ID: 323781
Sample Name: Direct Deposit.xlsx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 14:38:59
Date: 27/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

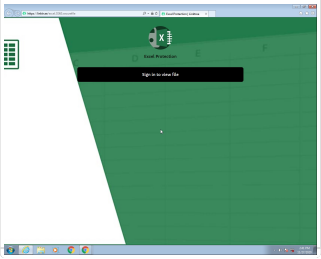
Analysis Report Direct Deposit.xlsx

Overview

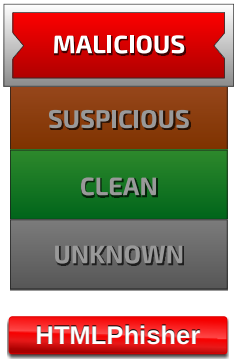
General Information

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

Most interesting Screenshot:



Detection

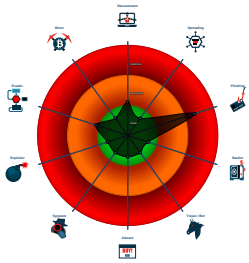


Score:	60
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Yara detected HtmlPhish_10
- Phishing site detected (based on log...
- HTML body contains low number of ...
- HTML title does not match URL
- IP address seen in connection with o...
- Invalid 'forgot password' link found
- JA3 SSL client fingerprint seen in co...

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 2448 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
- iexplore.exe (PID: 1748 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 4EB098135821348270F27157F7A84E65)
  - iexplore.exe (PID: 2352 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:1748 CREDAT:275457 /prefetch:2 MD5: 8A590F790A98F3D77399BE457E01386A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

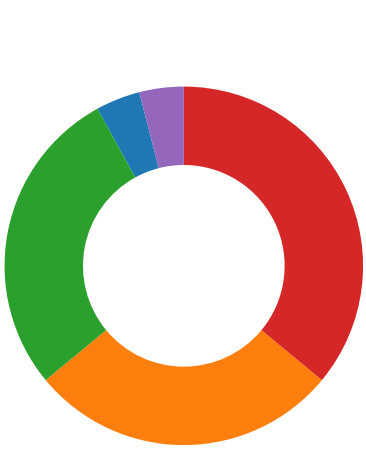
Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\07D9KDVU.htm	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Phishing:

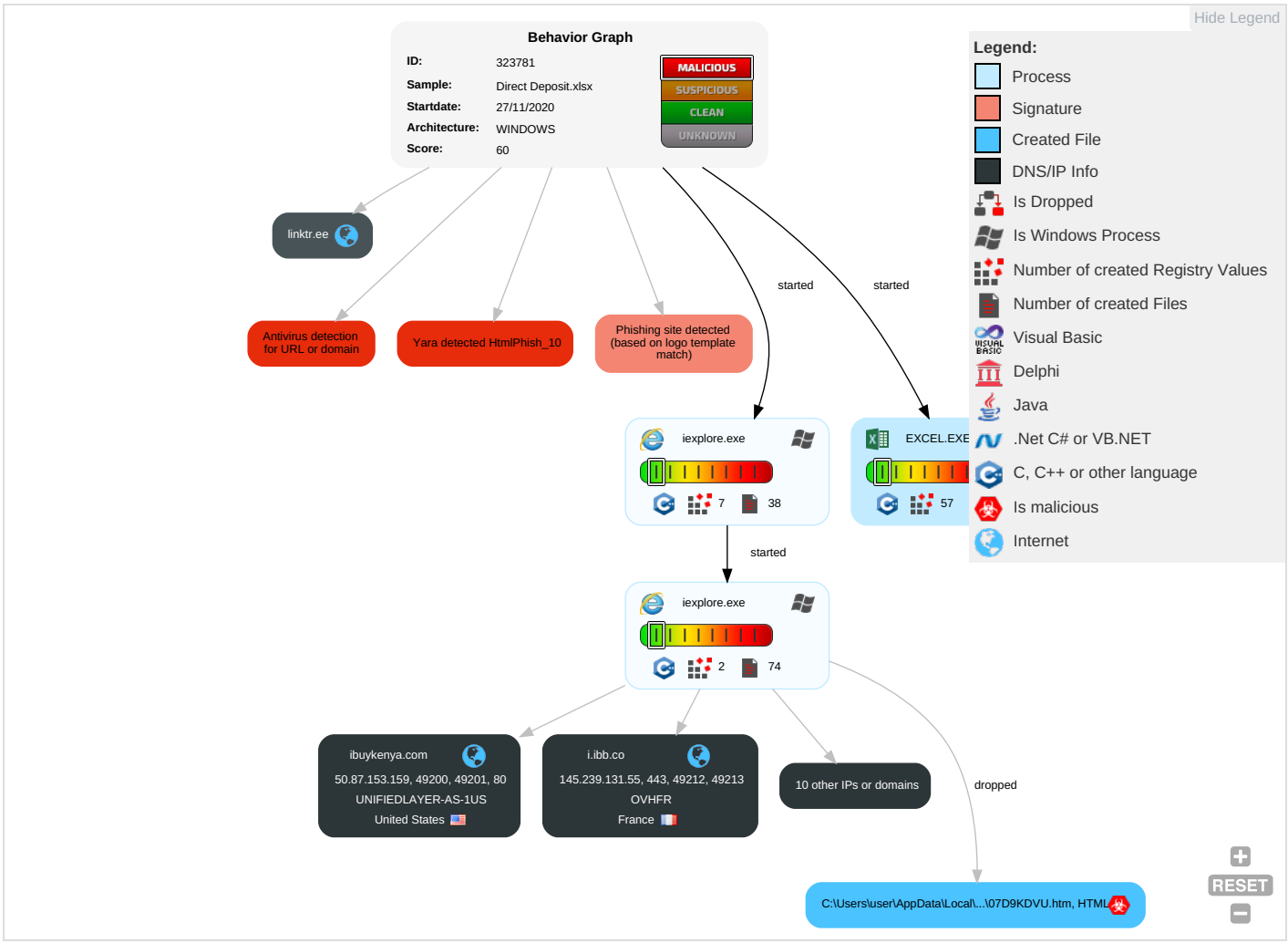
Yara detected HtmlPhish_10

Phishing site detected (based on logo template match)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	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 2	SIM Card Swap		Carri Billin Fraud

