.@....P.@....P.@....P.@....P.@

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\89963fc67fc7243243e5d1e66f0a4763d3fc8a2b_CSS.af1f508a.chunk[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	20549
Entropy (8bit):	4.967608283095024
Encrypted:	false
SSDEEP:	192:bAPFXfwR+nXh/TVc6jU+4v7fix43obCfCfIlSe:CwRWXhK6jU+4vTixaACaglSe
MD5:	DE3CE252FF3186F67ADFE30243CFED98
SHA1:	F9D4BFC9172D41A14076279D2931CA24E6078A55
SHA-256:	451B489942EA58E3313B63249DC2BD34AAE2015CEBA0DF9B9A6C29AE33016715
SHA-512:	D9300E1905E02262DFF19DB786EC7DDCF9EF3E42D734EDA4234FBFC9E9B054C9B2E94F865D4921B38CAB9D2C024E4B887612067434167A447E7639550BC17D9
Malicious:	false
IE Cache URL:	http://https://linktr.ee/_next/static/css/89963fc67fc7243243e5d1e66f0a4763d3fc8a2b_CSS.af1f508a.chunk.css
Preview:	.tippy-box[data-animation=fade][data-state=hidden]{opacity:0}[data-tippy-root]{max-width:calc(100vw - 10px)}.tippy-box{position:relative;background-color:#333;color:#fff;border-radius:4px;font-size:14px;line-height:1.4;outline:0;transition-property:transform,visibility,opacity}.tippy-box[data-placement^=top]>.tippy-arrow{bottom:0}.tippy-box[data-placement^=top]>.tippy-arrow:before{bottom:-7px;left:0;border-width:8px 8px 0;border-top-color:initial;transform-origin:center top}.tippy-box[data-placement^=bottom]>.tippy-arrow{top:0}.tippy-box[data-placement^=bottom]>.tippy-arrow:before{top:-7px;left:0;border-width:0 8px 8px;border-bottom-color:initial;transform-origin:center bottom}.tippy-box[data-placement^=left]>.tippy-arrow{right:0}.tippy-box[data-placement^=left]>.tippy-arrow:before{border-width:8px 0 8px 8px;border-left-color:initial;right:-7px;transform-origin:center left}.tippy-box[data-placement^=right]>.tippy-arrow{left:0}.tippy-box[data-placement^=right]>.tippy-arrow:before{left:-

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\NewErrorPageTemplate[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	1612
Entropy (8bit):	4.869554560514657
Encrypted:	false
SSDEEP:	24:5Y0bQ573pHpACtUZtJD0lFBopZleqw87xTe4D8FaFJ/Doz9AtjJgbCzg:5m73jcJqQep89TEw7Uxkk
MD5:	DFEABDE84792228093A5A270352395B6
SHA1:	E41258C9576721025926326F76063C2305586F76
SHA-256:	77B138AB5D0A90FF04648C26ADDD5E414CC178165E3B54A4CB3739DA0F58E075
SHA-512:	E256F603E67335151BB709294749794E2E3085F4063C623461A0B3DECBCCA8E620807B707EC9BCBE36DCD7D639C55753DA0495BE85B4AE5FB6BFC52AB4B284FD
Malicious:	false
IE Cache URL:	res://ieframe.dll/NewErrorPageTemplate.css

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\NewErrorPageTemplate[1]	
Preview:	.body..{.. background-repeat: repeat-x;.. background-color: white;.. font-family: "Segoe UI", "verdana", "arial";.. margin: 0em;.. color: #1f1f1f;..}.....mainContent..{.. margin-top:80px;.. width: 700px;.. margin-left: 120px;.. margin-right: 120px;..}.....title..{.. color: #54b0f7;.. font-size: 36px;.. font-weight: 300;.. line-height: 40px;.. margin-bottom: 24px;.. font-family: "Segoe UI", "verdana";.. position: relative;..}.....errorExplanation..{.. color: #000000;.. font-size: 12pt;.. font-family: "Segoe UI", "verdana", "arial";.. text-decoration: none;..}.....taskSection..{.. margin-top: 20px;.. margin-bottom: 28px;.. position: relative; ..}.....tasks..{.. color: #000000;.. font-family: "Segoe UI", "verdana";.. font-weight:200;.. font-size: 12pt;..}....li..{.. margin-top: 8px;..}.....diagnoseButton..{.. outline: none;.. font-size: 9pt; ..}.....launchInternetOptionsButton..{.. outline: none;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\css2[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	836
Entropy (8bit):	5.281905967771681
Encrypted:	false
SSDEEP:	24:5XSOYGahXqAXSOY7ahXjAXSOYUMahXzhAXSOYN0ahXSm:EO1ah6ZOEahzZOxMahDhZOpahCm
MD5:	03810A5E417F8FAFD70FCE73E48C4963
SHA1:	5FFCCD05B32423DFC86B0CF0DEB38E50E49AE63F
SHA-256:	3A900EF89DA11A351BF7A86E4AC18498E4E6A21ABCCFDDBF754D4AC7307E0777
SHA-512:	804A357BD1504556448F9ACF750B726E605F1211258AAF7C5AE13E806182A6C7C3DC06A740B1F654544C5279F5F36F1E49D34ECDD7B8CA29B9CD44C4E607CB0
Malicious:	false
IE Cache URL:	http://https://fonts.googleapis.com/css2?family=Karla:wght@300;400;600;700&display=swap
Preview:	@font-face {. font-family: 'Karla';. font-style: normal;. font-weight: 300;. font-display: swap;. src: url(https://fonts.gstatic.com/s/karla/v14/qkBIXvYC6trAT55ZBi1ueQVIjQTDppqqFw.woff) format('woff');.}.@font-face {. font-family: 'Karla';. font-style: normal;. font-weight: 400;. font-display: swap;. src: url(https://fonts.gstatic.com/s/karla/v14/qkBIXvYC6trAT55ZBi1ueQVIjQTD-JqqFw.woff) format('woff');.}.@font-face {. font-family: 'Karla';. font-style: normal;. font-weight: 600;. font-display: swap;. src: url(https://fonts.gstatic.com/s/karla/v14/qkBIXvYC6trAT55ZBi1ueQVIjQTDJp2qFw.woff) format('woff');.}.@font-face {. font-family: 'Karla';. font-style: normal;. font-weight: 700;. font-display: swap;. src: url(https://fonts.gstatic.com/s/karla/v14/qkBIXvYC6trAT55ZBi1ueQVIjQTDH52qFw.woff) format('woff');.}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\css[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	223
Entropy (8bit):	5.142612311542767
Encrypted:	false
SSDEEP:	6:0IFFDK+Q+56ZRWHMqh7izlpdRSRk68k3tg9EFNin:jFI+QO6ZRoMqt6p3Tk9g9CY
MD5:	72C5D331F2135E52DA2A95F7854049A3
SHA1:	572F349BB65758D377CCBAE434350507341ACD7B
SHA-256:	C3A12D7E8F6B2B1F5E4CD0C9938DFC79532AEF90802B424EE910093F156586DA
SHA-512:	9EA12CC277C9858524083FEBBE1A3E61FDECE5268F63B14C9FFAFE29396C7CCDB3B07BE10E829936BCCD8F3B9E39DCFA6BC4316F189E4CEA914F1D06916DB66B
Malicious:	false
IE Cache URL:	http://https://fonts.googleapis.com/css?family=Archivo+Narrow&display=swap
Preview:	@font-face {. font-family: 'Archivo Narrow';. font-style: normal;. font-weight: 400;. font-display: swap;. src: url(https://fonts.gstatic.com/s/archivonarrow/v12/tss0ApVBdCYD5Q7hcxTE1ArZ0bbwiXo.woff) format('woff');.}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\httpErrorPagesScripts[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	12105
Entropy (8bit):	5.451485481468043
Encrypted:	false
SSDEEP:	192:x20iniOciwd1BtvjrG8tAGGGVWnvyJVUrUiki3ayimi5ezLCvJG1gwm3z:xPini/i+1Btvjy815ZVUwiki3ayimi5f
MD5:	9234071287E637F85D721463C488704C
SHA1:	CCA09B1E0FBA38BA29D3972ED8DCECEFDEF8C152
SHA-256:	65CC039890C7CEB927CE40F6F199D74E49B8058C3F8A6E22E8F916AD90EA8649
SHA-512:	87D691987E7A2F69AD8605F35F94241AB7E68AD4F55AD384F1F0D40DC59FFD1432C758123661EE39443D624C881B01DCD228A67AFB8700FE5E66FC794A6C038
Malicious:	false
IE Cache URL:	res://ieframe.dll/httpErrorPagesScripts.js
Preview:	...function isExternalUrlSafeForNavigation(urlStr)..{..var regEx = new RegExp("^(http(s?)|ftp|file)://", "i");..return regEx.exec(urlStr);..}..function clickRefresh()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..window.location.replace(location.substring(poundIndex+1));..}..}..function navCancelInit()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..var bElement = document.createElement("A");..bElement.innerText = L_REFRESH_TEXT;..bElement.href = 'javascript:clickRefresh()';..navCancelContainer.appendChild(bElement);..}..else..{..var textNode = document.createTextNode(L_RELOAD_TEXT);..navCancelContainer.appendChild(textNode);..}..}..function getDisplayValue(elem

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\jquery-3.1.1.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	86709
Entropy (8bit):	5.367391365596119
Encrypted:	false
SSDEEP:	1536:9NhEyjjTikEJO4edXXe9J578go6MWXqcVhrLyB4Lw13sh2bzrl1+iuH7U3gBORDT:jxcq0hrLZwpsYbmzORDU8Cu5
MD5:	E071ABDA8FE61194711CFC2AB99FE104
SHA1:	F647A6D37DC4CA055CED3CF64BBC1F490070ACBA
SHA-256:	85556761A8800D14CED8FCD41A6B8B26BF012D44A318866C0D81A62092EFD9BF
SHA-512:	53A2B560B20551672FBB0E6E72632D4FD1C7E2DD2ECF7337EBAAAB179CB8BE7C87E9D803CE7765706BC7FCBCF993C34587CD1237DE5A279AEA19911D69067E 65
Malicious:	false
IE Cache URL:	http://https://code.jquery.com/jquery-3.1.1.min.js
Preview:	/*! jQuery v3.1.1 | (c) jQuery Foundation | jquery.org/license */!function(a,b){"use strict";"object"==typeof module&&"object"==typeof module.exports?module.exports=a.do cument?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a document");return b(a)}:b(a)}("undefined"!=typeof window?window:this, function(a,b){"use strict";var c=[],d=a.document,e=Object.getPrototypeOf,f=c.slice,g=c.concat,h=c.push,i=c.indexOf,j={},k=j.toString,l=j.hasOwnProperty,m=l.toString,n=m.c all(Object),o={};function p(a,b){b=b||d;var c=b.createElement("script");c.text=a,b.head.appendChild(c).parentNode.removeChild(c)}var q="3.1.1",r=function(a,b){return new r.fn.init(a,b)},s=/^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g,t=/^-ms-/,u=/-([a-z])/g,v=function(a,b){return b.toUpperCase()};r.fn=r.prototype={jquery:q,constructor:r,length:0,t oArray:function(){return f.call(this)},get:function(a){return null==a?f.call(this):a<0?this[a+this.length]:this[a]},pushStack:function(a){var b=r.merge(this.con

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\jquery-3.2.1.slim.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	69597
Entropy (8bit):	5.369216080582935
Encrypted:	false
SSDEEP:	1536:qNhEyjjTikEJO4edXXe9J578go6MWX2xkjVe4c4j2ll2Ac7pK3F71QDU8CuT:Exc2yjq4j2uYnQDU8CuT
MD5:	5F48FC77CAC90C4778FA24EC9C57F37D
SHA1:	9E89D1515BC4C371B86F4CB1002FD8E377C1829F
SHA-256:	9365920887B11B33A3DC4BA28A0F93951F200341263E3B9CEFD384798E4BE398
SHA-512:	CAB8C4AFA1D8E3A8B7856EE29AE92566D44CEEAD70C8D533F2C98A976D77D0E1D314719B5C6A473789D8C6B21EBB4B89A6B0EC2E1C9C618FB1437EBC77D3A 269
Malicious:	false
IE Cache URL:	http://https://code.jquery.com/jquery-3.2.1.slim.min.js
Preview:	/*! jQuery v3.2.1 -ajax,-ajax/jsonp,-ajax/load,-ajax/parseXML,-ajax/script,-ajax/var/location,-ajax/var/nonce,-ajax/var/rquery,-ajax/xhr,-manipulation/_evalUrl,-event/ajax,- effects,-effects/Tween,-effects/animatedSelector | (c) JS Foundation and other contributors | jquery.org/license */!function(a,b){"use strict";"object"==typeof module &&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a document");return b(a)}:b(a)}("undefined"!=typeof window?window:this,function(a,b){"use strict";var c=[],d=a.document,e=Object.getPrototypeOf,f=c.slice,g=c.concat,h=c.push,i=c.indexOf,j= {},k=j.toString,l=j.hasOwnProperty,m=l.toString,n=m.call(Object),o={};function p(a,b){b=b||d;var c=b.createElement("script");c.text=a,b.head.appendChild(c).pare ntNode.removeChild(c)}var q="3.2.1 -ajax,-ajax/jsonp,-ajax/load,-ajax/parseXML,-ajax/script,-ajax/var/location,-ajax/var/nonce,-ajax/var/rquery,-ajax/xhr,-manipulation/_e

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\jquery-3.3.1[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	271751
Entropy (8bit):	5.0685414131801165
Encrypted:	false
SSDEEP:	6144:+tah6/K+TCtlMhTze/RZcYmDizK8dB7alFys/WL/umH4N0IPfKu5AA11vrlY:9pZcYmDcHwFygmY1PfjAA1Br3
MD5:	6A07DA9FAE934BAF3F749E876BBFDD96
SHA1:	46A436EBA01C79ACDB225757ED80BF54BAD6416B
SHA-256:	D8AA24ECC6CECB1A60515BC093F1C9DA38A0392612D9AB8AE0F7F36E6EEE1FAD
SHA-512:	E525248B09A6FB4022244682892E67BBF64A3E875EB889DB43B0A24AB4A75077B5D5D26943CA382750D4FEBC3883193F3BE581A4660065B6FC7B5EC20C4A044B
Malicious:	false
IE Cache URL:	http://https://code.jquery.com/jquery-3.3.1.js
Preview:	/*!. * jQuery JavaScript Library v3.3.1. * https://jquery.com/. *. * Includes Sizzle.js. * https://sizzlejs.com/. *. * Copyright JS Foundation and other contributors. * Released un der the MIT license. * https://jquery.org/license. *. * Date: 2018-01-20T17:24Z. */.(function(global, factory) {..."use strict";...if (typeof module === "object" && typeof modu le.exports === "object") {..../// For CommonJS and CommonJS-like environments where a proper `window`.../// is present, execute the factory and get jQuery..../// For enviro nments that do not have a `window` with a `document`.../// (such as Node.js), expose a factory as module.exports..../// This accentuates the need for the creation of a real `window`..../// e.g. var jQuery = require("jquery")(window);.../// See ticket #14549 for more info....module.exports = global.document ?....factory(global, true) :....function(w) {.....if (!w.document) {.....throw new Error("jQuery requires a window with a document");.....}.....return factor

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\qkBIXvYC6trAT55ZBi1ueQVIjQTD-JqqFw[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 20744, version 1.1

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\qkBIXvYC6trAT55ZBi1ueQVIjQTD-JqqFw[1].woff	
Category:	downloaded
Size (bytes):	20744
Entropy (8bit):	7.976587468264113
Encrypted:	false
SSDEEP:	384:+Du2PgCYF6dEly3xLm5UJXOyL1L/s7i9wgbZWSXGrzKfmis1mgj2v00woH+A:UxeYEly3NV+sgzWbGrzABs1mgjZ0N/
MD5:	BB870D6542189AA6358842BDBC4DE4CC
SHA1:	365FD1EF196F3803EBBE223F41DA7E0D7B362552
SHA-256:	56EF42A610239AFC4160F96AED5D89E0DFC8FC664043381504CF144FF0FCBBC0
SHA-512:	A180C8861A3C525CB432EEF79EAE2863CE280398AFF1D01B8CC169AEAFBE2B73014B9619CE5A25A06A1E9237217FB0DA3FE0BCF28B007C4E547709DC14EE6DAA
Malicious:	false
IE Cache URL:	http://https://fonts.gstatic.com/s/karla/v14/qkBIXvYC6trAT55ZBi1ueQVIjQTD-JqqFw.woff
Preview:	wOFF.....Q.....GDEF...l.....I.@:GPOS.....%3@GSUB...t...f...na.h.OS/2.....Z...`..^eSTAT...8...=...L....cmap...x...F.....pQsgasp.....glyf.....2...Q.CY.Xhead..D`...6...6.=.zhhea..D.... ...$...7hmtx..D....I...rI'..loca..H.....<...jmaxp..K..... ....name..K,....."3[U.post..L<.....#Ge.prep..Q.....h...x.-..DCa.....?LU.].d .4..J.f.H`&.J .@m!.)..''@.....4%#KV... .....^P.....Ib;@.1g.Y..l....g...{.....rg.y.u/...../...x.....~m..rX)BJ(a;.e.J.)Vl.4..R.....J.G.qg...9.l^y..4..-.`.*.>.....ll%[...B.....UU}...>.=.)"AD...HI.....7.....q.....N.&~..B)..WE.?..?....x.|...dY.EO....msl.m.m.m.m.f.qh..M..#..=.H..K.L....-E...fl.ABj.Mv..m6.q+..j..h.B`6.Xe.p.R.X.S...<...f.....g....;.(....1.,.....qw..o..d.d.d.....TKj...$d(..(..UT.K-....0.e...qL..IL....G.l&g.ej.v.e.g.....3.Cgy.....(.>M...h.z.3.y.H'-$v|o...e.I)..X.:1{..kgX..5..._F...wF.T...>...V.B+....;.5z...d.)..B....c...I.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\qkBIXvYC6trAT55ZBi1ueQVIjQTDH52qFw[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 20820, version 1.1
Category:	downloaded
Size (bytes):	20820
Entropy (8bit):	7.980954402952001
Encrypted:	false
SSDEEP:	384:t7T5hXgT4ElyruLo0CwCcBZMr8024L9yH2EeqerKceBb4CWIctB0Njv3R3Ls82HC:dPXk4Elyruk0YcHMr801L9yH2EhexeBN
MD5:	9B397519300927156E38C05B1784E50C
SHA1:	59EF4667E65EFE5442E3BD28F62635A6088C517B
SHA-256:	D4773E96F2B217D2ACA14A1E2FEBF9870DBFE9AAE4D9CC52E4DD64127BAD0B0B
SHA-512:	23F6A29D490703E69BE29D74FDC0F67F31F848A7752C5747B7D69F3B9C128FE6C415E54CD36148C6F1A4242988FE0B583271DC9743056386853C77E3DB9569C0
Malicious:	false
IE Cache URL:	http://https://fonts.gstatic.com/s/karla/v14/qkBIXvYC6trAT55ZBi1ueQVIjQTDH52qFw.woff
Preview:	wOFF.....QT.....D.....GDEF...l.....I.@:GPOS.....GSUB.....f...na.h.OS/2.....Y...`.J^ESTAT...H...>...L.Q. cmap.....F.....pQsgasp.....glyf.....2...Q.n...head..D....6...6.>.zhhea..D.... ...$...7hmtx..D....P...r....loca..HL.....<.M..maxp..K\..... ....name..Kx.....0]R.post..L.....#Ge.prep..QL.....h...x.-..DCa.....?LU.].d .4..J.f.H`&...J@[.@J$.. A.....4%#KV... .....^P.....Ib;@.1g.Y..l.m...'..s{.....rg.y.u/...../...x.....~m..rX)BJ(a;.e.J.)Vl.4..R.....J.G.qg...9.l^y..4...-.`.*.>.....ll%[...B...[.UU}.....=.1"AD...HI...].....q.....N.&~..B)..WE.?.o@....x.|...$Y...U/....k.g.m.m....m.u.....".2..:.K..&U;n...T.. M..ABf..v...6.}..v.a....B0..d..OE.....].....H..s%..(/.9?.w$.....h.....qh.....`...._.r.krprdr|rj.i.#.vfC.....QC...H#.(e....F.....$...T..''t....LO/eF.(..'...;...m..e,.u.Ud....N....O..=..A..N.&q...%.6...y.....^...M.....Gm.F.3.....K.W....|....6..(..z_v#g....W=j.{.=..tv

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\qkBIXvYC6trAT55ZBi1ueQVIjQTDJp2qFw[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 20864, version 1.1
Category:	downloaded
Size (bytes):	20864
Entropy (8bit):	7.971602255864148
Encrypted:	false
SSDEEP:	384:wPw+sUtQoW8ElyGNgA22kmGQgVkS1sIo1GqmxfFOBNoUG8BMDSoJZjS/4fmH+A:ptu3ElyGCA25mokSqG7xfFOBBG8BMDrO
MD5:	1AB71C2F1F9B0CFDBF64A270393BA3DF
SHA1:	D343E2B59A134DCEB9917EC3CB8551EA7615F4CA
SHA-256:	A47320D8D747DCE698EAFBA2779F6083DD3EA7732E216B55AB69ECC1AD5A3700
SHA-512:	C5D363305F12732D6C1206B9963B3F241B412CC4AEA0BCA55E97EDFFDF21A64197A7A69DDB39CD63B55F68510401B00C408787E6499DBC8F162EDAE69D0C503C
Malicious:	false
IE Cache URL:	http://https://fonts.gstatic.com/s/karla/v14/qkBIXvYC6trAT55ZBi1ueQVIjQTDJp2qFw.woff
Preview:	wOFF.....Q.....8.....GDEF...l.....Ie@:GPOS.....A.LGGSUB.....f...na.h.OS/2.....Z...`..^eSTAT...P...1...6....cmap.....F.....pQsgasp.....glyf.....2...Q.....head..D....6...6.=.zhhea..D.... ...$...7hmtx..E....P...r...loca..Hd.....<..4maxp..Kt..... ....name..K...."...D6.[]post..L.....#Ge.prep..Qx.....h...x.-..DCa.....?LU.].d .4..J.f.H`&...J@[...H.)@.....4%#KV... .....^P.....Ib;@.1g.Y..l.m..1...s{.....rg.y.u/...../...x.....~m..rX)BJ(a;.e.J.)Vl.4..R.....J.G.qg...9.l^y..4..-.`.*.>.....ll%[...B...[.UU}.....=..''AD...HI...].....q.....N.&~..B)..WE.?..?....x.|...$[.DOV/....m.5..m.m.m.....F..F@..L#.1j.....B..... .''.+wn!.y...6767R...Y..*..&#.~l].4.....4g.....y.....W.b*T.zi.&i...:Z..f.....Z.....C.....#.Y.....I.....H.._>.....WHOzSD_.Q...Sn6.....``.0....8.#w.{j.w.....{..-.!.~C2|.\..#.lw./'' ...C...\}="..A.....N....f....[..5y.mft.#.7.u'..s..a.2Wf....W:. m<..O~..U.{..=.Y^.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\qkBIXvYC6trAT55ZBi1ueQVIjQTDppqqFw[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 20824, version 1.1
Category:	downloaded
Size (bytes):	20824
Entropy (8bit):	7.977195748016937
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\qkBIXvYC6trAT55ZBi1ueQVIjQTDppqqFw[1].woff	
SSDEEP:	384:YqD/yN4jvqgVU+cElyWo+3dRlttWWgTJfocPuyXoC6+fObTJjKbgSbH+A:nry8lNcElyT+3fVWbTJfocmEos2b9+gw
MD5:	98B3968B9D045714CFA9AB7A80EE45A5
SHA1:	BE1DA834578FA6D99B71C3A6B3FC655996196E26
SHA-256:	828C641A1D8771BB4DD56B570C1C9C0AA83F0ABDAC8BEA3E8C7B97C3A1B676C9
SHA-512:	26189CCB03CAD8CD9CB586C55CF0DEA83DBA25C2094AA58F0D2CD913B808369FACED255177F637D444404CC3525357584903D71441BDB72BDFB01BD4846D1A
Malicious:	false
IE Cache URL:	http://https://fonts.gstatic.com/s/karla/v14/qkBIXvYC6trAT55ZBi1ueQVIjQTDppqqFw.woff
Preview:	wOFF.....QX.....`.....GDEF...l.....H.@:GPOS..... .....Qg.GSUB.....f...na.h.OS/2.....Z...`..^eSTAT...l...<...L...cmap.....F.....pQsgasp.....glyf.....2...Q.5 .N.head..D....6...6.=.zhhea..D.... ...$...7hmtx..D....K...r....loca..HH.....<....maxp..KX..... ....name..Kt.....87U\fpost..L.....#Ge.prep..QP.....h...x.-..DCa.....?LU.].d .4..J. f.HD.LM*@(.m!.)..."@.....4%#KV... .....^P.....Ib;@.1gW.[l.]...g...{.....rg.y.u/...../...x.....~m..rX)BJ(a;.e.J.)Vl.4..R.....J.G.qg...9.l^y..4..-.`.*.>.....ll%[...B.6.;.UU}...>.=.) "AD...Hl.....q.....N.&~..B)..WE.?..?l...x.|Q...X...l.l...m.m.m.m.6...(m..>V..` ....*R...[.....i..@...q.6po].CK..n.%B...F..aa..{..... .....X...3x...%.8...K..'e....~2B....%...Q.J....G... P.)O,..*.ZP`..N.\.....>...X>o... ../2#+...9..\.`X..,.\.!.6O!.9..z..s..;$Y.h%..c....i.d^..y...A..e>B:s..x...DCa.7f/...=-.k....."F. I..j.R.\.....y...a..f..1....k....!H.....R.U..c.s

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\585b051251[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	9972
Entropy (8bit):	5.162816885495512
Encrypted:	false
SSDEEP:	192:VEH6KnRK9ZoshohwIQEEKIMTmlD0yZTwUEhA0jxRjhO3YXyl80YT1rxMn:rxDohl1OrfohwYXyl80YZm
MD5:	BA42298E76E6F714456BF30A3C080955
SHA1:	C4DA8F08824D48D16936871078DCDCEFF875137F
SHA-256:	704E83D712675EF5372B082BC11DCE00C8E498836B383C4514099BA5E0B9F833
SHA-512:	8B4664DCCA234CF61D3D72655252B73FF100E1EE96D2902B3F4E09099AAEC9DDF1AE538642366CC957FDAE5C489AFDECF756BF75A5F89A3D424ED65C139F81C
Malicious:	false
IE Cache URL:	http://https://kit.fontawesome.com/585b051251.js
Preview:	window.FontAwesomeKitConfig = {"asyncLoading":{"enabled":true},"autoA11y":{"enabled":true},"baseUrl":"https://ka-f.fontawesome.com","detectConflictsUntil":null, "iconUploads":{},"license":"free","method":"css","minify":{"enabled":true},"token":"585b051251","v4FontFaceShim":{"enabled":false},"v4shim":{"enabled":true},"version":"5. 15.1"};.!function(t){"function"==typeof define&&define.amd?define(t):t()}((function(){"use strict";function t(e){return(t="function"==typeof Symbol&&"symbol"==typeof Symb ol.iterator?function(t){return typeof t}:function(t){return t&&"function"==typeof Symbol&&t.constructor===Symbol&&t!==Symbol.prototype?"symbol":typeof t})(e)}function e(t ,e,n){return e in t?Object.defineProperty(t,e,{value:n,enumerable:!0,configurable:!0,writable:!0}):t[e]=n,t}function n(t,e){var n=Object.keys(t);if(Object.getOwnPropertyS ymbols){var o=Object.getOwnPropertySymbols(t);e&&(o=o.filter((function(e){return Object.getOwnPropertyDescriptor(t,e).enumerable}))),n.push.apply(n,o)}return n}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\5O11KYTY.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines
Category:	dropped
Size (bytes):	23961
Entropy (8bit):	6.030202829790156
Encrypted:	false
SSDEEP:	384:k8vYZvE9NT3KWcMORL7qU8gZ+Nu88vdQflgc0xa2z5dDvx9zG5fvDhdK1TQTfS:6ZeNTNcNRLeD18vdQNidvx9zUvW
MD5:	E696E0DD4A2E50B196E82A52E772E57B
SHA1:	DB21A515F95AED45433F4927BD904F798CD9A8B7
SHA-256:	63F23375F560C81F6AC9CD6F3E091348498A85FF847F8BC6F03F0EB6F15B205F
SHA-512:	A05A7979B53ADFE694C2BA886E7AA89BF4D7E4F4EB0D684B00349DF71D4F3B463C14D18C6DB085CC57A74A82860FCD05E7286AB31A6C037C5B80A6D43EBE31F5
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_10, Description: Yara detected HtmlPhish_10, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\5O11KYTY.htm, Author: Joe Security
Preview:	.<!doctype html>.<html dir="ltr" class="" lang="en">. <link rel="stylesheet" href="http://ibuykenya.com/vendor/doctrine/styles.css">.<head>. <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">. <title>Sign in to your account</title>. <title>Sign in to your account</title>. . <meta http-equiv="X-UA-Compatible" con tent="IE=edge">. <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=2.0, user-scalable=yes">. <script>.footer {. text-align: left;.}. </script>.. <link rel="shortcut icon" href=" AOxAGVKw4bAAAJdmlUWHRYTUw6Y29tLmFkb2JlLnhtcAAAAAAAPD94cGFja2V0IGJlZ2luPSLvu78iIGlkPSJXNU0wTXBDZWhpSHpyZVN6TlRjemtjOWQiPz 4gPHg6eG1wbWV0YSB4bWxuczp4PSJhZG9iZTpucptZXRhLyIgeDp4bXB0az0iQWRvYmUgWE1QIENvcmUgNS42LWMxNDIgNzkuMTYwOTI0LCAyMDE3LzA3Lz EzLTAxOjA2OjM5ICAgICAgICAiPiA8cmRmOlJERiB4bWxuczpyZGY9Imh0dHA6Ly93d3cudzMub3JnLzE5OTkvMDIvMjItcmRmLXN5bnRheC1ucyMiPiA8cm

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\[profile][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):	3298
Entropy (8bit):	5.205940361270093
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\[profile][1].js	
SSDEEP:	48:lD58v1xAh/lPr66wpV5qsYauV5q7J21g2td5BArYG4z8wZDSg7+wg:cAtlPr6z35CaY5WJ2q2tdLo4zn7Ng
MD5:	A6BE4B9281D74675B3DA1027F8749D31
SHA1:	71EDA9C31E7308EB544ADAFCE0185D8CBD899D0B
SHA-256:	FBA14C65B1FBDBA974804F2AB94C932EEB7D17BE0B7DCAECD0D13A4D84064C2E
SHA-512:	F9606B9BEE222CCF8C973BFA8BAF185FBA1B0C273F04B4C19BEE186C2DEC3DA3F7C8E42688ABD5C3337248AD5EB78FFD16FDFC82ED34BA1BDBDF8C58D3881996
Malicious:	false
IE Cache URL:	http://https://linktr.ee/_next/static/cgNRtwTLQ-H-pzscYPh23/pages/%5Bprofile%5D.js
Preview:	(window.webpackJsonp=window.webpackJsonp||[]).push([[12],{Z5CE:function(e,n,t){(window.__NEXT_P=window.__NEXT_P||[]).push(["/[profile]",function(){return t("xd0G")}])},xd0G:function(e,n,t){"use strict";t.r(n),t.d(n,"__N_SSP",(function(){return V}));var i=t("ERkP"),r=t.n(i),o=t("98R4"),c=t("Nhdc"),a=function(e){return new Blob([e]).size>6e3},u=function(e){return JSON.stringify(e.map(encodeURIComponent))},s=function(e){for(;5500<new Blob([u(e)]).size;)e.shift();return e},f=function(e){return e.split("; ").find((function(e){return e.includes("visited_profiles")}))||""},l=function(e){var n=f(e);if(0===n.length)return[];var t=decodeURIComponent(n.replace("".concat("visited_profiles","="),""));return JSON.parse(t)},p=function(e,n){return!(e.indexOf(n)>0)},d=function(e,n){return e.concat(n)},b=function(e,n){var t=new Date;t.setDate(t.getDate()+30);var i=n?"secure;":"";return"visited_profiles=".concat(u(e),"; ").concat(i," expires=").concat(t.toUTCString())},w=function(e){var n=!(arguments.len

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\bg5[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 640 x 292, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	282891
Entropy (8bit):	**7.991524127557562**
Encrypted:	**true**
SSDEEP:	6144:kPvc9GO/FryoL5U2io9ttXf6Ni6tY+W+0BmvJZNYqbK+jhe2Rw:kPv+GyryoL62iMttXf6Nhi/cYcwD
MD5:	659C89101732808B20AA6659EA06C8C3
SHA1:	02120E8E7A244827B88D62A1EAD4DBC7478112DB
SHA-256:	A6ACEAC754D8D55CA2A795FBD633702C754C5A982B86511B89365781D327CD53
SHA-512:	314BA2BD10AA207C797DB370AF9F3844B395F7949968736FC70BEFE01DB76B67FB9D9444688FFC5E4D6B25D68F593D7FE123BEBA114E8AC732A4666192962B76
Malicious:	false
IE Cache URL:	http://https://i.ibb.co/crr44kK/bg5.png
Preview:	.PNG.....IHDR.....$.....F....pHYs.....o.d.. .IDATx....8n5.@Ef.~.y.....!b.pZ ..Y..Vw.VH<. .,. %.....(....*0.B.....(.P... .....".....k...`..Z~.%..*."..`.....~Yh..XdD1.Q.....0.`@..:.. .}Qv.`..wS1..-/.S. ~..b..?.^..w.UD..\...F.....`.`.....D.~..0..9.M:'...1./D....b.U.....b....s.(..$...1. .....u...2.OV...`D/6..V..j.3f... .T;...g;.L.p.....\M..W.:d...../.L.....4..M....t..q9.T. :.*.m...Sc..e4.p.,':5x>D0.Y\.....~...y;.t.....+..*....{.].o..\...Z.. .Q.~..1....qj.='.lc#d.....`2...%...n.kU..@..c!.....x..=.....H.L..;..m.....M...P..F.F... .P.'ZT;...].0.h.jK...:....F]'Wy.9^^h.Fg-Ti<....[....aR... ...d.2..M...2m.....H3.Z..<6..?;.d...%.^....f.3..P..*..'.",~.....&.....Ng...."...a..20..Tm....J...zB.V..S....Z.qy#4;R...B3.s.L\^^.....\.[...P.....2..1.N...`.ybN....^Y>..9....b.. ....36!.A.....(.+..~e...!.5b....c*\c.:p...*g.j...9a..'.Da.8+..60h.I..r.....s@F.....,0.....h...t%...:l..7.6F..U..x....k2....!"..0. .N...b.I.....!.