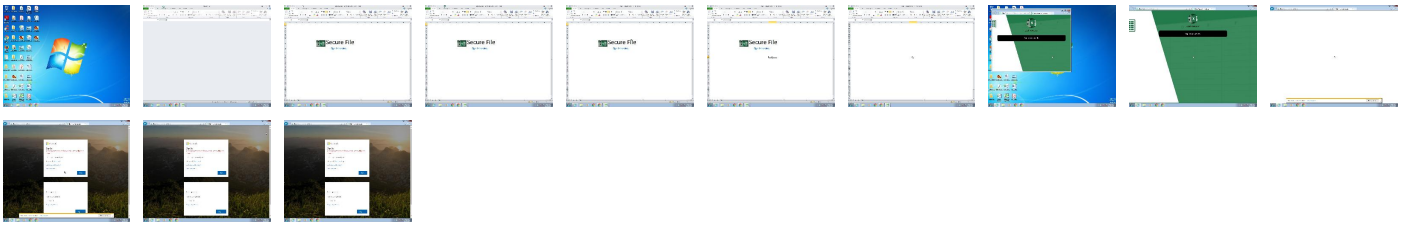
Behavior Graph

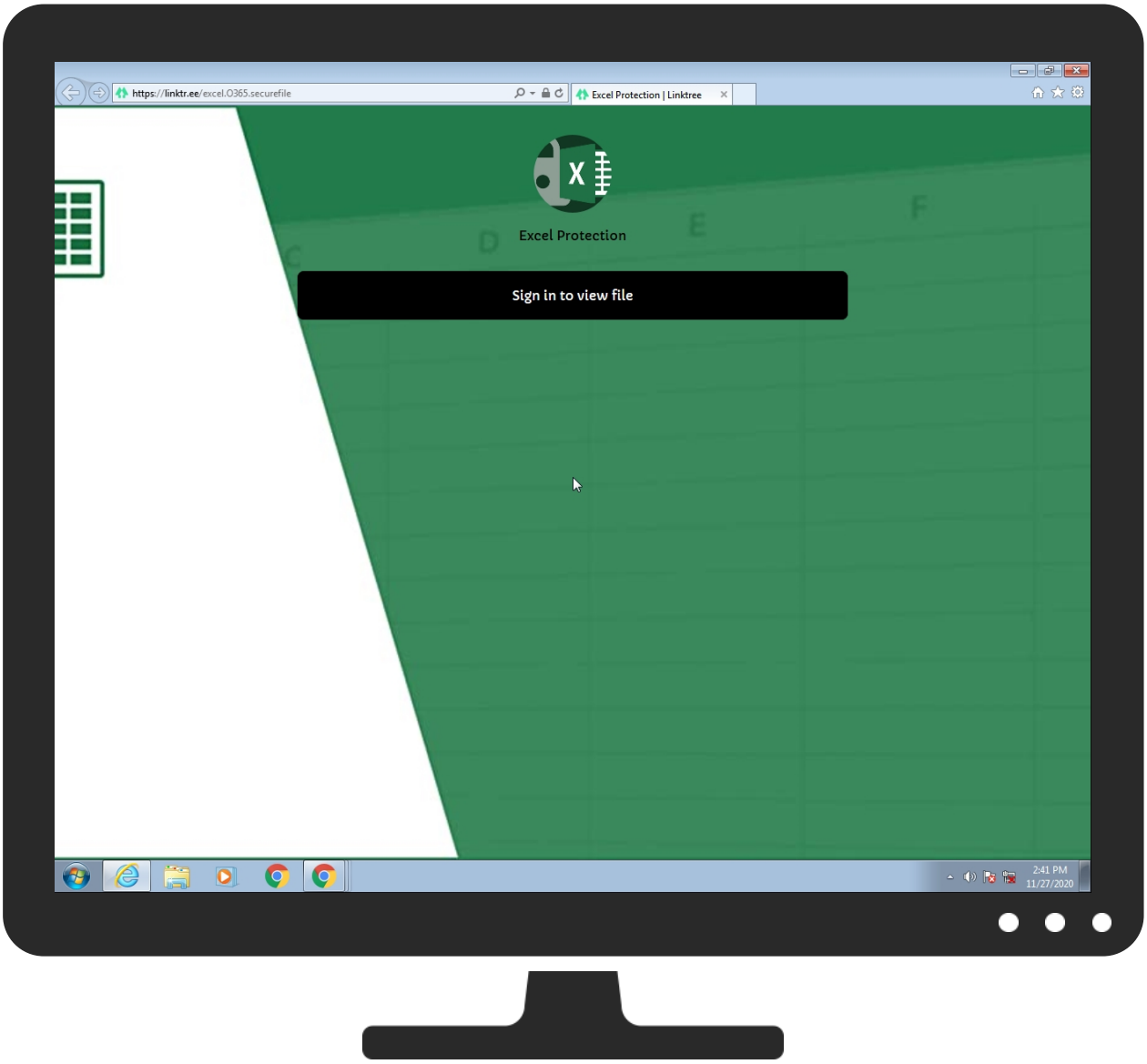


Screenshots

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%	ReversingLabs		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://secure-excel-file.glitch.me/	100%	UrlScan	phishing brand: generic microsoft	Browse
http://ibuykenya.com/vendor/doctrine/styles.css	0%	Avira URL Cloud	safe	
http://https://secure-excel-fl.O365.securefilep	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://promisesaplus.com/#point-75	0%	URL Reputation	safe	
http://https://promisesaplus.com/#point-75	0%	URL Reputation	safe	
http://https://promisesaplus.com/#point-75	0%	URL Reputation	safe	
http://https://fontawesome.comhttps://fontawesome.comFont	0%	Avira URL Cloud	safe	
http://https://promisesaplus.com/#point-64	0%	URL Reputation	safe	
http://https://promisesaplus.com/#point-64	0%	URL Reputation	safe	
http://https://promisesaplus.com/#point-64	0%	URL Reputation	safe	
http://https://cnhind-onmicrosoft-com.ml/email.php	0%	Avira URL Cloud	safe	
http://https://promisesaplus.com/#point-61	0%	URL Reputation	safe	
http://https://promisesaplus.com/#point-61	0%	URL Reputation	safe	
http://https://promisesaplus.com/#point-61	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	151.101.130.133	true	false		high
ibuykenya.com	50.87.153.159	true	false		unknown
secure-excel-file.glitch.me	52.205.236.122	true	false		high
pagead.l.doubleclick.net	172.217.168.2	true	false		high
cdnjs.cloudflare.com	104.16.19.94	true	false		high
d1fdloi71mui9q.cloudfront.net	143.204.214.108	true	false		high
i.ibb.co	145.239.131.55	true	false		high
secure.aadcdn.microsoftonline-p.com	unknown	unknown	false		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	• Avira URL Cloud: safe	unknown
http://https://secure-excel-file.glitch.me/	false	• 100%, UrlScan, Browse	high
http://https://linktr.ee/excel.O365.securefile	false		high