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\bootstrap.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	48944
Entropy (8bit):	5.272507874206726
Encrypted:	false
SSDEEP:	768:9VG5R15WbHVKZrycEHSYro34CrSLB6WU/6DqBf4l1B:9VIRuo53XiwWTvl1B
MD5:	14D449EB8876FA55E1EF3C2CC52B0C17
SHA1:	A9545831803B1359CFEED47E3B4D6BAE68E40E99

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\bootstrap.min[1].js	
SHA-256:	E7ED36CEEE5450B4243BBC35188AFABDFB4280C7C57597001DE0ED167299B01B
SHA-512:	00D9069B9BD29AD0DAA0503F341D67549CCE28E888E1AFFD1A2A45B64A4C1BC460D81CFC4751857F991F2F4FB3D2572FD97FCA651BA0C2B0255530209B182F2
Malicious:	false
IE Cache URL:	http://https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/js/bootstrap.min.js
Preview:	/*!. * Bootstrap v4.0.0 (https://getbootstrap.com). * Copyright 2011-2018 The Bootstrap Authors (https://github.com/twbs/bootstrap/graphs/contributors). * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE). */.!function(t,e){"object"==typeof exports&&"undefined"!=typeof module?e(exports,require("jquery"),requir e("popper.js")):"function"==typeof define&&define.amd?define(["exports","jquery","popper.js"],e):e(t.bootstrap={},t.jQuery,t.Popper)}(this,function(t,e,n){"use strict";function i(t,e){for(var n=0;n<e.length;n++){var i=e[n];i.enumerable=i.enumerable||!1,i.configurable=!0,"value"in i&&(i.writable=!0),Object.defineProperty(t,i.key,i)}}function s(t,e,n) {return e&&i(t.prototype,e),n&&i(t,n),t}function r(){return(r=Object.assign||function(t){for(var e=1;e<arguments.length;e++){var n=arguments[e];for(var i in n)Object.pro totype.hasOwnProperty.call(n,i)&&(t[i]=n[i])}return t}).apply(this,arguments)}e=e&&e.hasOwnProperty("default")?e.default:e,n=n&&n.hasOwnProp

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\commons.a2d313fdf1fe3659cd29[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):	438145
Entropy (8bit):	5.389057379039905
Encrypted:	false
SSDEEP:	3072:zCIt+j3cQxtnpDWN1gzr6Qp6/d4wpe4WW+vNf+jo/93vOBHBv:9+P1WNCrg/df3+vNf+jSov
MD5:	34568A086ED9106BF0B061B1C85B2AE6
SHA1:	C73EE4952113A5A4F957CB3E748B52EBC2E8689A
SHA-256:	A7B75F8A7782A7C69F155650C793341028DEA8BA1866F3EBCFA40423E9180342
SHA-512:	B70AF4B16C64B38401058136103BE36EEC08E57D4DD47D6CF921711A9744E05F78AD37625071CC283CD3714CE73421C391F293644147FED109EE397D932D527D
Malicious:	false
IE Cache URL:	http://https://linktr.ee/_next/static/chunks/commons.a2d313fdf1fe3659cd29.js
Preview:	(window.webpackJsonp=window.webpackJsonp||[]).push([[0],{"+6fG":function(e,t,r){"use strict";r("K1iI")(t,"__esModule",{value:!0}),t.default=void 0;var n={abstract:!1,acce ssibleNameRequired:!1,baseConcepts:[],childrenPresentational:!1,nameFrom:["author"],prohibitedProps:[],props:{"aria-posinset":null,"aria-setsize":null},relatedConcepts:[{ concept:{name:"article"},module:"HTML"}],requireContextRole:[],requiredContextRole:[],requiredOwnedElements:[],requiredProps:{},superClass:[["roletype","structu re","document"]]};t.default=n},"+8d6":function(e,t,r){e.exports=r("X+IB")},"+Pc/":function(e,t,r){r("91A9"),r("p++B");var n=r("j0PW");e.exports=n.Array.from},"+r8s":funct ion(e,t,r){r("tCEB")("patternMatch")},"/6So":function(e,t,r){var n=r("LTNl");e.exports=function(e,t,r,o){try{return o?t(n(r)[0],r[1]):t(r)}catch(a){var i=e.return;throw void 0!==i& &n(i.call(e)),a}}},"/HG3":function(e,t,r){r("iaIM");var n=r("j0PW");n.JSON||(n.JSON={stringify:JSON.stringify}),e.exports=function(e,t,r){return n.JSO

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\dnserror[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	2997
Entropy (8bit):	4.4885437940628465
Encrypted:	false
SSDEEP:	48:u7u5V4VyhhV2lFUW29vj0RkpNc7KpAP8Rra:vlIJ6G7Ao8Ra
MD5:	2DC61EB461DA1436F5D22BCE51425660
SHA1:	E1B79BCAB0F073868079D807FAEC669596DC46C1
SHA-256:	ACDEB4966289B6CE46ECC879531F85E9C6F94B718AAB521D38E2E00F7F7F7993
SHA-512:	A88BECB4FBDDC5AFC55E4DC0135AF714A3EEC4A63810AE5A989F2CECB824A686165D3CEDB8CBD8F35C7E5B9F4136C29DEA32736AABB451FE8088B978B493AC6D
Malicious:	false
IE Cache URL:	res://ieframe.dll/dnserror.htm?ErrorStatus=0x800C0005&DNSError=1460
Preview:	.<!DOCTYPE HTML>..<html>.. <head>.. <link rel="stylesheet" type="text/css" href="NewErrorPageTemplate.css" >.. <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.. <title>Can’t reach this page</title>.. <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="getInfo(); initMo reInfo('infoBlockID');">.. .. Can’t reach this page .. .. <ul id="cantDisplayTasks" class="tasks">.. <li id="task1-1">Make sure the web address is correct .. <li id="task1-2">Search for this site on Bing ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\framework.8293b41d86da2f0201a3[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):	140330
Entropy (8bit):	5.264341897147884
Encrypted:	false
SSDEEP:	1536:8u/vnhKNaf/xmH3Ny+lD0/WsWdDIkGCKRJMgaZ600+QUkc6:8QPhKNmfWIkUJti600+QUkc6
MD5:	B0A60D1A87C4C3F6089DE9984AC5B669
SHA1:	BD62DBBCE1B1B82500709E0C328014CC981F1E1B
SHA-256:	9FBAFE17CCF61EA39A66FFC6C9C4D1189B6BF3231DAFBDE36505105FBD38332F
SHA-512:	5E4CE1913035AD431E9D0DF3E755A18BCB53731688EEE1E54204CBA7E7F623DEA481C48FDB1F658D824D234169CD02C0B7A6F9643C26AE935368781B9396FBCB

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\framework.8293b41d86da2f0201a3[1].js	
Malicious:	false
IE Cache URL:	http://https://linktr.ee/_next/static/chunks/framework.8293b41d86da2f0201a3.js
Preview:	(window.webpackJsonp=window.webpackJsonp||[]).push([[2],{"7nmT":function(e,t,n){"use strict";!function e(){if("undefined"!==typeof __REACT_DEVTOOLS_GLOBAL_HOOK__&&"function"===typeof __REACT_DEVTOOLS_GLOBAL_HOOK__.checkDCE){0;try{__REACT_DEVTOOLS_GLOBAL_HOOK__.checkDCE(e)}catch(t){console.error(t)}}}(),e.exports=n("w/UT")},Dyo0:function(e,t,n){"use strict";e.exports=n("Sfmn")},ERkP:function(e,t,n){"use strict";e.exports=n("hLw4")},Sfmn:function(e,t,n){"use strict";(function(e){var t=n("Km8e"),r=n("ERkP"),l=n("7nmT"),i=n("jiMj");function o(e){for(var t="https://reactjs.org/docs/error-decoder.html?invariant="+e,n=1;n<arguments.length;n++)t+="&args[]="+encodeURIComponent(arguments[n]);return"Minified React error #"+e+"; visit "+t+" for the full message or use the non-minified dev environment for full errors and additional helpful warnings."}var a=r.__SECRET_INTERNALS_DO_NOT_USE_OR_YOU_WILL_BE_FIRED;function u(e){var t=e,n=e;if(e.alternate)for(;t.return;)t=t.return;else{e=t;do{0!==(1026&(t

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\free-fa-regular-400[1].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), Font Awesome 5 Free Regular family
Category:	downloaded
Size (bytes):	34350
Entropy (8bit):	6.320570887190345
Encrypted:	false
SSDEEP:	384:HbFILSQt3owpXUazLuDULbNVTH/oOkKQB3I+89AyI6WcRwkRcQUta:HbeLSe3yy6DOP/oDB29uc5RcQUA
MD5:	991B587DBEE2E132C9542FB1280F1372
SHA1:	660DA8C03735C9DFFB26205AAD19EA6B1916268A
SHA-256:	44F6500D0D5D7F3F8422B9790EAA47DF4E1D812C90239602E53429376B96D1DF
SHA-512:	A9AF4B58640B47D1EF7B6E2126BA6908AF9A4027D3961E3889732E433B9CED8E49F0BB17E54FEA602FFC46E93206DBA088EFC9CC41940477C3DCC3687D0C9B(D
Malicious:	false
IE Cache URL:	http://https://ka-f.fontawesome.com/releases/v5.15.1/webfonts/free-fa-regular-400.eot?
Preview:	.....LP.....6.F.o.n.t. .A.w.e.s.o.m.e. .5. .F.r.e.e. .R.e.g.u.l.a.r.....R.e.g.u.l.a.r...L.3.3.1...5.2.1. .(.F.o.n.t. .A.w.e.s.o.m.e. .v.e.r.s .i.o.n.:. .5...1.5...1.)...6.F.o.n.t. .A.w.e.s.o.m.e. .5. .F.r.e.e. .R.e.g.u.l.a.r.....PFFTM.,.....GDEF.*.....OS/2A.S....X...`cmap.....gasp.....glyf|.7.... ..n.head.. .....6hhea.5.....$hmtx...t.....Tloca.e.....6maxp.....8... name8.8"..w....[post.iA...}.....K.`._.<.....w.....z.....@. .....L.f...G.L.f.....PfEd.....T.....:..... .....@.....@.....@.....@.....@...@.....@...@..... ..`.....@.....@.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\free-fa-solid-900[1].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), Font Awesome 5 Free Solid family
Category:	downloaded
Size (bytes):	204814
Entropy (8bit):	6.34341654497633
Encrypted:	false
SSDEEP:	6144:5t+zd6McnODzpN2BDXTIRSwRKSK3NC5xMG:GELnODze58Rjg+55
MD5:	D3B45D588F61AB38CB31CBA544B4373C
SHA1:	627D2C71A5FFC7E5F17DA0897EE1B73CD30D255F
SHA-256:	366C63E48A15576AA55ED76DB0EBCCA8BCE15F6EFC881BD0AC75982FF1233699
SHA-512:	6D178A6671E6C1E4148770A4FD6351FD237628A48748047006B350E3FBD2BDFD0257BD908BAA26606D3326FE2F7D1E80B505E533716D9EFE8490A6EEC99D83BC
Malicious:	false
IE Cache URL:	http://https://ka-f.fontawesome.com/releases/v5.15.1/webfonts/free-fa-solid-900.eot?
Preview:	. .....LP.....O..O.....2.F.o.n.t. .A.w.e.s.o.m.e. .5. .F.r.e.e. .S.o.l.i.d.....S.o.l.i.d...L.3.3.1...5.2.1. .(.F.o.n.t. .A.w.e.s.o.m.e. .v.e.r.s.i.o.n.:. .5...1.5...1.)...2.F.o.n.t. .A.w.e.s.o.m.e. .5. .F.r.e.e. .S.o.l.i.d.....PFFTM.,.....GDEF.*.....OS/23.V`...X...`cmap.j.4...h....gasp.....glyfh.....-....dhead.,.....6 hhea.C.-.....$hmtx.Q.....loca.....8....maxp.N.`...8... name!.-....P...+post..Fa...|..1.....K.`O..O_.<.....x.....z.....]. .....@..... .....L.f...G.L.f.....PfEd.....T.....:..... .....@.....@. .....@.....@..... .....@.....`.....@.....@.....@.....@....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\free.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	60351
Entropy (8bit):	4.728636008010348
Encrypted:	false
SSDEEP:	768:OUh31IPiyXNq4YxBowbgJlkwF//zMQyYJYX9Bft6VSz8:OU0PxXE4YXJgndFTfy9lt5Q
MD5:	319D424BA89A84BBD230A3B5F7024193
SHA1:	1AE1807CDED8F2E41D2541BCCA8E0D7077FBA6F4
SHA-256:	4F02BD6F018D6F08C37C39F2D114101BEAC342C2C065046635E5ED0C42853590
SHA-512:	A68CAB17CCD1C4DDEAD9124B75CF0CF0C12C4E914902AECE79DCC4C42167B58B565467F20F72C48DFA85490F1895F89F074C85E825D548AD12410741A3302E
Malicious:	false
IE Cache URL:	http://https://ka-f.fontawesome.com/releases/v5.15.1/css/free.min.css

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\free.min[1].css	
Preview:	/*!. * Font Awesome Free 5.15.1 by @fontawesome - https://fontawesome.com. * License - https://fontawesome.com/license/free (Icons: CC BY 4.0, Fonts: SIL OFL 1.1, Code: MIT License). */.fa,.fab,.fad,.fal,.far,.fas{-moz-osx-font-smoothing:grayscale;-webkit-font-smoothing:antialiased;display:inline-block;font-style:normal;font-variant:normal;text-rendering:auto;line-height:1}.fa-lg{font-size:1.33333em;line-height:.75em;vertical-align:-.0667em}.fa-xs{font-size:.75em}.fa-sm{font-size:.875em}.fa-1x{font-size:1em}.fa-2x{font-size:2em}.fa-3x{font-size:3em}.fa-4x{font-size:4em}.fa-5x{font-size:5em}.fa-6x{font-size:6em}.fa-7x{font-size:7em}.fa-8x{font-size:8em}.fa-9x{font-size:9em}.fa-10x{font-size:10em}.fa-fw{text-align:center;width:1.25em}.fa-ul{list-style-type:none;margin-left:2.5em;padding-left:0}.fa-ul>li{position:relative}.fa-li{left:-2em;position:absolute;text-align:center;width:2em;line-height:inherit}.fa-border{border:.08em solid #eee;border-radius:.1em;padding:.2em .25em .15em}.fa-pul