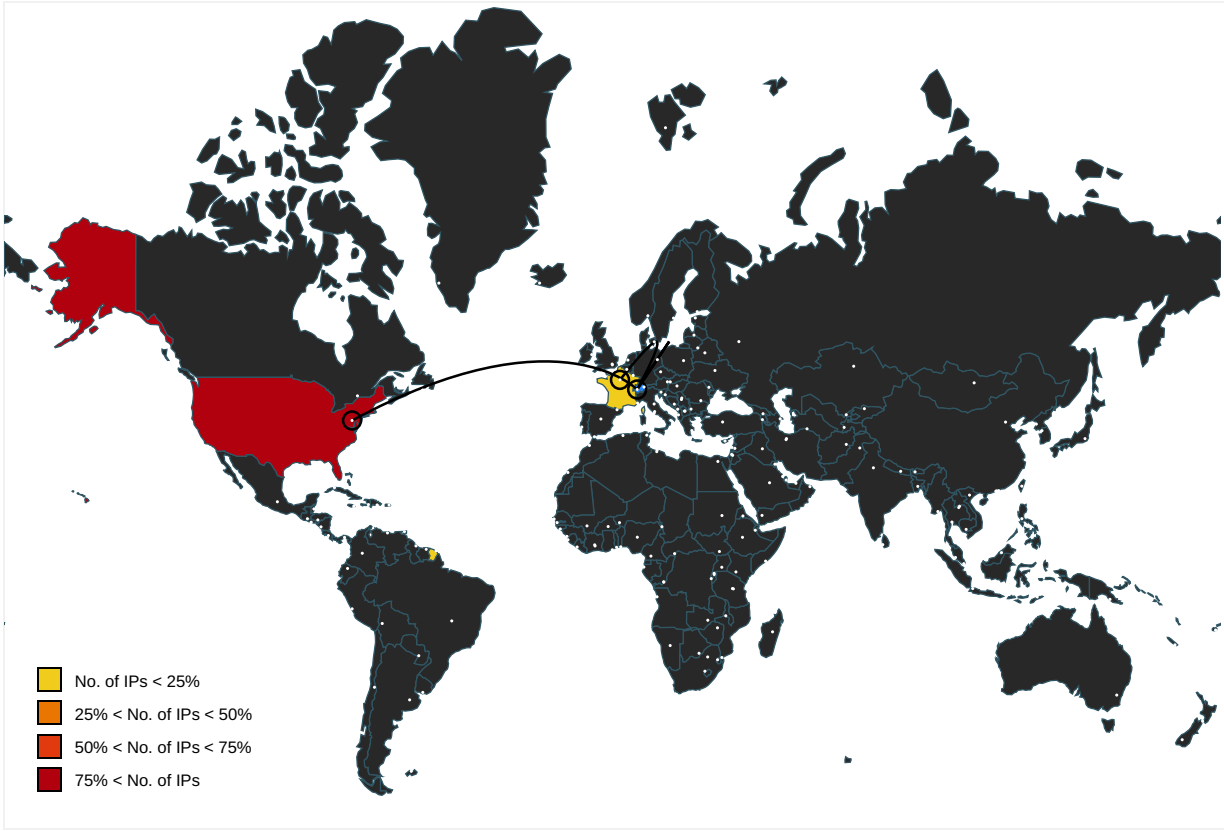
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.imagemagick.org	imagestore.dat.3.dr	false		high
http://https://bugs.webkit.org/show_bug.cgi?id=136851	jquery-3.3.1[1].js.3.dr	false		high
http://https://secure-excel-file.glitch.me/.Sign	~DF393BF7B86FA4A2BC.TMP.2.dr	false		high
http://jquery.org/license	jquery-3.3.1[1].js.3.dr	false		high
http://https://secure-excel-fl.O365.securefilep	{7E9128FA-3101-11EB-ADCF-ECF4BBB5915B}.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://jsperf.com/thor-indexof-vs-for/5	jquery-3.3.1[1].js.3.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://linktr.ee/excel.O365.securefile6Excel	~DF393BF7B86FA4A2BC.TMP.2.dr	false		high
http://https://bugs.jquery.com/ticket/12359	jquery-3.3.1[1].js.3.dr	false		high
http://https://code.jquery.com/jquery-3.2.1.slim.min.js	07D9KDVU.htm.3.dr	false		high
http://https://d1fdloi71mui9q.cloudfront.net/YS99cwPS1yJGdXcJU31Y_62xa7aqirVCeh6yn);background-image:url(ht	excel.O365[1].htm.3.dr	false		high
http://https://linktr.ee/excel.O365.securefileRoot	{7E9128FA-3101-11EB-ADCF-ECF4BBB5915B}.dat.2.dr	false		high
http://https://secure-excel-file.glitch.me/	~DF393BF7B86FA4A2BC.TMP.2.dr	false	• 100%, UrlScan, Browse	high
http://https://web.archive.org/web/20100324014747/blindsignals.com/index.php/2009/07/jquery-delay/	jquery-3.3.1[1].js.3.dr	false		high
http://https://html.spec.whatwg.org/#strip-and-collapse-whitespace	jquery-3.3.1[1].js.3.dr	false		high
http://https://promisesaplus.com/#point-75	jquery-3.3.1[1].js.3.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://web.archive.org/web/20141116233347/fluidproject.org/blog/2008/01/09/getting-setting-a	jquery-3.3.1[1].js.3.dr	false		high
http://https://fontawesome.comhttps://fontawesome.comFont	free-fa-regular-400[1].eot.3.dr, free-fa-solid-900[1].eot.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://drafts.csswg.org/cssom/#common-serializing-idioms	jquery-3.3.1[1].js.3.dr	false		high
http://https://html.spec.whatwg.org/multipage/forms.html#concept-fe-disabled	jquery-3.3.1[1].js.3.dr	false		high
http://https://bugs.webkit.org/show_bug.cgi?id=29084	jquery-3.3.1[1].js.3.dr	false		high
http://https://fontawesome.com/license/free	free.min[1].css.3.dr	false		high
http://https://infra.spec.whatwg.org/#strip-and-collapse-ascii-whitespace	jquery-3.3.1[1].js.3.dr	false		high
http://https://fontawesome.com	free-fa-regular-400[1].eot.3.dr, free.min[1].css.3.dr	false		high
http://https://github.com/eslint/eslint/issues/6125	jquery-3.3.1[1].js.3.dr	false		high
http://https://html.spec.whatwg.org/multipage/forms.html#concept-option-disabled	jquery-3.3.1[1].js.3.dr	false		high
http://https://github.com/jquery/jquery/pull/557)	jquery-3.3.1[1].js.3.dr	false		high
http://https://github.com/twbs/bootstrap/graphs/contributors)	bootstrap.min[1].js.3.dr	false		high
http://https://bugs.chromium.org/p/chromium/issues/detail?id=378607	jquery-3.3.1[1].js.3.dr	false		high
http://https://github.com/jrburke/requirejs/wiki/Updating-existing-libraries#wiki-anon	jquery-3.3.1[1].js.3.dr	false		high
http://https://bugzilla.mozilla.org/show_bug.cgi?id=687787	jquery-3.3.1[1].js.3.dr	false		high
http://https://bugs.chromium.org/p/chromium/issues/detail?id=470258	jquery-3.3.1[1].js.3.dr	false		high
http://opensource.org/licenses/MIT).	popper.min[1].js.3.dr	false		high
http://https://bugs.jquery.com/ticket/13378	jquery-3.3.1[1].js.3.dr	false		high
http://https://kit.fontawesome.com/585b051251.js	07D9KDVU.htm.3.dr	false		high
http://https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/js/bootstrap.min.js	07D9KDVU.htm.3.dr	false		high
http://https://promisesaplus.com/#point-64	jquery-3.3.1[1].js.3.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://cnhind-onmicrosoft-com.ml/email.php	07D9KDVU.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://promisesaplus.com/#point-61	jquery-3.3.1[1].js.3.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.3.dr	false		high
http://https://outlook.office365.com/owa/&resource=00000002-0000-0ff1-ce00-000000000000&response_mode=form_	07D9KDVU.htm.3.dr	false		high
http://https://bugs.chromium.org/p/chromium/issues/detail?id=589347	jquery-3.3.1[1].js.3.dr	false		high
http://https://code.jquery.com/jquery-3.1.1.min.js	07D9KDVU.htm.3.dr	false		high
http://https://html.spec.whatwg.org/multipage/syntax.html#attributes-2	jquery-3.3.1[1].js.3.dr	false		high
http://https://linktr.ee/excel.O365.securefilep	~DF393BF7B86FA4A2BC.TMP.2.dr	false		high
http://https://promisesaplus.com/#point-59	jquery-3.3.1[1].js.3.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.3.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://promisesaplus.com/#point-57	jquery-3.3.1[1].js.3.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.3.dr	false		high
http://https://promisesaplus.com/#point-54	jquery-3.3.1[1].js.3.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://code.jquery.com/jquery-3.3.1.js	07D9KDVU.htm.3.dr	false		high
http://https://linktr.ee/excel.O365.securefile6Excelile.glitch.me/eRoot	{7E9128FA-3101-11EB-ADCF-ECF4BBB5915B}.dat.2.dr	false		high
http://https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/css/bootstrap.min.css	07D9KDVU.htm.3.dr	false		high
http://https://linktr.ee/static/favicon.png.	imagestore.dat.3.dr	false		high
http://https://www.ilo.org/actemp/publications/WCMS_740375/lang--en/index.htm	07D9KDVU.htm.3.dr	false		high
http://https://secure.aadcdn.microsoftonline-p.com/ests/2.1.8576.13/content/images/microsoft_logo_ee5c8d9fb	07D9KDVU.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://html.spec.whatwg.org/multipage/forms.html#category-listed	jquery-3.3.1[1].js.3.dr	false		high
http://https://html.spec.whatwg.org/multipage/scripting.html#selector-disabled	jquery-3.3.1[1].js.3.dr	false		high
http://https://developer.mozilla.org/en-US/docs/CSS/display	jquery-3.3.1[1].js.3.dr	false		high
http://https://www.office.com/?auth=2	07D9KDVU.htm.3.dr	false		high
http://https://jquery.org/license	jquery-3.3.1[1].js.3.dr	false		high
http://https://bid.g.doubleclick.net/xbbe/pixel?d=KAE	f[1].txt.3.dr	false		high
http://https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.12.9/umd/popper.min.js	07D9KDVU.htm.3.dr	false		high
http://https://jquery.com/	jquery-3.3.1[1].js.3.dr	false		high
http://https://getbootstrap.com)	bootstrap.min[1].css.3.dr, bootstrap.min[1].js.3.dr	false	• Avira URL Cloud: safe	low
http://https://linktr.ee/excel.O365.securefile	~DF393BF7B86FA4A2BC.TMP.2.dr	false		high
http://https://bugs.webkit.org/show_bug.cgi?id=137337	jquery-3.3.1[1].js.3.dr	false		high
http://https://html.spec.whatwg.org/multipage/scripting.html#selector-enabled	jquery-3.3.1[1].js.3.dr	false		high
http://https://linktr.ee/excel.O365.securefile6ExcelRoot	{7E9128FA-3101-11EB-ADCF-ECF4BBB5915B}.dat.2.dr	false		high
http://https://github.com/twbs/bootstrap/blob/master/LICENSE)	bootstrap.min[1].css.3.dr, bootstrap.min[1].js.3.dr	false		high
http://https://promisesaplus.com/#point-48	jquery-3.3.1[1].js.3.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://logo.clearbit.com/	07D9KDVU.htm.3.dr	false		high
http://https://github.com/jquery/sizzle/pull/225	jquery-3.3.1[1].js.3.dr	false		high
http://https://i.ibb.co/crr44kK/bg5.png	07D9KDVU.htm.3.dr	false		high
http://https://sizzlejs.com/	jquery-3.3.1[1].js.3.dr	false		high
http://https://bugs.chromium.org/p/chromium/issues/detail?id=449857	jquery-3.3.1[1].js.3.dr	false		high
http://https://secure-excel-file.glitch.me/ed	~DF393BF7B86FA4A2BC.TMP.2.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
151.101.130.133	unknown	United States		54113	FASTLYUS	false
172.217.168.2	unknown	United States		15169	GOOGLEUS	false
143.204.214.108	unknown	United States		16509	AMAZON-02US	false
50.87.153.159	unknown	United States		46606	UNIFIEDLAYER-AS-1US	false
52.205.236.122	unknown	United States		14618	AMAZON-AESUS	false
104.16.19.94	unknown	United States		13335	CLOUDFLARENETUS	false
145.239.131.55	unknown	France		16276	OVHFR	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	323781
Start date:	27.11.2020
Start time:	14:38:59
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 56s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Direct Deposit.xlsx
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	6
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:	• EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default

Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal60.phis.winXLSX@4/67@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): dllhost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 104.108.39.131, 192.35.177.64, 8.253.204.249, 8.241.121.126, 8.248.123.254, 8.241.122.254, 8.248.119.254, 8.241.123.254, 67.26.81.254, 8.248.117.254, 8.241.122.126, 8.248.121.254, 2.20.142.210, 2.20.142.209, 142.250.74.200, 216.58.215.234, 172.217.168.3, 13.107.13.80, 204.79.197.200, 13.107.21.200, 152.199.19.161, 209.197.3.24, 172.217.168.74, 104.18.23.52, 104.18.22.52, 209.197.3.15, 92.122.39.6, 172.64.203.28, 172.64.202.28 • Excluded domains from analysis (whitelisted): gstaticadssl.l.google.com, au.download.windowsupdate.com.edgesuite.net, cds.s5x3j6q5.hwcdn.net, www.googleadservices.com, ka-f.fontawesome.com.cdn.cloudflare.net, api.bing.com, afd.e-0001.dc-msedge.net, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, go.microsoft.com, www.googletagmanager.com, audownload.windowsupdate.nsatc.net, www-bing-com.dual-a-0001.a-msedge.net, e13761.dscg.akamaiedge.net, auto.au.download.windowsupdate.com.c.footprint.net, apps.identrust.com, au-bg-shim.trafficmanager.net, api-bing-com.e-0001.e-msedge.net, www.bing.com, kit.fontawesome.com.cdn.cloudflare.net, e-0001.dc-msedge.net, fonts.googleapis.com, fonts.gstatic.com, dual-a-0001.a-msedge.net, ie9comview.vo.msecnd.net, ajax.googleapis.com, www-googletagmanager.l.google.com, secure.aadcdn.microsoftonline-p.com.edgekey.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, r20swj13mr.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, go.microsoft.com.edgekey.net, apps.digsigtrust.com, cds.j3z9t3p6.hwcdn.net, cs9.wpc.v0cdn.net • Report size getting too big, too many NtDeviceIoControlFile calls found. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/323781/sample/Direct Deposit.xlsx