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\styles[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	83656
Entropy (8bit):	3.775380377875336
Encrypted:	false
SSDEEP:	384:3c4tBf6Q9C2OC9F1ZHr+xoFznknxDt1H34TF8BdHsT:M4td6Q9P76CMxDtN4TF8BdHsT
MD5:	C050E5B0035E3A95D55EB078536DF6B7
SHA1:	25A10BE0A42C8C1B5E4C0A5724A1277A3F7C7EF7
SHA-256:	FDDC8007E5B4300217CA36667B4C865FC0EBDD58E5BEF8B9A7DEE1AFED6E1960
SHA-512:	B315F5DDA7E96C412B5889AF3F1766DBCB560EBE5EF38105FD174767AC9BEE504C56C753D0B4816E66AE0E01F41EE801B9C75BFAC17C4B0DE6F482AE4A1C2C54
Malicious:	false
Preview:	<style type="text/css"> html {. font-family: sans-serif;. -ms-text-size-adjust: 100%;. -webkit-text-size-adjust: 100%. }. . body {. margin: 0. }. . article,. aside,. details,. figcaption,. figure,. footer,. header,. hgroup,. main,. menu,. nav,. section,. summary {. display: block. }. . audio,. canvas,. progress,. video {. display: inline-block;. vertical-align: baseline. }. . audio:not([controls]) {. display: none;. height: 0. }. . [hidden],. template {. display: none. }. . a {. background-color: transparent. }. . a:active,. a:hover {. outline: 0. }. . abbr[title] {.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\wXKoE3YSppcvo1PDln__[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 44016, version 1.1
Category:	downloaded
Size (bytes):	44016
Entropy (8bit):	7.9887700485141915
Encrypted:	false
SSDEEP:	768:JSLL4oYuB0dVg7RilXSORmHosE1urdKCLviiqv/8uH0+IBim6L60nTwTWiTdVHv:HoYuWXgVi35mdKmibSf6LpTwqiRVP
MD5:	426EF8802433882B5234D3422EF1E15C
SHA1:	BA726D7223C9C11F4DBAA63FF0A6AF94220A384A
SHA-256:	A01454F736CCF522E0776E0BAD6E95BA7EAFC4DE37AF25C4FDAE44DF26292552
SHA-512:	B764D205C6813F84B795D6B70F0FD380F9BF3BEF459B69ECEACE477D4E1C50147B2631F7C81367FFAB8A042D0E5F8324334610494EFBB419F2EE7F75BFF5C2D
Malicious:	false
IE Cache URL:	http://https://fonts.gstatic.com/s/capriola/v8/wXKoE3YSppcvo1PDln__.woff
Preview:	wOFF.....h.....GDEF...X.....OS/2...p...Y...`...*cmap.....8.qcvt .....%...0....fpgm.....IAy..gasp.....glyf.....g...0<head.....6...6!..2hhea..... ...$.=. hmtx.....p.E..loca.....:N..Smaxp..... ... ....name...<.....TIvpost...@...P.....prep.....`...`.Ex+.....x.-....A.....<.2.....,#....k..]WfP:.O.....tV.W.Ha.2.....9.7.%..<..r.....&.<.....x.\..L.Q...{o.]..k..l{6.....lf...4+.....w.....&.H...T.....$.....O.i?.....mvi..F`.....=0.....A.....K:?]...3...s.....p.|.F.....w.9.)*.{a-.B!|0w!l..!0...t(.F.A.C'tGoD..` 8..Z....%.?.....__.<...F>..F.Z..B4g.Z3Vo.Q.MiV..F.N)U...,.B.[.)i\...../..~....}..g.....Nc...ai..x.c@.....1.....[.K../.O..oY.@l.;!.I...x.T.z.F..S.\.....n...).s.nHn....5O3Hy.<Z.....?..N.....K..}|..bCA..{i..$.....$....I..C....d.....D ...<...c..,KAy.kh. ...g..I.8byIR.....m.;.N.!.n.]Y...PV.6.k*..\6.gb.Ou.V..<.;.mM..S:.|[..O.7#....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\webpack-6ef28db84b4c42ad34e9[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):	1531
Entropy (8bit):	5.147145845956062
Encrypted:	false
SSDEEP:	24:ExffRGjwLhrYRc7zsHkwBmaclBmGL0BTMWwMWIeazflvJks8if:EBRIoYO7fwFgfKTMWLdYks8G
MD5:	40B4095B5B68A142C856F388CCB756F2
SHA1:	31905340609587E1A7C5D4A92D08A2FA3B404DB1
SHA-256:	E2FBB88B4D15A9F7702CA58EBBE8D1D927FFD2667E585E70A5F3D51ACB1A37D2
SHA-512:	3FAB812739B50D25209FE4EC6A72D2441ECE9D4A9347DFD0A47CEC27CCB07676ED8B9958E4985831A896166492DB33D9D88951C88F1FD0BB185890820905825
Malicious:	false
IE Cache URL:	http://https://linktr.ee/_next/static/runtime/webpack-6ef28db84b4c42ad34e9.js
Preview:	!function(e){function r(r){for(var n,l,f=r[0],i=r[1],a=r[2],c=0,s=[];c<f.length;c++)l=f[c],Object.prototype.hasOwnProperty.call(o,l)&&o[l]&&s.push(o[l][0]),o[l]=0;for(n in i)Object.prototype.hasOwnProperty.call(i,n)&&(e[n]=i[n]);for(p&&p(r);s.length;)s.shift()();return u.push.apply(u,a||[]),t()}function t(){for(var e,r=0;r<u.length;r++){for(var t=u[r],n=!0,f=1;f<t.length;f++){var i=t[f];0!==o[i]&&(n=!1)}n&&(u.splice(r--,1),e=l(l.s=t[0]))}return e}var n={},o={1:0},u=[];function l(r){if(n[r])return n[r].exports;var t=n[r]={i:r,l:!1,exports:{}};o[r].call(t.exports,t,t.exports,l),t.l=!0,t.exports}l.m=e,l.c=n,l.d=function(e,r,t){l.o(e,r)||Object.defineProperty(e,r,{enumerable:!0,get:t})},l.r=function(e){"undefined"!==typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(e,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(e,"__esModule",{value:!0})},l.t=function(e,r){if(1&r&&(e=l(e)),8&r)return e;if(4&r&&"object"===typeof e&&e&&e.__esMo

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\37aee9ee.023bc762744cd0548817[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):	244165
Entropy (8bit):	4.68737820103819
Encrypted:	false
SSDEEP:	3072:c8Er84Awjj03k4PV03C4PcpiXoLyEZn+3+6DvzZtpSBm6sRTbgQLcn4CQrixrbMp:c8NZgWPZn+3+6D9+s
MD5:	240379080B94CB962C365F3634D48E4E
SHA1:	887A81FE5C5AED45B9B849AD1E414AB6C5CD9F4F
SHA-256:	18C0E02037833073A6C1312310F391C55A47DD81974B36B99406D24555B982CD
SHA-512:	F00EB0D140EF538BCF896C248C59B2F13AF035E2D24A9257C9D3B4F52CDB48678C2F20B5946E31FDA39F7FE246D0F1D46B656EFAAA9576BD0D29DE7896847DA
Malicious:	false
IE Cache URL:	http://https://linktr.ee/_next/static/chunks/37aee9ee.023bc762744cd0548817.js
Preview:	(window.webpackJsonp=window.webpackJsonp||[]).push([[3],{lanT:function(d,$){!function(){var d=this||self;function $($,e){$=$.split(".");var n,t=d;$[0]in t||"undefined"==typeof t.execScript||t.execScript("var "+$[0]);for(;$.length&&(n=$.shift());)$.length||void 0===e?t=t[n]&&t[n]!==Object.prototype[n]?t[n]:t[n]={}:t[n]=e}function e(d,$){function e(){}e.prototype=$.prototype,d.o=$.prototype,d.prototype=new e,d.prototype.constructor=d}var n=Array.prototype.indexOf?function(d,$,e){return Array.prototype.indexOf.call(d,$,e)}:function(d,$,e){if(e=null==e?0:0>e?Math.max(0,d.length+e):e,"string"===typeof d)return"string"!==typeof $||1!=$.length?-1:d.indexOf($,e);for(;e<d.length;e++)if(e in d&&d[e]===$)return e;return-1};function t(d,$){d.sort($||r)}function r(d,$){return d>$?1:d<$?-1:0}function u(d,$){switch(this.a=d,this.h=!!$.i,this.c=$.b,this.m=$.type,this.l=!1,this.c){case a:case o:case l:case c:case s:case f:case i:this.l=!0}this.g=$.defaultValue}var i=1,f=2,a=3,o=4,l=6,c=16,s=18;function

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\4674618e.7a549f670d4ea1a99faf[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):	77857
Entropy (8bit):	5.399465664008807
Encrypted:	false
SSDEEP:	1536:VkZvrhmBnYKpKllf91gE0Mwr+LvVzVg592FXq7:fBnA1gQwrD32Fl
MD5:	2099A0B679B578D738056778DA5C2EA8
SHA1:	8AE37F705D9D752CEB47339AA10ABDAE84D18098
SHA-256:	7E7F002B8581918FFDEA2637DE6C963C9B7B0DDB0ACAD2816ACBFE073E798658
SHA-512:	402535AAE6237542F2605FA4D9751F642D4C21CAFD04AC6742B2D854E571B153F1397D4DC258D7D5A584D07024FFCD336EB7D35780CD457459C844D3DA36BAC
Malicious:	false
IE Cache URL:	http://https://linktr.ee/_next/static/chunks/4674618e.7a549f670d4ea1a99faf.js
Preview:	(window.webpackJsonp=window.webpackJsonp||[]).push([[4],{L5US:function(t,e,n){window.eve=n("m+n/");var r=function(t){var e,n={},r=window.requestAnimationFrame||window.webkitRequestAnimationFrame||window.mozRequestAnimationFrame||window.oRequestAnimationFrame||window.msRequestAnimationFrame||function(t){return setTimeout(t,16,(new Date).getTime()),!0},i=Array.isArray||function(t){return t instanceof Array||"[object Array]"==Object.prototype.toString.call(t)},a=0,o="M"+(+new Date).toString(36),s=Date.now||function(){return+new Date},u=function(t){var e=this;if(null==t)return e.s;var n=e.s-t;e.b+=e.dur*n,e.B+=e.dur*n,e.s=t},l=function(t){if(null==t)return this.spd;this.spd=t},c=function(t){var e=this;if(null==t)return e.dur;e.s=e.s*t/e.dur,e.dur=t},h=function(){var e=this;delete n[e.id],e.update(),t("mina.stop."+e.id,e)},f=function(){var t=this;t.pdif||(delete n[t.id],t.update(),t.pdif=t.get()-t.b)},d=function(){var t=this;t.pdif&&(t.b=t.get()-t.pdif,delete t.pdif,n[t.id]=t,g())},p=functi

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\71eea0b16954fa49b00816d2602a02cddd90f3fe.95252ede6ddf438ef692[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):	17647
Entropy (8bit):	5.24185037672425
Encrypted:	false
SSDEEP:	384:/a7lC/PJRaczQA5tMCsbgMlVLA/Hhk3YCEymUCFL12NJGZTR:wlC/PJcA5hssMwCEymUCFmGZTR
MD5:	97E177EB14CAA6814B4BFCB67809C895
SHA1:	7A544BCB395A81D1DD6B0388A1809DA0BD33FCA9
SHA-256:	74D37117F86D8C26DF232B8EAB5B0C4B9EF16E4CB7A7B9910AF9FE17B12A17E5
SHA-512:	C29B458C07F2FD2D79C18EDB3D37A26861F87BEDE9945A2B7751A8CE2082B2EC3A7CF236B2FCFF6E8BCBDCB472E70CF821A136007E593FAC492F17421DC0E3C
Malicious:	false
IE Cache URL:	http://https://linktr.ee/_next/static/chunks/71eea0b16954fa49b00816d2602a02cddd90f3fe.95252ede6ddf438ef692.js
Preview:	(window.webpackJsonp=window.webpackJsonp||[]).push([[5],{"2MIm":function(t,e,n){"use strict";var r=n("Y3ZS");e.__esModule=!0,e.default=function(t){function e(e){return o.default.createElement(t,Object.assign({router:(0,a.useRouter)()},e))}e.getInitialProps=t.getInitialProps,e.origGetInitialProps=t.origGetInitialProps,!1;return e};var o=r(n("ERkP")),a=n("7xIC")},"4mCN":function(t,e){function n(t,e,n,r,o,a,i){try{var u=t[a](i),c=u.value}catch(s){return void n(s)}u.done?e(c):Promise.resolve(c).then(r,o)}t.exports=function(t){return function(){var e=this,r=arguments;return new Promise((function(o,a){var i=t.apply(e,r);function u(t){n(i,o,a,u,c,"next",t)}function c(t){n(i,o,a,u,c,"throw",t)}u(void 0)}))}}},"5t7+":function(t,e){t.exports=function(t){if(Array.isArray(t))return t}},"7xIC":function(t,e,n){"use strict";var r=n("JiiP");function o(t,e){var n;if("undefined"===typeof Symbol||null==t[Symbol.iterator]){if(Array.isArray(t)||(n=function(t,e){if(!t)return;if("string"===typeof t)return a(

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\75e92289.e259db20f580424981e7[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\75e92289.e259db20f580424981e7[1].js	
Category:	downloaded
Size (bytes):	316787
Entropy (8bit):	4.666205524171314
Encrypted:	false
SSDEEP:	1536:ud88peKF7AhqIMq8EWRtIjuqWCsDY4cH3qEjLI8iLPiBCD3X8jUnw:6kwPIjuLCSYBLi0CDcb
MD5:	C5A27CC16F8AC36E78926FF633DB9E22
SHA1:	E52A5D8A3ABFEE447CB04D8625F8D0A51A6DFFFA
SHA-256:	CFB058EDF8CC6FEDC301AEB3D78B1562B82E48F93CFB734999173C4E5AB7D092
SHA-512:	1B4DA11C1FBB88A0871C9A15AAF789A9100BE22626B9B5863BE13C61A1B5EB228340AAAF22208D70F1FCEF417A9D204E9209FBAE0BDB9AF160E078AF557EBF86
Malicious:	false
IE Cache URL:	http://https://linktr.ee/_next/static/chunks/75e92289.e259db20f580424981e7.js
Preview:	(window.webpackJsonp=window.webpackJsonp||[]).push([[6],{fPAk:function(e){e.exports=JSON.parse('{"version":"2.0","metadata":{"apiVersion":"2016-11-15","endpointPrefix":"ec2","protocol":"ec2","serviceAbbreviation":"Amazon EC2","serviceFullName":"Amazon Elastic Compute Cloud","serviceId":"EC2","signatureVersion":"v4","uid":"ec2-2016-11-15","xmlNamespace":"http://ec2.amazonaws.com/doc/2016-11-15"},"operations":{"AcceptReservedInstancesExchangeQuote":{"input":{"type":"structure","required":["ReservedInstanceIds"],"members":{"DryRun":{"type":"boolean"},"ReservedInstanceIds":{"shape":"S3","locationName":"ReservedInstanceId"},"TargetConfigurations":{"shape":"S5","locationName":"TargetConfiguration"}}},"output":{"type":"structure","members":{"ExchangeId":{"locationName":"exchangeId"}}}},"AcceptTransitGatewayPeeringAttachment":{"input":{"type":"structure","required":["TransitGatewayAttachmentId"],"members":{"TransitGatewayAttachmentId":{},"DryRun":{"type":"boolean"}}},"output":{"type":"structur