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
50.87.153.159	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-2F2sJcIWacwxf41PdlItZuKCDTDX9lriBog1LoLAGz59LzA-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/CO72216191330692354O1.zip	Get hash	malicious	Browse	• jeevanmate.com/assets/plugins/bootstrap-modal/img/_vti_cnf/CO722161913306923540 1.zip
151.101.130.133	http://https://app.meltwater.com/mwTransition/?url=https%3A%2F%2Fforums.iboats.com%2Fforum%2Fboat-repair-and-restoration%2Fboat-restoration-building-and-hull-repair%2F10917787-infinity-vinyl-flooring-in-a-fishing-boat%23post&uId=5b9934f7dfbe5b981627d919&cId=596d7295a0d48bc5096c9e6d&contextId=5f3a72f0b5a6bb31da4ff476&dId=1597616400000_3F3zZkGhPGTEsGaWZ39EP6n9_n0&op=open&sentiment=N&isHosted=false&id=2745345&name=Crestliner%20%7C%20Social&type=search&transitionToken=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzUxMiJ9.eyJob3N0bmFtZSI6ImZvcnVtcy5pYm9hdHMuY29tIn0._HbwDOuxTMFMyn78c3KoKrcNlQtWEWgNmfHWFvyDrFI1dARgoBKEa75qJIVu3p4FH2Orr5dgnLoglj3m2Z6PgQ&s=mail-digest	Get hash	malicious	Browse	
	http://https://forums.iboats.com/forum/engine-repair-and-maintenance/mercruiser-i-o-inboard-engines-outdrives/591523-mercruiser-3-0l-drive-lube-refill	Get hash	malicious	Browse	
	.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
172.217.168.2	http://inbox.lv	Get hash	malicious	Browse	• www.googletagservices.com/tag/js/gpt.js
	http://trip-suggest.com/fiji/northern/urata/	Get hash	malicious	Browse	• pagead2.googlesyndication.com/pagead/js/r20180613/r20180604/show_ads_impl.js
	http://ak.imgfarm.com/images/nocache/vicinio/installers/v2/223906514.TTAB02.1/nsis/866449-TTAB02.1/180517185905058/msniEverydayLookup/EverydayLookup.84b303f4de8f4dbeb7d827720e672a45.exe	Get hash	malicious	Browse	• googleads.g.doubleclick.net/pagead/viewthroughconversion/953497956/?value=1.00&currency_code=USD&label=QDfJCOfQg2gQ5PLUxgM&guid=ON&script=0&ctc_id=CAIVAgAAAB0CAAAA&ct_cookie_present=false&ocp_id=Is-HXOa3E4K03gOX0ZLADg&random=1835501294&crd=CMnTGw&gtd=

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://gYPuB_e9W-TmH/yw/Attachments/02_19	Get hash	malicious	Browse	• cm.g.doubleclick.net/pixel?google_nid=adspend&google_cm=&google_hm=5c79457387bae07121c723eb&r=%2F%2Fx01.aidata.io%2F0.gif%3Fpid%3D6472613%26id%3D5c79457387bae07121c723eb%26dest%3D%252F%252Fdmg.digitaltarget.ru%252F1%252F224%252Fi%252Fi%253Fa%253D224%2526e%253D5c79457387bae07121c723eb%2526i%253D20638329125589843 14%2526r%253D%25252F%25252F%25252Fsync.1dmp.io%25252Fpixel.gif%25253Fcid%25253Dfe2375b0-c617-4a6d-ab2d-f9f457ba8100%252526pid%25253Dw%252526uid%25253D5c79457387bae07121c723eb%252526ru%25253D%25252F%25252F%25252Fmc.yandex.ru%25252Fwatch%2525252F45493809%2525253Fas-user%25252525A5c79457387bae07121c723eb&google_tc=
	http://https://urldefense.proofpoint.com/v2/url?u=https-3A__www.e-2Daccess.att.com_abgmas-5Fn_imail_dispatcher-3Faction-3Dsm.unsub-26ct-5Fid-3Dd93e425c959f38a0&d=DwIFAg&c=euGZstcaTDllvimEN8b7jXrwqOf-v5A_CdpgnVfiiMM&r=kOsMS0a61_b_h_foqF1756MSq9w7uqLN5RrsselaQRw&m=VPCss2mfVShNnAVlrIqRm_TqySIhsdqag9KaqHu8cck&s=fhmt5ahwQfahtpQ-YaFUMzShnT6eRLEPWgq7AQHbt18&e	Get hash	malicious	Browse	• googleads.g.doubleclick.net/pagead/viewthroughconversion/1070858700/?value=0&guid=ON&script=0
143.204.214.108	http://https://www.evernote.com/shard/s511/sh/84baa11f-b2e0-4201-9af2-705098f1cea4/e87339f9e3ffcc585b3eb5dd45076f92	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ibuykenya.com	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
pagead.l.doubleclick.net	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
	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
	http://https://www.canva.com/design/DAEOEcu9Gnc/C6LvqPRfMOYoF6OWlu9bVg/view?utm_content=DAEOEcu9Gnc&utm_campaign=designshare&utm_medium=link&utm_source=sharebutton	Get hash	malicious	Browse	• 216.58.205.226
cdnjs.cloudflare.com	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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-2BsRItFMcwpTA18DVdBlGBJyUhFuIaAEybVNgKjH795y-2Bjn2esAEGPPa76dl-2BxD62wo4xT0BtNrFdVu0eWgx-2F6eRqupI7yZWQAa-2FBr1dlsLgX0hlcDSdDmAHsaZaG3WUUyADLR7thqFcU32Djt0AEfQ9qS0428-2BH1u-2Fk1E3KVFo9IePxc9mOWOHzwBkFv-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
	http://https://www.canva.com/design/DAEObyDZ7GY/6ub0uSCO4OtxCxpRjJZrYg/view	Get hash	malicious	Browse	• 104.16.19.94

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
GOOGLEUS	http://https://is.gd/NLY8Sb	Get hash	malicious	Browse	• 74.125.128.156
	REQUEST FOR BID 26-11-2020.ppt	Get hash	malicious	Browse	• 172.217.168.1
	http://https://offiubtj7banjz48zrg8d4nz2ns9.web.app/?c=brynjar.t.gudmundsson@landsbanki.is	Get hash	malicious	Browse	• 216.58.215.244
	http://https://docs.google.com/forms/d/e/1FAIpQLScMM9oeboGCqCY9IhNTWcPfX75sr8KJDxUhz1WOhVNCro9dgQ/viewform	Get hash	malicious	Browse	• 74.125.128.155
	http://https://erabansoupala.blogspot.com//?m=0	Get hash	malicious	Browse	• 172.217.168.1
	http://https://mincast.us-south.cf.appdomain.cloud/redirect/?email=prampon@soteb.fr	Get hash	malicious	Browse	• 74.125.128.155
	MAL.PPT	Get hash	malicious	Browse	• 172.217.168.2

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://event.apiv9.com/	Get hash	malicious	Browse	• 35.205.61.67
	http://https://bit.do/fLppr	Get hash	malicious	Browse	• 74.125.128.155
	Exodus.exe	Get hash	malicious	Browse	• 216.239.34.21
	http://https://bit.ly/3kUgQ0H	Get hash	malicious	Browse	• 172.217.168.34
	P. I.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	http://https://ptfsca-my.sharepoint.com/:b:/g/personal/kevin_ptfs_ca/EboJWCmd9RVCrP7-u8pvAqYBYBaOrLxrf1qbZLFVjshCAA?e=4%3aaaD17Q&at=9	Get hash	malicious	Browse	• 216.58.215.225
	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	• 172.217.168.20
	http://45.146.165.216	Get hash	malicious	Browse	• 172.217.22.98
	Shipping INVOICE-BL Shipment..exe	Get hash	malicious	Browse	• 34.102.136.180
	2zv940v7.dll	Get hash	malicious	Browse	• 216.58.215.225
	zojNE48815.apk	Get hash	malicious	Browse	• 8.8.4.4
	ANGEBOTXANFORDERNXXXXXXXXX26-11-2020.ppt	Get hash	malicious	Browse	• 172.217.168.1
	http://nity.midlidl.com/index	Get hash	malicious	Browse	• 216.58.206.1
UNIFIEDLAYER-AS-1US	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	document-1616029928.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
AMAZON-02US	http://https://is.gd/NLY8Sb	Get hash	malicious	Browse	• 99.86.2.22
	DHL_Nov 2020 at 1.85_8BZ290_PDF.jar	Get hash	malicious	Browse	• 54.190.165.96
	DHL_Nov 2020 at 1.85_8BZ290_PDF.jar	Get hash	malicious	Browse	• 54.190.165.96
	http://https://34.75.2o2.lol/XYWNc0aW9uPWwNsaWNrJngVybD1ovndHRwnczovL3NleY3wVyZWQtbG9naW4ubmV0nL3BhZ2VzLzQyY2FkNTJhZmU3YSZyZWNpcGllbnRfaWQ9NzM2OTg3ODg4JmNhbXBhaWduX3J1bl9pZD0zOTM3OTcz	Get hash	malicious	Browse	• 52.216.164.5
	http://https://bit.do/fLppr	Get hash	malicious	Browse	• 52.210.2.133
	http://https://rb.gy/flx7ju	Get hash	malicious	Browse	• 13.248.219.100
	Shipping documents.xlsx	Get hash	malicious	Browse	• 52.58.78.16
	PO_0012009.xlsx	Get hash	malicious	Browse	• 99.79.190.44
	paperport_3753638839.exe	Get hash	malicious	Browse	• 13.224.89.193
	opzi0n1[1].dll	Get hash	malicious	Browse	• 13.224.89.96
	http://email.balluun.com/ls/click?upn=0tHwWGqJA7fIfwq261XQPoa-2Bm5KwDIa4k7cEZI4W-2FdMZ1Q80M51jA5s51EdYNFwUO080OaXBwsUkIwQ6bL8cCo1cNcDJzlw2uVCKEfhUzZ7Fudhp6bkdbJB13EqLH9-2B4kEnaIsd7WRusADisZIU-2FqT0gWvSPQ-2BUMBeGniMV23Qog3fOaT300-2Fv2T0mA5uuaLf6MwKyAEEDv4vRU3MHAWtQ-3D-3DaUdf_BEBGVEU6IBswk46BP-2FJGpTLX-2FIf4Ner2WBFJyc5PmXI5kSwVWq-2FIninIJmDnNhUsSuO8YJPXc32diFLFly8-2FlazGQr8nbzBIO-2BSvdfUqJySNySwNZh5-2F7tiFSU4CooXZWp-2FjpdCX-2Fz89pGPVGN3nhMItFmIBBYMcjwlGWZ8vS3fpyiPHr-2BxekPNfR4Lq-2Baznil07vpcMoEZofdPQTnqnmg-3D-3D	Get hash	malicious	Browse	• 34.209.19.120
	http://searchlf.com	Get hash	malicious	Browse	• 13.224.93.71
	http://https://pembina.sharepoint.com/teams/BOandP/_layouts/15/guestaccess.aspx?share=Ev8UHcgPkQRPnPpDIa8PTeUBDnUZj2epg0IcLzD6O0XQNQ&e=5:GyiSQ3&at=9	Get hash	malicious	Browse	• 13.224.93.10
	http://https://tenderdocsrfp.typeform.com/to/RVzhstxV	Get hash	malicious	Browse	• 52.33.248.165
	http://https://www.canva.com/design/DAEOhhihuRE/ilbmdiYYv4SZabsnRUealQ/view?utm_content=DAEOhhihuRE&utm_campaign=designshare&utm_medium=link&utm_source=sharebutton	Get hash	malicious	Browse	• 44.236.72.93
	http://https://omgzone.co.uk/	Get hash	malicious	Browse	• 13.224.93.77
	http://https://doc.clickup.com/p/h/84zph-7/c3996c24fc61b45	Get hash	malicious	Browse	• 54.77.92.238
	http://t.comms.officeworks.com.au/r/?id=hb22c4478,920a576c,91374a10&p1=developerhazrat.com/p13p13yu13/bGVnYWxpbnRAc2VhcnNoYy5jb20=%23#c13c13v13h13h13u13l13j13m##	Get hash	malicious	Browse	• 18.136.188.28
	http://email.balluun.com/ls/click?upn=KzNQqcw6vAwizrX-2Fig1Ls6Y5D9N6j9I5FZfBCN8B2wRxBmpXcbUQvKOFUzJGiw-2F3Qy64T8VZ2LXT8NNNJG9bemh7vjcLDgF5-2FXPBBBqdJ0-2BpvIlXlKrZECAirL9YySN2b1LT-2Bcy1l-2F0fp1Pwvv3l4j7XHHKagv-2FxlVdd85P38ZuA-2Bvv5JF3QaAOx19sqG0-2BnULpm_J-2BsRItFMcwpTA18DVdBlGBJyUhFuIaAEybVNgKjH795y-2Bjn2esAEGPPa76dl-2BxD62wo4xT0BtNrFdVu0eWgx-2F6eRqupI7yZWQAa-2FBr1dlsLgX0hlcDSdDmAHsaZaG3WUUyADLR7thqFcU32Djt0AEfQ9qS0428-2BH1u-2Fk1E3KVFo9IePxc9mOWOHzwBkFv-2FOdeNUShdwqtjGBw2zuSNSTyLDRcypBOMpUtPdiR8ihMQ0-3D	Get hash	malicious	Browse	• 34.209.19.120
	http://https://epl.paypal-communication.com/H/2/v600000175fc9567aec3e4496e965fc958/d07dcaec-c38a-4069-96dc-06e53581f535/HTML	Get hash	malicious	Browse	• 13.224.93.119
FASTLYUS	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
	lzezma64.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
	tjbdhdvi1.zip.dll	Get hash	malicious	Browse	• 151.101.1.44