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\89963fc67fc7243243e5d1e66f0a4763d3fc8a2b.db7b909395c9b5951944[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):	3440614
Entropy (8bit):	5.340565879453573
Encrypted:	false
SSDEEP:	12288:2W9+wyT7amscqC49UHpzgKOQLu4FdUCMYrN+FXZbvbrOx6byeVzyXlQnAO4RXA5X:SZXI9SpzgUuIdUYMbvbrOx6byelyXw+8
MD5:	5A648B52451DAE83212DD49C5F61E717
SHA1:	83F46576F25BDA0FF2A0CD656ABF403BA2AB200A
SHA-256:	92B8367793DCF89E95E5AD6B1A9C6CA02D18772966D39C90BA5BF4D7278661D3
SHA-512:	5BCC39351E69E0D996A1442213E13AC626723F4E60D12023B79C4050F9AB7BA14EB0A1606B4FD8C32530D9159B859F4C5914C38E5E63D0D8A0A3FD6884DF0081
Malicious:	false
IE Cache URL:	http://https://linktr.ee/_next/static/chunks/89963fc67fc7243243e5d1e66f0a4763d3fc8a2b.db7b909395c9b5951944.js
Preview:	(window.webpackJsonp=window.webpackJsonp||[]).push([[7],{"+1bT":function(e){e.exports=JSON.parse('{"pagination":{"DescribeDocumentVersions":{"input_token":"Marker","limit_key":"Limit","output_token":"Marker","result_key":"DocumentVersions"},"DescribeFolderContents":{"input_token":"Marker","limit_key":"Limit","output_token":"Marker","result_key":["Folders","Documents"]},"DescribeUsers":{"input_token":"Marker","limit_key":"Limit","output_token":"Marker","result_key":"Users"}}}')},"+26Y":function(e){e.exports=JSON.parse('{"version":"2.0","metadata":{"apiVersion":"2013-09-09","endpointPrefix":"rds","protocol":"query","serviceAbbreviation":"Amazon RDS","serviceFullName":"Amazon Relational Database Service","serviceId":"RDS","signatureVersion":"v4","uid":"rds-2013-09-09","xmlNamespace":"http://rds.amazonaws.com/doc/2013-09-09/"},"operations":{"AddSourceIdentifierToSubscription":{"input":{"type":"structure","required":["SubscriptionName","SourceIdentifier"],"members":{"SubscriptionName":{},"S

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\89963fc67fc7243243e5d1e66f0a4763d3fc8a2b_CSS.244c3afbbfc751a1196f[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	61
Entropy (8bit):	4.445012903413859
Encrypted:	false
SSDEEP:	3:lD3ORZy/LBdORZzZqVRNrE+4Be:lD3r1daZurl
MD5:	8D9097E43D3FDAF69A58B2D76CFC0C2D
SHA1:	5E7B1737270738819AC2BD6DE475BB399D3BD5AB
SHA-256:	846BD2506FF67E6FB04C1B886FA912D325ECC49F6A5045E71E2BEC59BC843341
SHA-512:	18D677E56CE18014B82ABAE9C4B34A3B53832556D28249E440103096458971A193170C4459CAEB1B37632E36FACB01F8E388E58DD8B010E935BCB57EC7C89908
Malicious:	false
IE Cache URL:	http://https://linktr.ee/_next/static/chunks/89963fc67fc7243243e5d1e66f0a4763d3fc8a2b_CSS.244c3afbbfc751a1196f.js
Preview:	(window.webpackJsonp=window.webpackJsonp||[]).push([[8],[]]);

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4_buildManifest[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):	752
Entropy (8bit):	5.323445431451699
Encrypted:	false
SSDEEP:	12:Z3xfwS/4EUAVkpk3FI5XylfmQtJExw9aR3pJxw9aRP+2Exw9aRNXztDfza:ZBYXAVik1jPtD9gG9gmS9gNDt3a

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4_buildManifest[1].js	
MD5:	CD7B46D9C70D36D2ADAC1B587CF6FDBC
SHA1:	995D16AAB76D598122D05F5FD6BB983B817ED429
SHA-256:	FD8DA1ED843C0F0D3DDC47749FBE252386F8FD307D08A4136066627E51477068
SHA-512:	D9A68E8F5E34DCEEAB62F287B388745446818E8858948FA4C4C576645658458BF0CB5B6BAF3A8B32B5AE951651ED79806BD2933DD7108AA99EE4E35E52ABB3AE
Malicious:	false
IE Cache URL:	http://https://linktr.ee/_next/static/cgNRtwTLQ-H-pzscYPh23/_buildManifest.js
Preview:	self.__BUILD_MANIFEST = (function(a,b,c,d,e,f,g,h){return {"/[profile]":[a,b,c,d,e,f,g,h],"/status/blocked":[a,b,c,d,e,f,g,h]}}("static\u002Fchunks\u002F75e92289.e259db20f580424981e7.js","static\u002Fchunks\u002F4674618e.7a549f670d4ea1a99faf.js","static\u002Fchunks\u002F37aee9ee.023bc762744cd0548817.js","static\u002Fchunks\u002Fddbbc6a8.91a110ad55746e11f584.js","static\u002Fchunks\u002Ff5f15f9f.38f5b5554764d92b9414.js","static\u002Fchunks\u002F89963fc67fc7243243e5d1e66f0a4763d3fc8a2b.db7b909395c9b5951944.js","static\u002Fcss\u002F89963fc67fc7243243e5d1e66f0a4763d3fc8a2b_CSS.af1f508a.chunk.css","static\u002Fchunks\u002F89963fc67fc7243243e5d1e66f0a4763d3fc8a2b_CSS.244c3afbbfc751a1196f.js"));self.__BUILD_MANIFEST_CB && self.__BUILD_MANIFEST_CB()

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4_ssgManifest[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	76
Entropy (8bit):	4.327646996939871
Encrypted:	false
SSDEEP:	3:k0WYL12AkZ/W6QfpX/W6Qen:UYR2Ak06EpXO6h
MD5:	ABEE47769BF307639ACE4945F9CFD4FF
SHA1:	C0A0DC51EE8A2852BAF5FF30C33B1478FF302585
SHA-256:	653F3E53E89B4F8548FF86C19E92BB3C6B84B6BE7485A320B1E00893ED877479
SHA-512:	2B074799106698DF69A28FCD8255C3CFD1CCF40FD4C1BF5D463C42E63B32856F801E066706FBD960A0DA4EBE645C070C398DCF01BD722DC4FA592266361AE8
Malicious:	false
IE Cache URL:	http://https://linktr.ee/_next/static/cgNRtwTLQ-H-pzscYPh23/_ssgManifest.js
Preview:	self.__SSG_MANIFEST=new Set;self.__SSG_MANIFEST_CB&&self.__SSG_MANIFEST_CB()

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\bfcd7a435e3e3c741a3c8cae70d839f00beee574.f1828304484b272de08a[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):	31189
Entropy (8bit):	5.34374163979729
Encrypted:	false
SSDEEP:	384:bjfDHieCzprWQjwq1FGF1zjvRDSSme7StIIDDvR3bkjOngzTPli:LHlQjwGFGF1/Vz+tleFLkjdPg
MD5:	70FBD1C2089AC29D84CC191A0FE5C2BD
SHA1:	7ED9D06230EF7CD09024DBD0C304EFF4A5578E39
SHA-256:	4EDCF81B31C22CB65332D92AEB21B6664BB5FA827A8BF3D5CF80090508F75AA3
SHA-512:	83A6D249D65F3A2DCBA918F3AE6D62E4C76365E788A789D7F8016BA81D03A0D767204EAAF8C50D76746B32AD6552F2FC294F1952E98AD836729F62C88AF3FCC
Malicious:	false
IE Cache URL:	http://https://linktr.ee/_next/static/chunks/bfcd7a435e3e3c741a3c8cae70d839f00beee574.f1828304484b272de08a.js
Preview:	(window.webpackJsonp=window.webpackJsonp||[]).push([[9],{LixI:function(e,t,n){"use strict";n.r(t),n.d(t,"default",(function(){return s}));var r=n("ERkP"),i=n.n(r),o=n("ABxZ"),a=(n("gz9i"),i.a.createElement);function s(e){switch(e.statusCode){case 404:return a(o.a,{pageTitle:"Linktree | Page Not Found",message:"The page you\u2019re looking for doesn\u2019t exist."});default:return a(o.a,{pageTitle:"Linktree",message:"Linktree is currently undergoing maintenance. Back soon!",cta:{title:"Get updates",url:"https://systems.linktr.ee/"}})}}s.getInitialProps=function(e){var t=e.res,n=e.err;return{statusCode:t?t.statusCode:n?n.statusCode:404}}},gz9i:function(e,t,n){"use strict";n.d(t,"a",(function(){return ye})),n.d(t,"b",(function(){return at}));var r=function(){return(r=Object.assign||function(e){for(var t,n=1,r=arguments.length;n<r;n++)for(var i in t=arguments[n])Object.prototype.hasOwnProperty.call(t,i)&&(e[i]=t[i]);return e}).apply(this,arguments)};function i(e,t,n,r){return new(n||(n=Pro

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\ddbbc6a8.91a110ad55746e11f584[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):	105978
Entropy (8bit):	4.642262654405873
Encrypted:	false
SSDEEP:	768:4GLCvB726ZanS1Op2vIEgFSoBBY8Y3rS88h87PuIC+hbFyDk1H3eZ5QV/ppWB/qk:UCX+ITK3r32+LXNppGgOiMCr0+sYg/b
MD5:	0734B12C251D97FC899A1B266CA67248
SHA1:	1C2D29E99B6F92491FD84D3DAA7D27C945C0EB40
SHA-256:	83A45B2B7BA76F57197BCE735D7ADFC9401F4ECED2ED09A52B029FC8BD3B1492
SHA-512:	40829385A7CBED6EE8863779377E10531C03E016DF116BF8BDB52B3CE750BAFB40B75219197EDF2C027FFE7A13B3FBBCC9AC533C5122C6FFAB531159A00770D6
Malicious:	false
IE Cache URL:	http://https://linktr.ee/_next/static/chunks/ddbbc6a8.91a110ad55746e11f584.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\ddbbc6a8.91a110ad55746e11f584[1].js	
Preview:	(window.webpackJsonp=window.webpackJsonp||[]).push([[10],{xPPc:function(e){e.exports=JSON.parse('{"version":"2.0","metadata":{"apiVersion":"2015-05-28","endpointPrefix":"iot","protocol":"rest-json","serviceFullName":"AWS IoT","serviceId":"IoT","signatureVersion":"v4","signingName":"execute-api","uid":"iot-2015-05-28"},"operations":{"AcceptCertificateTransfer":{"http":{"method":"PATCH","requestUri":"/accept-certificate-transfer/{certificateId}"},"input":{"type":"structure","required":["certificateId"],"members":{"certificateId":{"location":"uri","locationName":"certificateId"},"setAsActive":{"location":"querystring","locationName":"setAsActive","type":"boolean"}}}},"AddThingToBillingGroup":{"http":{"method":"PUT","requestUri":"/billing-groups/addThingToBillingGroup"},"input":{"type":"structure","members":{"billingGroupName":{},"billingGroupArn":{},"thingName":{},"thingArn":{}}},"output":{"type":"structure","members":{}}},"AddThingToThingGroup":{"http":{"method":"PUT","requestUri":"/thin

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\excel.O365[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	20316
Entropy (8bit):	5.50049230922666
Encrypted:	false
SSDEEP:	384:WtoJ9uAGuSRk41z/p0yGO3UPVFsFSCWQodH5uESu1utQIrAQ5DRPBevc:WtoJ9u5uSRk4N/p0yGO3UPVFsFS7QSH4
MD5:	124C7BDFAAA72AE6E2FFFB3FC1DAD252
SHA1:	BA4817FC0E116EFE04DE2C4ABE02C18BF84EE612
SHA-256:	08A74FB872037B7A628C95BD834E4A94AF0DD55293D48A2E7234F6A1E1F6B288
SHA-512:	A8EAC1DD93196C2A6E13D6BD649E7CE30CDC173F9772321B2876188E6DB1D70559314DD501512DD6CA95E663069E08984868E0C911669701347B5BA1990970D
Malicious:	false
IE Cache URL:	http://https://linktr.ee/excel.O365.securefile
Preview:	<!DOCTYPE html><html><head><meta name="viewport" content="width=device-width"/><meta charSet="utf-8"/><meta name="description" content="Linktree. Make your link do more."/><meta property="og:title" content="Excel Protection"/><meta property="og:description" content="Linktree. Make your link do more."/><meta property="og:url" content="https://linktr.ee/excel.O365.securefile"/><meta property="og:image" content="https://d1fdloi71mui9q.cloudfront.net/0xdj2JeSLyVbtWi1vLfM_v5dUoYjUI35n9j8l"/><meta property="og:image:secure_url" content="https://d1fdloi71mui9q.cloudfront.net/0xdj2JeSLyVbtWi1vLfM_v5dUoYjUI35n9j8l"/><meta property="profile:username" content="excel.O365.securefile"/><meta name="twitter:title" content="Excel Protection"/><meta name="twitter:description" content="Linktree. Make your link do more."/><meta name="twitter:image" content="https://d1fdloi71mui9q.cloudfront.net/0xdj2JeSLyVbtWi1vLfM_v5dUoYjUI35n9j8l"/><link rel="canonical" href="https://linktr.ee/excel.O365.securefile"/><

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\f5f15f9f.38f5b5554764d92b9414[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):	92194
Entropy (8bit):	4.81682935302897
Encrypted:	false
SSDEEP:	768:ZmC/fjPbyxjkjOLUxugFGlctRe1V/oENIT1CYf2yrXUp:Zm6v1rXUp
MD5:	901082983D13EDEA43F11265B9E7894C
SHA1:	43FCEE18646A717458647C81A80E44134420CC2A
SHA-256:	FD2C873DE0A6D49B7A5C665E010BCEBE8EB1522F93261ABCCEAD9D0A8C2B9C55
SHA-512:	D1FF1AF8464C30C641CD42CE6AC99AF05375CD9ABB5BCF18EB09DA29416FFCB239BAF15B1C537452FDEFE113CD344CCBC9D6AD7E78438B89FCE7D5986D46E0E
Malicious:	false
IE Cache URL:	http://https://linktr.ee/_next/static/chunks/f5f15f9f.38f5b5554764d92b9414.js
Preview:	(window.webpackJsonp=window.webpackJsonp||[]).push([[11],{n4Dh:function(e){e.exports=JSON.parse('{"version":"2.0","metadata":{"apiVersion":"2006-03-01","checksumFormat":"md5","endpointPrefix":"s3","globalEndpoint":"s3.amazonaws.com","protocol":"rest-xml","serviceAbbreviation":"Amazon S3","serviceFullName":"Amazon Simple Storage Service","serviceId":"S3","signatureVersion":"s3","uid":"s3-2006-03-01"},"operations":{"AbortMultipartUpload":{"http":{"method":"DELETE","requestUri":"/{Bucket}/{Key+}","responseCode":204},"input":{"type":"structure","required":["Bucket","Key","UploadId"],"members":{"Bucket":{"location":"uri","locationName":"Bucket"},"Key":{"location":"uri","locationName":"Key"},"UploadId":{"location":"querystring","locationName":"uploadId"},"RequestPayer":{"location":"header","locationName":"x-amz-request-payer"},"ExpectedBucketOwner":{"location":"header","locationName":"x-amz-expected-bucket-owner"}}},"output":{"type":"structure","members":{"RequestCharged":{"location":"header

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\main-593fd4ec7c5bf6bc85e3[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):	17397
Entropy (8bit):	5.254667326583684
Encrypted:	false
SSDEEP:	384:5IvZO8waylIr5IN7JdKcCoGb/KI2QPk3A7Ym:PTl4i7JdG+INkfm
MD5:	E1A119C1D0B2C1C52A051D1D9B9538AA
SHA1:	C604E4E9BEFABD63673A4E0FA107625FF2F510A5
SHA-256:	59961D1F7A55335F90A444C2352B1420B79B174E378731EDE62106ADB4F95278
SHA-512:	B63D53773B3F738E9259726CA718F9C608C5984672CBF0E146DA5C534B4C23480D49249783BE9AD63A7AFFA9FBB79E32F635BF2B929823DEFE1A7F55B354484D
Malicious:	false
IE Cache URL:	http://https://linktr.ee/_next/static/runtime/main-593fd4ec7c5bf6bc85e3.js

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\main-593fd4ec7c5bf6bc85e3[1].js</th></tr>
<tr><td>Preview:</td><td>(window.webpackJsonp=window.webpackJsonp||[]).push([[16],{"7t6h":function(e,t,n){"use strict";n.r(t),n.d(t,"getCLS",(function(){return m})),n.d(t,"getFCP",(function(){return v})),n.d(t,"getFID",(function(){return g})),n.d(t,"getLCP",(function(){return w})),n.d(t,"getTTFB",(function(){return E}));var r,a,o=function(){return"".concat(Date.now(),"-").concat(Math.floor(8999999999999*Math.random())+1e12)},i=function(e){var t=arguments.length>1&&void 0!==arguments[1]?arguments[1]:-1;return{name:e,value:t,delta:0,entries:[],id:o(),isFinal:!1}},c=function(e,t){try{if(PerformanceObserver.supportedEntryTypes.includes(e)){var n=new PerformanceObserver((function(e){return e.getEntries().map(t)}));return n.observe({type:e,buffered:!0}),n}}catch(e){}},u=!1,s=!1,f=function(e){u=!e.persisted},l=function(){addEventListener("pagehide",f),addEventListener("unload",(function(){}))},p=function(e){var t=arguments.length>1&&void 0!==arguments[1]&&arguments[1];s||(l(),s=!0),addEventListener("visibilitychange"</td></tr>
</table>