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
7dcce5b76c8b17472d024758970a406b	document-1696372388.xls	Get hash	malicious	Browse	• 151.101.130.133 • 172.217.168.2 • 143.204.214.108 • 52.205.236.122 • 104.16.19.94 • 145.239.131.55
	document-1627527350.xls	Get hash	malicious	Browse	• 151.101.130.133 • 172.217.168.2 • 143.204.214.108 • 52.205.236.122 • 104.16.19.94 • 145.239.131.55
	document-1585328522.xls	Get hash	malicious	Browse	• 151.101.130.133 • 172.217.168.2 • 143.204.214.108 • 52.205.236.122 • 104.16.19.94 • 145.239.131.55
	document-1728077580.xls	Get hash	malicious	Browse	• 151.101.130.133 • 172.217.168.2 • 143.204.214.108 • 52.205.236.122 • 104.16.19.94 • 145.239.131.55
	document-163667458.xls	Get hash	malicious	Browse	• 151.101.130.133 • 172.217.168.2 • 143.204.214.108 • 52.205.236.122 • 104.16.19.94 • 145.239.131.55
	document-1482657082.xls	Get hash	malicious	Browse	• 151.101.130.133 • 172.217.168.2 • 143.204.214.108 • 52.205.236.122 • 104.16.19.94 • 145.239.131.55
	document-1566598693.xls	Get hash	malicious	Browse	• 151.101.130.133 • 172.217.168.2 • 143.204.214.108 • 52.205.236.122 • 104.16.19.94 • 145.239.131.55

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	document-1653694473.xls	Get hash	malicious	Browse	• 151.101.13 0.133 • 172.217.168.2 • 143.204.21 4.108 • 52.205.236.122 • 104.16.19.94 • 145.239.131.55
	document-1584353867.xls	Get hash	malicious	Browse	• 151.101.13 0.133 • 172.217.168.2 • 143.204.21 4.108 • 52.205.236.122 • 104.16.19.94 • 145.239.131.55
	document-1603010935.xls	Get hash	malicious	Browse	• 151.101.13 0.133 • 172.217.168.2 • 143.204.21 4.108 • 52.205.236.122 • 104.16.19.94 • 145.239.131.55
	document-1596402252.xls	Get hash	malicious	Browse	• 151.101.13 0.133 • 172.217.168.2 • 143.204.21 4.108 • 52.205.236.122 • 104.16.19.94 • 145.239.131.55
	document-1565130283.xls	Get hash	malicious	Browse	• 151.101.13 0.133 • 172.217.168.2 • 143.204.21 4.108 • 52.205.236.122 • 104.16.19.94 • 145.239.131.55
	document-1595476859.xls	Get hash	malicious	Browse	• 151.101.13 0.133 • 172.217.168.2 • 143.204.21 4.108 • 52.205.236.122 • 104.16.19.94 • 145.239.131.55
	document-1714791743.xls	Get hash	malicious	Browse	• 151.101.13 0.133 • 172.217.168.2 • 143.204.21 4.108 • 52.205.236.122 • 104.16.19.94 • 145.239.131.55
	REQUEST FOR BID 26-11-2020.ppt	Get hash	malicious	Browse	• 151.101.13 0.133 • 172.217.168.2 • 143.204.21 4.108 • 52.205.236.122 • 104.16.19.94 • 145.239.131.55
	INV-FATURA010009.xlsx	Get hash	malicious	Browse	• 151.101.13 0.133 • 172.217.168.2 • 143.204.21 4.108 • 52.205.236.122 • 104.16.19.94 • 145.239.131.55
	INV-FATURA010009.xlsx	Get hash	malicious	Browse	• 151.101.13 0.133 • 172.217.168.2 • 143.204.21 4.108 • 52.205.236.122 • 104.16.19.94 • 145.239.131.55

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	document-1599331256.xls	Get hash	malicious	Browse	• 151.101.13 0.133 • 172.217.168.2 • 143.204.21 4.108 • 52.205.236.122 • 104.16.19.94 • 145.239.131.55
	document-154799845.xls	Get hash	malicious	Browse	• 151.101.13 0.133 • 172.217.168.2 • 143.204.21 4.108 • 52.205.236.122 • 104.16.19.94 • 145.239.131.55
	document-1745297819.xls	Get hash	malicious	Browse	• 151.101.13 0.133 • 172.217.168.2 • 143.204.21 4.108 • 52.205.236.122 • 104.16.19.94 • 145.239.131.55

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Microsoft Cabinet archive data, 58936 bytes, 1 file
Category:	dropped
Size (bytes):	117872
Entropy (8bit):	**7.994797855729196**
Encrypted:	**true**
SSDEEP:	1536:i/LAvEZrGclx0hoW6qCLdNz2p+/LAvEZrGclx0hoW6qCLdNz2pj:UcMqZVCp8pwcMqZVCp8pj
MD5:	DB381E85D86EA4484D20078E9EC667A6
SHA1:	4871FDAF0C2EEC8183FC3CE7710B18FD3C647CEA
SHA-256:	C3520E3A6EB43F6D416852C454414C5D7823A96FB9070BC30301ADDEBB334D4D
SHA-512:	D9E03A617D1D9505D3ADA3C41FC8A53504F4F1C44F92AF00869F2FE150D6677FD4450E85EB1E3D920D32BA01F190E7F14BF130F8CC69EB47D834CCE43CAA765 0
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	MSCF....8.....,.....I.....S.....LQ.v .authroot.stl..0(/.5..CK..8T....c_.d...:.(.....].M$[v.4CH)-.%.QIR..$t)Kd...D.....3.n..u.....|..=H4.U=...X..qn.+S..^J.....y.n.v.XC... 3a.!.....]...c(...p..]..M.....4.....i...}C.@.[..#xUU..*D..agaV..2.|.g...Y..j.^..@.Q.....n7R...`.../..s...f...+...c..9+[.|0.'..2!.s....a.....w.t:..L!.s....`.O>.`#..'.pfi7.U.....s..^...wz.A.g.Y.... ....g.....:7{.O.....N.....C..?....P0$.Y..?m....Z0.g3.>W0&.y](....].`>... ..R.qB..f.....y.cEB.V=.....hy}....t6b.q./~.p.....60...eCS4.o.....d..}.<,nh..;.....)....e..\|....Cxj...f.8.Z..&..G..... ..b.....OGQ.V..q..Y.....q...0..V.Tu?.Z..r...J...>R.ZsQ...dn.0.<...o.K....\|.....Q...'....X..C.....a;.*..Nq..x.b4..1,}.'.....z.N.N...Uf.q'.>}.....o\.cD"0.'.Y.....SV..g...Y.....o.=.....k..u. .s.kV?@....M...S.n^.:G.....U.e.v..>...q.'..$.)3..T...r.!.m.....6...r,lH.B <.ht..8.s..u[.N.dL.%...q....g..;T..l..5...\.....g...`...........A$:.....