C:\Users\user\AppData\Local\Temp\~DF48AB3BDE441DDBFB.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.34911106377658885
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laAgg9wc:kBqoxxJhHWSVSEab9wc
MD5:	6EB31D28AA7745AC5EA3EC5077A5C681
SHA1:	AD73FDD85BB2BB042ABFC1AAEB28622D669EB126
SHA-256:	F4E386D4F690E270A6810EE8F85822BC875772D8D0F0A5AC5FB13D9346983583
SHA-512:	DF007528D0818FFFD52DD5A1D27993D3CF5A6ED0ED38F626F7E60EBA90D3C4944BD2A36B3842E14A0C1EA50646646AF3180EBD1641A408B34A4DE09E2AF81D 6
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF7AB176D309131995.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13349
Entropy (8bit):	0.6670220553699899
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lokF9lok9lWfll1lUGaGk31lGkUGkr5:kBqoIfpdBUGaGk3bGkUGkr5
MD5:	FBFA984677E151C62D089E1EFBC10937
SHA1:	1D55AE3C1095FDD0EC049234A009D8202F9665AB
SHA-256:	6A618B0A00A9DD98F8E6AFB0E410950EE10BD8FF7B6F318C8B28FA4E2A5BDCD2
SHA-512:	33F5F60213D945190F6C92A5628D0759BEAA5F9A34992ECA76BB8311281BCCF83E50F622A1251EF100059A06D416F3AAF3D7E42BBF544A51F1D9A178897B3335
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFA61C54DA1C9AEE49.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	47875
Entropy (8bit):	0.6961462741941471
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+npLCJl9r6XgTIBPglr8qCMVwKWd+i/CHP:kBqoxKAuqR+npLCJl8KuYeqJi/a
MD5:	6E88E2287D13175A6C811F1A17220F9A
SHA1:	390E32065FEE2E597BCDE319620F884EAACA36CD
SHA-256:	A99F49EB4C087AB51A3F5902674E74EFC18071317694D00BFAF41FAADCA35113
SHA-512:	51C2401F146E91A86DE0791D7B50DE36DB1E2311FF4F0437D20A8B9D654DFAD20DB25E559EC2124F0F61D510ED8DBB37376B1AAE51A65CD52FD2271AEA1BCE 97
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFC7DF538CFEB55E09.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data

C:\Users\user\AppData\Local\Temp\~DFC7DF538CFEB55E09.TMP	
Category:	dropped
Size (bytes):	35179
Entropy (8bit):	0.46949072773532674
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+1bZILTfCqCn0xCgCSCHCJ56:kBqoxKAuqR+1bZILTf140xbF0
MD5:	D2713423A5046AED7E31AE7EB5FE2968
SHA1:	1DBDB7B8E178CF4FAB47748F90FAFB3B72C896BD
SHA-256:	BC973FB5A3B0A52AEC1AE272A66334177403FF20E2AFE537526444C5A3ACB8CB
SHA-512:	FD4CB7ECB70DF6C3107E60C09D2AB83F183889CF3F9E35C4E89A462512F0DA4DC5974976EE8FEE5AAC8DF49E712F4D021F7EFF471680092F8ADF6F4296F4796
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\Desktop\~$Direct Deposit.xlsx	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	165
Entropy (8bit):	1.6081032063576088
Encrypted:	false
SSDEEP:	3:RFXI6dtt:RJ1
MD5:	7AB76C81182111AC93ACF915CA8331D5
SHA1:	68B94B5D4C83A6FB415C8026AF61F3F8745E2559
SHA-256:	6A499C020C6F82C54CD991CA52F84558C518CBD310B10623D847D878983A40EF
SHA-512:	A09AB74DE8A70886C22FB628BDB6A2D773D31402D4E721F9EE2F8CCEE23A569342FEECF1B85C1A25183DD370D1DFFFF75317F628F9B3AA363BBB60694F5362C 7
Malicious:	false
Preview:	.pratesh ..p.r.a.t.e.s.h. . . . .

Static File Info

General

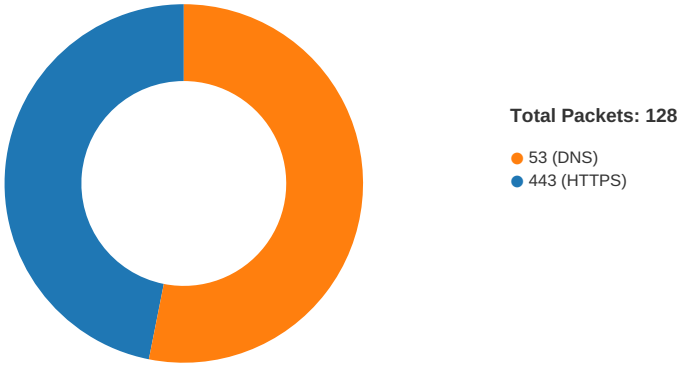
File type:	Microsoft Excel 2007+
Entropy (8bit):	7.875577413292684
TrID:	• Excel Microsoft Office Open XML Format document (40004/1) 83.33% • ZIP compressed archive (8000/1) 16.67%
File name:	Direct Deposit.xlsx
File size:	53638
MD5:	69e51c55e817ad606af9c380ff76ea90
SHA1:	0385a74d84fbf8964d363fb979ecf6afe14b5eba
SHA256:	c38e8675fe9efcc6c74ac66c182c58d458b091d14ababda 785b3144e3fbbfe6f
SHA512:	a4053c28b7697e1ecf5a0f9b63e39217e5c179318f21ea6 a502a270109460250c89a6000e57cf84d16c5396ad0a2e 34017609f369262fbc49c127f589fd6b255
SSDEEP:	1536:LFxJ4QsSxCGi2JGHCv3wcQMcK6XvI/R1ZtdVF+ +:JcQxC0JurUcTsJz
File Content Preview:	PK.....!..`p.....[Content_Types].xml ...(..... ....

File Icon

Icon Hash:	74ecd0d2d6d6d0dc

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 14:47:35.082258940 CET	49738	443	192.168.2.3	151.101.2.133
Nov 27, 2020 14:47:35.082637072 CET	49739	443	192.168.2.3	151.101.2.133
Nov 27, 2020 14:47:35.101594925 CET	443	49738	151.101.2.133	192.168.2.3
Nov 27, 2020 14:47:35.101703882 CET	443	49739	151.101.2.133	192.168.2.3
Nov 27, 2020 14:47:35.101747036 CET	49738	443	192.168.2.3	151.101.2.133
Nov 27, 2020 14:47:35.101819992 CET	49739	443	192.168.2.3	151.101.2.133
Nov 27, 2020 14:47:35.110439062 CET	49738	443	192.168.2.3	151.101.2.133
Nov 27, 2020 14:47:35.110507011 CET	49739	443	192.168.2.3	151.101.2.133
Nov 27, 2020 14:47:35.129683971 CET	443	49738	151.101.2.133	192.168.2.3
Nov 27, 2020 14:47:35.129733086 CET	443	49739	151.101.2.133	192.168.2.3
Nov 27, 2020 14:47:35.130861044 CET	443	49739	151.101.2.133	192.168.2.3
Nov 27, 2020 14:47:35.130901098 CET	443	49739	151.101.2.133	192.168.2.3
Nov 27, 2020 14:47:35.130939960 CET	443	49739	151.101.2.133	192.168.2.3
Nov 27, 2020 14:47:35.130983114 CET	443	49738	151.101.2.133	192.168.2.3
Nov 27, 2020 14:47:35.131015062 CET	49739	443	192.168.2.3	151.101.2.133
Nov 27, 2020 14:47:35.131021023 CET	443	49738	151.101.2.133	192.168.2.3
Nov 27, 2020 14:47:35.131036043 CET	49739	443	192.168.2.3	151.101.2.133
Nov 27, 2020 14:47:35.131052017 CET	443	49738	151.101.2.133	192.168.2.3
Nov 27, 2020 14:47:35.131098986 CET	49738	443	192.168.2.3	151.101.2.133
Nov 27, 2020 14:47:35.131120920 CET	49738	443	192.168.2.3	151.101.2.133
Nov 27, 2020 14:47:35.131123066 CET	49738	443	192.168.2.3	151.101.2.133
Nov 27, 2020 14:47:35.164391994 CET	49739	443	192.168.2.3	151.101.2.133
Nov 27, 2020 14:47:35.164434910 CET	49738	443	192.168.2.3	151.101.2.133
Nov 27, 2020 14:47:35.180423975 CET	49739	443	192.168.2.3	151.101.2.133
Nov 27, 2020 14:47:35.180752039 CET	49739	443	192.168.2.3	151.101.2.133
Nov 27, 2020 14:47:35.180783033 CET	49738	443	192.168.2.3	151.101.2.133
Nov 27, 2020 14:47:35.183917999 CET	443	49739	151.101.2.133	192.168.2.3
Nov 27, 2020 14:47:35.183957100 CET	443	49738	151.101.2.133	192.168.2.3
Nov 27, 2020 14:47:35.184067965 CET	49739	443	192.168.2.3	151.101.2.133
Nov 27, 2020 14:47:35.184082985 CET	49738	443	192.168.2.3	151.101.2.133
Nov 27, 2020 14:47:35.199711084 CET	443	49739	151.101.2.133	192.168.2.3
Nov 27, 2020 14:47:35.199836016 CET	49739	443	192.168.2.3	151.101.2.133
Nov 27, 2020 14:47:35.199842930 CET	443	49738	151.101.2.133	192.168.2.3
Nov 27, 2020 14:47:35.199996948 CET	49739	443	192.168.2.3	151.101.2.133
Nov 27, 2020 14:47:35.200061083 CET	49738	443	192.168.2.3	151.101.2.133
Nov 27, 2020 14:47:35.200293064 CET	49738	443	192.168.2.3	151.101.2.133
Nov 27, 2020 14:47:35.200823069 CET	443	49739	151.101.2.133	192.168.2.3
Nov 27, 2020 14:47:35.200901031 CET	49739	443	192.168.2.3	151.101.2.133
Nov 27, 2020 14:47:35.200913906 CET	443	49739	151.101.2.133	192.168.2.3
Nov 27, 2020 14:47:35.200998068 CET	443	49739	151.101.2.133	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 14:47:35.201018095 CET	49739	443	192.168.2.3	151.101.2.133
Nov 27, 2020 14:47:35.201039076 CET	443	49739	151.101.2.133	192.168.2.3
Nov 27, 2020 14:47:35.201056957 CET	49739	443	192.168.2.3	151.101.2.133
Nov 27, 2020 14:47:35.201076984 CET	443	49739	151.101.2.133	192.168.2.3
Nov 27, 2020 14:47:35.201117039 CET	49739	443	192.168.2.3	151.101.2.133
Nov 27, 2020 14:47:35.201211929 CET	49739	443	192.168.2.3	151.101.2.133
Nov 27, 2020 14:47:35.260289907 CET	443	49738	151.101.2.133	192.168.2.3
Nov 27, 2020 14:47:35.261503935 CET	443	49739	151.101.2.133	192.168.2.3
Nov 27, 2020 14:47:35.298533916 CET	49739	443	192.168.2.3	151.101.2.133
Nov 27, 2020 14:47:35.317771912 CET	443	49739	151.101.2.133	192.168.2.3
Nov 27, 2020 14:47:35.318054914 CET	443	49739	151.101.2.133	192.168.2.3
Nov 27, 2020 14:47:35.318141937 CET	443	49739	151.101.2.133	192.168.2.3
Nov 27, 2020 14:47:35.318217993 CET	443	49739	151.101.2.133	192.168.2.3
Nov 27, 2020 14:47:35.318269014 CET	49739	443	192.168.2.3	151.101.2.133
Nov 27, 2020 14:47:35.318315983 CET	49739	443	192.168.2.3	151.101.2.133
Nov 27, 2020 14:47:35.318324089 CET	49739	443	192.168.2.3	151.101.2.133
Nov 27, 2020 14:47:35.330845118 CET	49739	443	192.168.2.3	151.101.2.133
Nov 27, 2020 14:47:35.331098080 CET	49739	443	192.168.2.3	151.101.2.133
Nov 27, 2020 14:47:35.331271887 CET	49739	443	192.168.2.3	151.101.2.133
Nov 27, 2020 14:47:35.331460953 CET	49739	443	192.168.2.3	151.101.2.133
Nov 27, 2020 14:47:35.331607103 CET	49739	443	192.168.2.3	151.101.2.133
Nov 27, 2020 14:47:35.331759930 CET	49739	443	192.168.2.3	151.101.2.133
Nov 27, 2020 14:47:35.331907988 CET	49739	443	192.168.2.3	151.101.2.133
Nov 27, 2020 14:47:35.332068920 CET	49739	443	192.168.2.3	151.101.2.133
Nov 27, 2020 14:47:35.332201004 CET	49739	443	192.168.2.3	151.101.2.133
Nov 27, 2020 14:47:35.332350016 CET	49739	443	192.168.2.3	151.101.2.133
Nov 27, 2020 14:47:35.332740068 CET	49739	443	192.168.2.3	151.101.2.133
Nov 27, 2020 14:47:35.332845926 CET	49739	443	192.168.2.3	151.101.2.133
Nov 27, 2020 14:47:35.333158970 CET	49739	443	192.168.2.3	151.101.2.133
Nov 27, 2020 14:47:35.333425045 CET	49739	443	192.168.2.3	151.101.2.133
Nov 27, 2020 14:47:35.333622932 CET	49739	443	192.168.2.3	151.101.2.133
Nov 27, 2020 14:47:35.333842993 CET	49739	443	192.168.2.3	151.101.2.133
Nov 27, 2020 14:47:35.334022999 CET	49739	443	192.168.2.3	151.101.2.133
Nov 27, 2020 14:47:35.334240913 CET	49739	443	192.168.2.3	151.101.2.133
Nov 27, 2020 14:47:35.350168943 CET	443	49739	151.101.2.133	192.168.2.3
Nov 27, 2020 14:47:35.350506067 CET	443	49739	151.101.2.133	192.168.2.3
Nov 27, 2020 14:47:35.350653887 CET	49739	443	192.168.2.3	151.101.2.133
Nov 27, 2020 14:47:35.350698948 CET	443	49739	151.101.2.133	192.168.2.3
Nov 27, 2020 14:47:35.350740910 CET	443	49739	151.101.2.133	192.168.2.3
Nov 27, 2020 14:47:35.350780964 CET	443	49739	151.101.2.133	192.168.2.3
Nov 27, 2020 14:47:35.350809097 CET	49739	443	192.168.2.3	151.101.2.133
Nov 27, 2020 14:47:35.350821972 CET	443	49739	151.101.2.133	192.168.2.3
Nov 27, 2020 14:47:35.350832939 CET	49739	443	192.168.2.3	151.101.2.133
Nov 27, 2020 14:47:35.350861073 CET	443	49739	151.101.2.133	192.168.2.3
Nov 27, 2020 14:47:35.350871086 CET	49739	443	192.168.2.3	151.101.2.133
Nov 27, 2020 14:47:35.350902081 CET	443	49739	151.101.2.133	192.168.2.3
Nov 27, 2020 14:47:35.350904942 CET	49739	443	192.168.2.3	151.101.2.133
Nov 27, 2020 14:47:35.350941896 CET	443	49739	151.101.2.133	192.168.2.3
Nov 27, 2020 14:47:35.350959063 CET	49739	443	192.168.2.3	151.101.2.133
Nov 27, 2020 14:47:35.350991011 CET	443	49739	151.101.2.133	192.168.2.3
Nov 27, 2020 14:47:35.351007938 CET	49739	443	192.168.2.3	151.101.2.133
Nov 27, 2020 14:47:35.351033926 CET	49739	443	192.168.2.3	151.101.2.133
Nov 27, 2020 14:47:35.351035118 CET	443	49739	151.101.2.133	192.168.2.3
Nov 27, 2020 14:47:35.351073980 CET	443	49739	151.101.2.133	192.168.2.3
Nov 27, 2020 14:47:35.351089001 CET	49739	443	192.168.2.3	151.101.2.133
Nov 27, 2020 14:47:35.351125956 CET	49739	443	192.168.2.3	151.101.2.133
Nov 27, 2020 14:47:35.351712942 CET	443	49739	151.101.2.133	192.168.2.3
Nov 27, 2020 14:47:35.351767063 CET	443	49739	151.101.2.133	192.168.2.3
Nov 27, 2020 14:47:35.351809978 CET	443	49739	151.101.2.133	192.168.2.3
Nov 27, 2020 14:47:35.351821899 CET	49739	443	192.168.2.3	151.101.2.133

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 14:46:29.099612951 CET	49199	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:46:29.126678944 CET	53	49199	8.8.8.8	192.168.2.3
Nov 27, 2020 14:46:30.712130070 CET	50620	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:46:30.739326954 CET	53	50620	8.8.8.8	192.168.2.3
Nov 27, 2020 14:46:31.175241947 CET	64938	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:46:31.202406883 CET	53	64938	8.8.8.8	192.168.2.3
Nov 27, 2020 14:46:38.435497999 CET	60152	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:46:38.473359108 CET	53	60152	8.8.8.8	192.168.2.3
Nov 27, 2020 14:46:38.708340883 CET	57544	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:46:38.744191885 CET	53	57544	8.8.8.8	192.168.2.3
Nov 27, 2020 14:46:39.696630001 CET	57544	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:46:39.737029076 CET	53	57544	8.8.8.8	192.168.2.3
Nov 27, 2020 14:46:40.711402893 CET	57544	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:46:40.738310099 CET	53	57544	8.8.8.8	192.168.2.3
Nov 27, 2020 14:46:42.727555990 CET	57544	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:46:42.754827023 CET	53	57544	8.8.8.8	192.168.2.3
Nov 27, 2020 14:46:46.785114050 CET	57544	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:46:46.842192888 CET	53	57544	8.8.8.8	192.168.2.3
Nov 27, 2020 14:46:53.945122957 CET	55984	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:46:53.972429991 CET	53	55984	8.8.8.8	192.168.2.3
Nov 27, 2020 14:46:56.088944912 CET	64185	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:46:56.116077900 CET	53	64185	8.8.8.8	192.168.2.3
Nov 27, 2020 14:46:56.859697104 CET	65110	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:46:56.886919975 CET	53	65110	8.8.8.8	192.168.2.3
Nov 27, 2020 14:46:57.655550957 CET	58361	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:46:57.682653904 CET	53	58361	8.8.8.8	192.168.2.3
Nov 27, 2020 14:46:57.990993023 CET	63492	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:46:58.027961016 CET	53	63492	8.8.8.8	192.168.2.3
Nov 27, 2020 14:46:58.467108011 CET	60831	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:46:58.494237900 CET	53	60831	8.8.8.8	192.168.2.3
Nov 27, 2020 14:46:59.244803905 CET	60100	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:46:59.281605005 CET	53	60100	8.8.8.8	192.168.2.3
Nov 27, 2020 14:46:59.331382990 CET	53195	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:46:59.358388901 CET	53	53195	8.8.8.8	192.168.2.3
Nov 27, 2020 14:47:00.005183935 CET	50141	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:47:00.032151937 CET	53	50141	8.8.8.8	192.168.2.3
Nov 27, 2020 14:47:00.673638105 CET	53023	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:47:00.700829029 CET	53	53023	8.8.8.8	192.168.2.3
Nov 27, 2020 14:47:01.347470999 CET	49563	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:47:01.374476910 CET	53	49563	8.8.8.8	192.168.2.3
Nov 27, 2020 14:47:07.864713907 CET	51352	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:47:07.891802073 CET	53	51352	8.8.8.8	192.168.2.3
Nov 27, 2020 14:47:08.795947075 CET	59349	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:47:08.831490993 CET	53	59349	8.8.8.8	192.168.2.3
Nov 27, 2020 14:47:09.986284971 CET	57084	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:47:10.013732910 CET	53	57084	8.8.8.8	192.168.2.3
Nov 27, 2020 14:47:10.298171043 CET	58823	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:47:10.325375080 CET	53	58823	8.8.8.8	192.168.2.3
Nov 27, 2020 14:47:11.013269901 CET	57568	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:47:11.040349007 CET	53	57568	8.8.8.8	192.168.2.3
Nov 27, 2020 14:47:11.841718912 CET	50540	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:47:11.879539013 CET	53	50540	8.8.8.8	192.168.2.3
Nov 27, 2020 14:47:12.666131020 CET	54366	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:47:12.702115059 CET	53	54366	8.8.8.8	192.168.2.3
Nov 27, 2020 14:47:13.789660931 CET	53034	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:47:13.816951036 CET	53	53034	8.8.8.8	192.168.2.3
Nov 27, 2020 14:47:14.918428898 CET	57762	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:47:14.945622921 CET	53	57762	8.8.8.8	192.168.2.3
Nov 27, 2020 14:47:16.737513065 CET	55435	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:47:16.764647007 CET	53	55435	8.8.8.8	192.168.2.3
Nov 27, 2020 14:47:28.386796951 CET	50713	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:47:28.413939953 CET	53	50713	8.8.8.8	192.168.2.3
Nov 27, 2020 14:47:32.093544960 CET	56132	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:47:32.130310059 CET	53	56132	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 14:47:33.475047112 CET	58987	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:47:33.511924028 CET	53	58987	8.8.8.8	192.168.2.3
Nov 27, 2020 14:47:35.008076906 CET	56579	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:47:35.049248934 CET	53	56579	8.8.8.8	192.168.2.3
Nov 27, 2020 14:47:35.289158106 CET	60633	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:47:35.297141075 CET	61292	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:47:35.308268070 CET	63619	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:47:35.325802088 CET	64938	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:47:35.340728998 CET	53	61292	8.8.8.8	192.168.2.3
Nov 27, 2020 14:47:35.343794107 CET	53	63619	8.8.8.8	192.168.2.3
Nov 27, 2020 14:47:35.345407963 CET	53	60633	8.8.8.8	192.168.2.3
Nov 27, 2020 14:47:35.372904062 CET	53	64938	8.8.8.8	192.168.2.3
Nov 27, 2020 14:47:35.750427008 CET	61946	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:47:35.796478033 CET	53	61946	8.8.8.8	192.168.2.3
Nov 27, 2020 14:47:37.896871090 CET	64910	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:47:37.940021992 CET	53	64910	8.8.8.8	192.168.2.3
Nov 27, 2020 14:47:38.392133951 CET	52123	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:47:38.501888990 CET	56130	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:47:38.503247976 CET	56338	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:47:38.530493975 CET	53	56338	8.8.8.8	192.168.2.3
Nov 27, 2020 14:47:38.534224033 CET	59420	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:47:38.547789097 CET	53	56130	8.8.8.8	192.168.2.3
Nov 27, 2020 14:47:38.561460972 CET	53	59420	8.8.8.8	192.168.2.3
Nov 27, 2020 14:47:38.562694073 CET	53	52123	8.8.8.8	192.168.2.3
Nov 27, 2020 14:47:38.567331076 CET	58784	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:47:38.593970060 CET	63978	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:47:38.593997955 CET	62938	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:47:38.600243092 CET	55708	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:47:38.602770090 CET	53	58784	8.8.8.8	192.168.2.3
Nov 27, 2020 14:47:38.620968103 CET	53	62938	8.8.8.8	192.168.2.3
Nov 27, 2020 14:47:38.627202988 CET	53	55708	8.8.8.8	192.168.2.3
Nov 27, 2020 14:47:38.631197929 CET	53	63978	8.8.8.8	192.168.2.3
Nov 27, 2020 14:47:38.963567972 CET	56803	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:47:38.999099970 CET	53	56803	8.8.8.8	192.168.2.3
Nov 27, 2020 14:47:39.076328039 CET	57145	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:47:39.124172926 CET	53	57145	8.8.8.8	192.168.2.3
Nov 27, 2020 14:48:02.893215895 CET	55359	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:48:02.920351028 CET	53	55359	8.8.8.8	192.168.2.3
Nov 27, 2020 14:48:03.458997965 CET	58306	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:48:03.486264944 CET	53	58306	8.8.8.8	192.168.2.3
Nov 27, 2020 14:48:04.375013113 CET	64124	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:48:04.410578012 CET	53	64124	8.8.8.8	192.168.2.3
Nov 27, 2020 14:48:04.453280926 CET	58306	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:48:04.480391979 CET	53	58306	8.8.8.8	192.168.2.3
Nov 27, 2020 14:48:04.858535051 CET	49361	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:48:04.904463053 CET	53	49361	8.8.8.8	192.168.2.3
Nov 27, 2020 14:48:05.375094891 CET	64124	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:48:05.402359962 CET	53	64124	8.8.8.8	192.168.2.3
Nov 27, 2020 14:48:05.469671965 CET	58306	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:48:05.496870995 CET	53	58306	8.8.8.8	192.168.2.3
Nov 27, 2020 14:48:06.390693903 CET	64124	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:48:06.417737007 CET	53	64124	8.8.8.8	192.168.2.3
Nov 27, 2020 14:48:07.128603935 CET	63150	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:48:07.155899048 CET	53	63150	8.8.8.8	192.168.2.3
Nov 27, 2020 14:48:07.484389067 CET	58306	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:48:07.511636972 CET	53	58306	8.8.8.8	192.168.2.3
Nov 27, 2020 14:48:08.125349045 CET	63150	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:48:08.152558088 CET	53	63150	8.8.8.8	192.168.2.3
Nov 27, 2020 14:48:08.391643047 CET	64124	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:48:08.418883085 CET	53	64124	8.8.8.8	192.168.2.3
Nov 27, 2020 14:48:09.140721083 CET	63150	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:48:09.167875051 CET	53	63150	8.8.8.8	192.168.2.3
Nov 27, 2020 14:48:11.156466961 CET	63150	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:48:11.183748960 CET	53	63150	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 14:48:11.500576973 CET	58306	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:48:11.529196978 CET	53	58306	8.8.8.8	192.168.2.3
Nov 27, 2020 14:48:12.406932116 CET	64124	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:48:12.434143066 CET	53	64124	8.8.8.8	192.168.2.3
Nov 27, 2020 14:48:15.156784058 CET	63150	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:48:15.184125900 CET	53	63150	8.8.8.8	192.168.2.3
Nov 27, 2020 14:48:30.902879000 CET	53279	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:48:30.938793898 CET	53	53279	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 27, 2020 14:47:35.008076906 CET	192.168.2.3	8.8.8.8	0x6776	Standard query (0)	linktr.ee	A (IP address)	IN (0x0001)
Nov 27, 2020 14:47:35.325802088 CET	192.168.2.3	8.8.8.8	0x114e	Standard query (0)	d1fdloi71m ui9q.cloud front.net	A (IP address)	IN (0x0001)
Nov 27, 2020 14:47:37.896871090 CET	192.168.2.3	8.8.8.8	0x9f5a	Standard query (0)	secure-excel-file.glitch.me	A (IP address)	IN (0x0001)
Nov 27, 2020 14:47:38.392133951 CET	192.168.2.3	8.8.8.8	0xae8d	Standard query (0)	ibuykenya.com	A (IP address)	IN (0x0001)
Nov 27, 2020 14:47:38.503247976 CET	192.168.2.3	8.8.8.8	0x7723	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)
Nov 27, 2020 14:47:38.534224033 CET	192.168.2.3	8.8.8.8	0x4708	Standard query (0)	maxcdn.bootstrapcdn.com	A (IP address)	IN (0x0001)
Nov 27, 2020 14:47:38.593970060 CET	192.168.2.3	8.8.8.8	0x6e12	Standard query (0)	secure.aadcdn.microsoftonline-p.com	A (IP address)	IN (0x0001)
Nov 27, 2020 14:47:38.593997955 CET	192.168.2.3	8.8.8.8	0x749f	Standard query (0)	kit.fontawesome.com	A (IP address)	IN (0x0001)
Nov 27, 2020 14:47:38.600243092 CET	192.168.2.3	8.8.8.8	0xdf5e	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
Nov 27, 2020 14:47:38.963567972 CET	192.168.2.3	8.8.8.8	0x925b	Standard query (0)	ka-f.fontawesome.com	A (IP address)	IN (0x0001)
Nov 27, 2020 14:47:39.076328039 CET	192.168.2.3	8.8.8.8	0x43e4	Standard query (0)	i.ibb.co	A (IP address)	IN (0x0001)
Nov 27, 2020 14:48:30.902879000 CET	192.168.2.3	8.8.8.8	0x11fc	Standard query (0)	linktr.ee	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 27, 2020 14:47:35.049248934 CET	8.8.8.8	192.168.2.3	0x6776	No error (0)	linktr.ee		151.101.2.133	A (IP address)	IN (0x0001)
Nov 27, 2020 14:47:35.049248934 CET	8.8.8.8	192.168.2.3	0x6776	No error (0)	linktr.ee		151.101.194.133	A (IP address)	IN (0x0001)
Nov 27, 2020 14:47:35.049248934 CET	8.8.8.8	192.168.2.3	0x6776	No error (0)	linktr.ee		151.101.130.133	A (IP address)	IN (0x0001)
Nov 27, 2020 14:47:35.049248934 CET	8.8.8.8	192.168.2.3	0x6776	No error (0)	linktr.ee		151.101.66.133	A (IP address)	IN (0x0001)
Nov 27, 2020 14:47:35.340728998 CET	8.8.8.8	192.168.2.3	0x72dc	No error (0)	pagead.l.doubleclick.net		172.217.168.66	A (IP address)	IN (0x0001)
Nov 27, 2020 14:47:35.372904062 CET	8.8.8.8	192.168.2.3	0x114e	No error (0)	d1fdloi71m ui9q.cloud front.net		13.224.195.11	A (IP address)	IN (0x0001)
Nov 27, 2020 14:47:35.372904062 CET	8.8.8.8	192.168.2.3	0x114e	No error (0)	d1fdloi71m ui9q.cloud front.net		13.224.195.143	A (IP address)	IN (0x0001)
Nov 27, 2020 14:47:35.372904062 CET	8.8.8.8	192.168.2.3	0x114e	No error (0)	d1fdloi71m ui9q.cloud front.net		13.224.195.64	A (IP address)	IN (0x0001)
Nov 27, 2020 14:47:35.372904062 CET	8.8.8.8	192.168.2.3	0x114e	No error (0)	d1fdloi71m ui9q.cloud front.net		13.224.195.67	A (IP address)	IN (0x0001)
Nov 27, 2020 14:47:37.940021992 CET	8.8.8.8	192.168.2.3	0x9f5a	No error (0)	secure-excel-file.glitch.me		34.231.129.212	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 27, 2020 14:47:37.940021992 CET	8.8.8.8	192.168.2.3	0x9f5a	No error (0)	secure-excel-file.glitch.me		52.205.236.122	A (IP address)	IN (0x0001)
Nov 27, 2020 14:47:38.530493975 CET	8.8.8.8	192.168.2.3	0x7723	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Nov 27, 2020 14:47:38.561460972 CET	8.8.8.8	192.168.2.3	0x4708	No error (0)	maxcdn.bootstrapcdn.com	cds.j3z9t3p6.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Nov 27, 2020 14:47:38.562694073 CET	8.8.8.8	192.168.2.3	0xae8d	No error (0)	ibuykenya.com		50.87.153.159	A (IP address)	IN (0x0001)
Nov 27, 2020 14:47:38.620968103 CET	8.8.8.8	192.168.2.3	0x749f	No error (0)	kit.fontawesome.com	kit.fontawesome.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Nov 27, 2020 14:47:38.627202988 CET	8.8.8.8	192.168.2.3	0xdf5e	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Nov 27, 2020 14:47:38.627202988 CET	8.8.8.8	192.168.2.3	0xdf5e	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Nov 27, 2020 14:47:38.631197929 CET	8.8.8.8	192.168.2.3	0x6e12	No error (0)	secure.aadcdn.microsoftonline-p.com	secure.aadcdn.microsoftonline-p.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Nov 27, 2020 14:47:38.999099970 CET	8.8.8.8	192.168.2.3	0x925b	No error (0)	ka-f.fontawesome.com	ka-f.fontawesome.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Nov 27, 2020 14:47:39.124172926 CET	8.8.8.8	192.168.2.3	0x43e4	No error (0)	i.ibb.co		145.239.131.51	A (IP address)	IN (0x0001)
Nov 27, 2020 14:47:39.124172926 CET	8.8.8.8	192.168.2.3	0x43e4	No error (0)	i.ibb.co		145.239.131.55	A (IP address)	IN (0x0001)
Nov 27, 2020 14:47:39.124172926 CET	8.8.8.8	192.168.2.3	0x43e4	No error (0)	i.ibb.co		145.239.131.60	A (IP address)	IN (0x0001)
Nov 27, 2020 14:48:30.938793898 CET	8.8.8.8	192.168.2.3	0x11fc	No error (0)	linktr.ee		151.101.66.133	A (IP address)	IN (0x0001)
Nov 27, 2020 14:48:30.938793898 CET	8.8.8.8	192.168.2.3	0x11fc	No error (0)	linktr.ee		151.101.194.133	A (IP address)	IN (0x0001)
Nov 27, 2020 14:48:30.938793898 CET	8.8.8.8	192.168.2.3	0x11fc	No error (0)	linktr.ee		151.101.130.133	A (IP address)	IN (0x0001)
Nov 27, 2020 14:48:30.938793898 CET	8.8.8.8	192.168.2.3	0x11fc	No error (0)	linktr.ee		151.101.2.133	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- ibuykenya.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49758	50.87.153.159	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Nov 27, 2020 14:47:38.859451056 CET	7429	OUT	GET /vendor/doctrine/styles.css HTTP/1.1 Accept: text/css, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: ibuykenya.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Nov 27, 2020 14:47:39.040015936 CET	7445	IN	HTTP/1.1 200 OK Date: Fri, 27 Nov 2020 13:47:38 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, Keep-Alive Last-Modified: Sun, 23 Feb 2020 01:10:17 GMT Accept-Ranges: bytes Vary: Accept-Encoding Content-Encoding: gzip Keep-Alive: timeout=5, max=75 Transfer-Encoding: chunked Content-Type: text/css Data Raw: 31 66 61 61 0d 0a 1f 8b 08 00 00 00 00 00 00 03 cc b2 61 93 e3 38 76 25 fa fd fd 0a 4e 56 54 6c a5 9d d4 12 94 48 4a ac d7 1d 1d de e7 b0 67 77 c6 e1 f0 8c d7 de a8 57 f1 02 24 40 12 9b 20 c0 05 a1 94 b2 26 fa bf 3f 90 92 52 22 04 82 40 56 4d db 59 39 3d cc 7b 2f ce 3d f7 9c 13 04 c1 ff dd cb 57 8a 03 f9 da e1 9f 1e 24 3e ca ff 5a f6 fd c3 cf c1 f8 d3 c8 96 06 7f f9 bf 82 9b 9f 8a 33 19 56 b0 25 f4 35 0f 7a c8 fa b0 c7 82 54 9f 27 43 61 db 87 03 56 d8 93 6f 38 84 e8 7f ef 7b 99 07 20 8a 3e 6a 73 07 5c 3c 13 39 33 fb 36 fa eb db d7 db 47 c1 d1 ab c6 ac 85 a2 26 2c 0f 22 db 3b 28 24 29 29 7e ba 16 7a 82 6e fe 44 58 42 42 fb 6b a1 22 75 09 3b 49 38 9b d4 f6 e2 e6 51 c5 b9 c4 e2 fa 77 83 21 9a fc 5d 0b be ef ae 7f b7 90 dc a0 b5 98 ed af 7f 31 f8 72 fd a3 c7 e5 74 73 bf 6f d5 99 fa e5 88 f4 1d 85 ca 8f 82 f2 f2 d9 7a fe 1e 11 7e 85 2b 21 7b 81 37 c7 76 82 d7 02 f7 37 95 17 a5 0e 9f 5b 47 18 25 0c 87 e3 d6 a9 b1 2f 78 d0 19 d2 10 52 52 2b 4f 0a d8 e3 61 76 91 5b ce b8 fc f4 a5 54 21 13 9c f6 5f 1f e7 56 33 ce f0 74 65 83 49 dd c8 05 fb bf 34 04 21 cc be 5e 0f 94 b8 55 88 12 db 16 59 59 6b 0f 0b 58 3e 0f 76 33 14 96 9c 72 91 07 52 40 d6 77 50 60 26 ad 40 39 54 66 bf dc 46 33 6f b8 12 52 5b c0 f7 72 50 72 29 e7 45 21 be 48 22 29 fe aa 13 e4 42 85 33 2c b8 94 bc cd 03 d0 1d 03 a4 be 31 b2 c1 15 37 11 54 ce b0 5a 03 ad 94 61 e1 e1 ec 40 c1 a9 15 0c 55 cc f4 bc 97 af 54 9d 45 a4 ca 4c 69 7b df 00 e3 73 f2 4d bd 8e 71 3b 8d 45 0b 45 4d 54 02 57 69 86 5b bb 66 6a f4 79 d6 cd 3c f8 50 55 d1 14 fb 6c f0 87 28 b2 e2 f6 2d a4 74 9e f2 36 fa 68 7d bd bf 15 7f df cd 03 65 c9 c7 29 bf 21 27 61 73 76 45 e3 de f1 9e 48 c2 95 32 02 53 38 04 6f da 57 c1 93 a4 84 34 54 6e d4 6a aa 80 3d 1e f0 ec 54 75 76 92 77 79 10 46 ab 04 b7 0b 37 de a5 f4 14 4f f5 36 5e 78 4c 5a 3d 8d a7 88 e7 76 b7 fb 97 3a 67 5c 7e ca 05 e7 f2 51 43 e0 ea fc 8a f2 43 1e 34 04 21 cc 6c 40 15 a9 f7 02 6b 00 97 d8 01 15 ba 4d d4 1d ad 79 16 da e3 b0 e5 df c2 82 1f 07 5f 09 ab 73 15 34 26 b1 f2 59 d5 3e 6b 97 3a 0c bd 25 c0 46 a2 bb 3b e1 aa 01 dc 4b 6e 7b 5b 72 84 af 19 7d 2e d0 d3 2d ec 4d 7a 61 6b 8c 6f 05 5b 42 5f f3 a0 e5 8c f7 1d 2c f1 d3 f5 f3 f3 fd f8 29 ed c0 9e 8a 62 af 02 c4 ae bb 09 eb f6 f2 fa 27 ef 64 2d f8 be bb 21 87 29 2e 6f 26 24 3e 4a 28 30 d4 08 97 9c 72 15 2d c2 1a 2c 88 bc 67 37 d3 ba e4 c1 ea c1 89 f3 ac 0d 2f a4 27 05 c5 3e 57 9f 8e d2 10 87 cb 42 29 20 eb 2b 2e da 3c 60 9c 79 81 36 b2 a5 27 3d bf c8 d7 0e ff f4 70 1a 78 f8 aa a9 7d ee 0a dc 63 39 d7 ec f7 45 4b 54 57 a3 18 1e 70 f1 4c 64 08 bb 0e 43 c5 b4 54 86 9f b6 4c 65 2d f7 a2 1f ec e8 38 61 12 8b e5 2b be 20 d2 43 25 22 fa 6a bc e7 ad ab bb 7e de 83 70 05 f7 54 2e ef c9 f3 b0 e5 df c2 8a 97 fb 3e 24 8c 61 a1 dd 7f 3f a0 ad 2c b8 40 58 ad 8c a6 17 77 10 21 c2 ea 85 24 8d 2b 34 40 4a 18 0e 1b 4c ea 46 0e 9e 8b 16 d2 45 88 b3 4b 65 83 cb e7 82 1f 67 2d 86 88 f0 3b 13 d5 83 b0 27 df 46 b6 a7 6b 42 55 7a f7 39 e7 5d 6c df 16 58 3c 7c 55 02 9e 43 32 aa 17 f6 1d 61 a1 1e 55 fb 43 be 97 d3 87 da 01 17 b1 e0 5e 72 57 7a bd ca 6b d9 38 05 5a e2 a3 ac 08 a6 68 2a c9 98 8b 5b ed 4a ae Data Ascii: 1faaa8v%NVTlHJgwW$@ &?R"@VMY9={/=W$>Z3V%5zT'CaVo8{ >js\<936G&,";($))~znDXBBk"u;I8Qw!]1rt soz~+!{7v7[G%/xRR+Oav[T!_V3tel4!^UYYkX>v3rR@wP`&@9TfF3oR[rPr)E!H")B3,17TZa@UTELi{sMq;EEMTWi[fjy<PUl(-t6h}e)!'asvEH2S8oW4Tnj=TuvwyF7O6^xLZ=v:g\~QCC4!l@kMy_s4&Y>k:%F;Kn{[r}.-Mzako[B_,)b'd-!).o&$>J(0r-,g7/'>WB) +.<`y6'=px}c9EKTWpLdCTLe-8a+ C%"j~pT.>$a?,@Xw!$+4@JLFEKeg-;'FkBUz9]lX<|UC2aUC^rWzk8Zh*[J

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
Nov 27, 2020 14:47:35.130901098 CET	151.101.2.133	443	192.168.2.3	49739	CN=linktr.ee CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Tue Sep 29 08:35:49 CEST 2020 Thu Mar 17 17:40:46 CET 2016	Mon Dec 28 07:35:49 CET 2020 Wed Mar 17 17:40:46 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 17 17:40:46 CET 2016	Wed Mar 17 17:40:46 CET 2021		
Nov 27, 2020 14:47:35.131021023 CET	151.101.2.133	443	192.168.2.3	49738	CN=linktr.ee CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Tue Sep 29 08:35:49 CEST 2020 Thu Mar 17 17:40:46 CET 2016	Mon Dec 28 07:35:49 CET 2020 Wed Mar 17 17:40:46 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 17 17:40:46 CET 2016	Wed Mar 17 17:40:46 CET 2021		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Nov 27, 2020 14:47:35.450189114 CET	172.217.168.66	443	192.168.2.3	49742	CN=www.googleadservices.com, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Nov 03 08:38:18 CET 2020 Thu Jun 15 02:00:42 CEST 2017	Tue Jan 26 08:38:18 CET 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Nov 27, 2020 14:47:35.471040964 CET	13.224.195.11	443	192.168.2.3	49744	CN=*.cloudfront.net, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Global CA G2, O=DigiCert Inc, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global CA G2, O=DigiCert Inc, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=VeriSign Class 3 Public Primary Certification Authority - G5, OU="(c) 2006 VeriSign, Inc. - For authorized use only", OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US	Tue May 26 02:00:00 CEST 2020 Thu Aug 01 14:00:00 CEST 2013 Mon Nov 06 01:00:00 CET 2017	Wed Apr 21 14:00:00 CEST 2021 Tue Aug 01 14:00:00 CEST 2028 Sun Nov 06 00:59:59 CET 2022	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert Global CA G2, O=DigiCert Inc, C=US	CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Aug 01 14:00:00 CEST 2013	Tue Aug 01 14:00:00 CEST 2028		
					CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=VeriSign Class 3 Public Primary Certification Authority - G5, OU="(c) 2006 VeriSign, Inc. - For authorized use only", OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US	Mon Nov 06 01:00:00 CET 2017	Sun Nov 06 00:59:59 CET 2022		
Nov 27, 2020 14:47:35.481376886 CET	172.217.168.66	443	192.168.2.3	49743	CN=www.googleadservices.com, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Nov 03 08:38:18 CET 2020 Thu Jun 15 02:00:42 CEST 2017	Tue Jan 26 08:38:18 CET 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Nov 27, 2020 14:47:35.484180927 CET	13.224.195.11	443	192.168.2.3	49745	CN=*.cloudfront.net, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Global CA G2, O=DigiCert Inc, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global CA G2, O=DigiCert Inc, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=VeriSign Class 3 Public Primary Certification Authority - G5, OU="(c) 2006 VeriSign, Inc. - For authorized use only", OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US	Tue May 26 02:00:00 CEST 2020 Thu Aug 01 14:00:00 CEST 2013 Mon Nov 06 01:00:00 CET 2017	Wed Apr 21 14:00:00 CEST 2021 Tue Aug 01 14:00:00 CEST 2028 Sun Nov 06 00:59:59 CET 2022	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert Global CA G2, O=DigiCert Inc, C=US	CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Aug 01 14:00:00 CEST 2013	Tue Aug 01 14:00:00 CEST 2028		

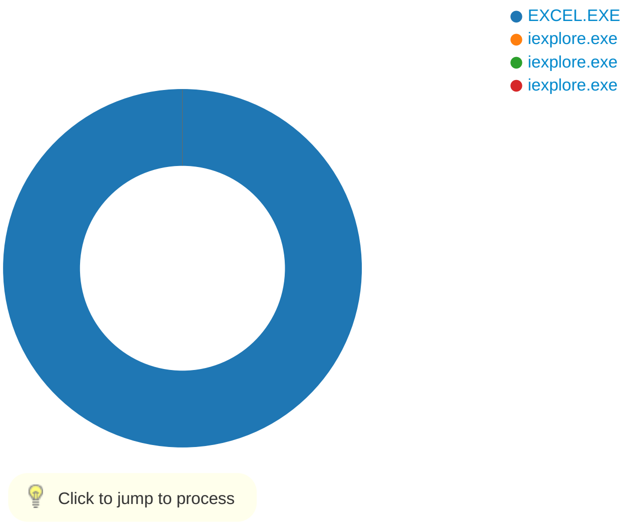
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=VeriSign Class 3 Public Primary Certification Authority - G5, OU="(c) 2006 VeriSign, Inc. - For authorized use only", OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US	Mon Nov 06 01:00:00 CET 2017	Sun Nov 06 00:59:59 CET 2022		
Nov 27, 2020 14:47:38.175476074 CET	34.231.129.212	443	192.168.2.3	49751	CN=glitch.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Tue Feb 18 01:00:00 CET 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Thu Mar 18 13:00:00 CET 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	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=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Nov 27, 2020 14:47:38.176366091 CET	34.231.129.212	443	192.168.2.3	49752	CN=glitch.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Tue Feb 18 01:00:00 CET 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Thu Mar 18 13:00:00 CET 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	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=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Nov 27, 2020 14:47:38.718868017 CET	104.16.19.94	443	192.168.2.3	49766	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Oct 21 02:00:00 CEST 2020	Thu Oct 21 01:59:59 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Nov 27, 2020 14:47:38.719126940 CET	104.16.19.94	443	192.168.2.3	49767	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Oct 21 02:00:00 CEST 2020	Thu Oct 21 01:59:59 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Nov 27, 2020 14:47:39.204296112 CET	145.239.131.51	443	192.168.2.3	49772	CN=ibb.co CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Fri Oct 02 08:53:44 CEST 2020	Thu Dec 31 07:53:44 CET 2020	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=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 17 17:40:46 CET 2016	Wed Mar 17 17:40:46 CET 2021		
Nov 27, 2020 14:47:39.215820074 CET	145.239.131.51	443	192.168.2.3	49773	CN=ibb.co CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Fri Oct 02 08:53:44 CEST 2020	Thu Dec 31 07:53:44 CET 2020	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=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 17 17:40:46 CET 2016	Wed Mar 17 17:40:46 CET 2021		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 6684 Parent PID: 792

General

Start time:	14:46:36
Start date:	27/11/2020
Path:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding
Imagebase:	0x130000
File size:	27110184 bytes
MD5 hash:	5D6638F2C8F8571C593999C58866007E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\3FEF62D9.tmp	success or wait	1	2A495B	DeleteFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$Direct Deposit.xlsx	unknown	55	07 70 72 61 74 65 73 68 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.pratesh	success or wait	1	2951E4	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$Direct Deposit.xlsx	unknown	110	07 00 70 00 72 00 61 00 74 00 65 00 73 00 68 00 20 00	..p.r.a.t.e.s.h.	success or wait	1	295241	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache	success or wait	1	1A20F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	1A211C	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSForms	dword	1	success or wait	1	1A213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	1A213B	RegSetValueExW

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

Analysis Process: iexplore.exe PID: 4900 Parent PID: 792

General

Start time:	14:47:32
Start date:	27/11/2020
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff6672a0000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

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: 4280 Parent PID: 4900

General

Start time:	14:47:32
Start date:	27/11/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4900 CREDAT:17410 /prefetch:2
Imagebase:	0x12d0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 7040 Parent PID: 4900

General

Start time:	14:47:35
Start date:	27/11/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4900 CREDAT:17414 /prefetch:2
Imagebase:	0x12d0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

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

Disassembly