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\E0F5C59F9FA661F6F4C50B87FEF3A15A	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	1786
Entropy (8bit):	7.366016576663508
Encrypted:	false
SSDEEP:	48:3ntmD5QQD5XC5RqHHXmXvp++hntmD5QQD5XC5RqHHXmXvp++x:3AJ8RAXmXvcOAJ8RAXmXvcu
MD5:	6AEB4E76C6F68EFD7A48092E9F0F3492
SHA1:	823A035C0BDCC3DC09C881E788F7FACA53C6B458
SHA-256:	FE1B9A0EABF44FDBE4DDE97C3CC1209FAD2FBB2D2D7476FFBF64066BD9919A4F
SHA-512:	50D98FB4C9875B1AED0AEC06A9C934DB5010B6C5F54539E323EC14FD487E1D92D01652E4614DDF308AB2F1EDEA9E9CB1E23030C971255CC106016C6E7BBAF4 C
Malicious:	false
Reputation:	moderate, very likely benign file

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\E0F5C59F9FA661F6F4C50B87FEF3A15A	
Preview:	0..y..*.H.....j0..f...1.0...*.H.....N0..J0..2.....D....'..09...@k0...*.H.....0?1$0"..U....Digital Signature Trust Co.1.0...U....DST Root CA X30...0009302112 19Z..210930 140115Z0?1$0"..U....Digital Signature Trust Co.1.0...U....DST Root CA X30.."0...*.H.....0.....P..W..be.....,k0.[...}.@.....3vI*.?!I..N..>H.e...!.e.*.2....w..{.....s.z..2..~ ..0....*8.y.1.P..e.Qc...a.Ka..Rk...K.(.H.....>.... .[.*....p....%.tr.{j.4.0...h.{T....Z...=d.....Ap..r.&.8U9C....\@.....%.....:..n.>..\..<.i....*.)W..=....].....B0@0...U.....0....0...U..... ....0...U.....{.q...K.u...`...0...*.H.....,...\...(f7:...?K.... ]..YD.>.>..K.t.....t..~.....K. D....}..j.....N..:.pl.....:^H...X._..Z.....Y..n.....f3.Y[...sG.+..7H..VK....r2...D.SrmC.&H.Rg. X..gvqx...V..9$1....Z0G..P.....dc`.....}...=2.e..|.Wv..(9..e...w.j..w.....)...55.1.0..y..*.H.....j0..f...1.0...*.H.....N0..J0..2.....D....'..09...@k0...*.H.....0?1$0"..U....Dig

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.11930763095091
Encrypted:	false
SSDEEP:	12:8WkPlE99SNxAhUegeT9kPlE99SNxAhUegeT2:nkPcUQU769kPcUQU762
MD5:	8FD1AA3D3E08F810B87B96EE42390CFC
SHA1:	E07FCA2E3F4B0DA31659BA8EDCC2F044246C49E9
SHA-256:	1510721DDB4CEA3B4FADE892CA1F5A5835B71FBC35A127CB4FF369A4E2D280BA
SHA-512:	39478660E5B64984D6F03503C49C6D86417EC489DDCA5D08EE8172A231277E1276D300A790F6399D2B82EC4E30F791FD40ED0BC5099EE8AC26F056AF4D882EE
Malicious:	false
Reputation:	low
Preview:	p..... .....@[B....(..... .....Y.....$.....8...h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s .t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.6.9.5.5.9.e.2.a.0.d.6.1.:.0."...p..... .....lB....(..... .....Y.....$.....8...h.t.t.p.:. /./.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.6.9.5.5.9.e.2.a.0.d.6.1.:.0."...

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\E0F5C59F9FA661F6F4C50B87FEF3A15A	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	504
Entropy (8bit):	3.0197480023253434
Encrypted:	false
SSDEEP:	6:kKfliBAIdQZV7eAYLiWK/T3liBAIdQZV7eAYLit:3lidKO6T3lidKOe
MD5:	71ECC2F250B120F2E591F9516ECF5D5E
SHA1:	5FA05787DD504E6D3BBE6B25949F596C504D7D66
SHA-256:	E7453A9448314C03DCB3431DD2A19E49B3F90FE9A6684E8EC9E93E52872F40F1
SHA-512:	D3C31C80D324B08E981E653532D22D202A6B0EE13E49230EE2D2A01FBB01FF170B8A4ECAD43FD9979F130917EC408C46CFAE62FB56534B8D344FDD862F5AE5 9
Malicious:	false
Reputation:	low
Preview:	p..... ....`....+-B....(..... .....u.....(.....}...h.t.t.p.:././.a.p.p.s...i.d.e.n.t.r.u.s.t...c.o.m./.r.o.o.t.s./.d.s.t.r.o.o.t.c.a.x.3...p.7.c...".3.7.d.-.5.9.e.7.6 .b.3.c.6.4.b.c.0."...p..... ....`...[..B....(..... .....u.....(.....}...h.t.t.p.:././.a.p.p.s...i.d.e.n.t.r.u.s.t...c.o.m./.r.o.o.t.s./.d.s.t.r.o.o.t.c.a.x.3...p.7.c. .."3.7.d.-.5.9.e.7.6.b.3.c.6.4.b.c.0."...

C:\Users\user\AppData\LocalLow\Microsoft\Internet Explorer\Services\search_{0633EE93-D776-472f-A0FF-E1416B8B2E3A}.ico	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 4-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	237
Entropy (8bit):	6.1480026084285395
Encrypted:	false
SSDEEP:	6:6v/lhPIF6R/C+u1fXNg1XQ3yslRtNO+cKvAElRApGCp:6v/7b/C1fm1ZslRTvAElR47
MD5:	9FB559A691078558E77D6848202F6541
SHA1:	EA13848D33C2C7F4F4BAA39348AEB1DBFAD3DF31
SHA-256:	6D8A01DC7647BC218D003B58FE04049E24A9359900B7E0CEBAE76EDF85B8B914
SHA-512:	0E08938568CD123BE8A20B87D9A3AAF5CB05249DE7F8286FF99D3FA35FC7AF7A9D9797DD6EFB6D1E722147DCFB74437DE520395234D0009D452FB96A8ECE23 B
Malicious:	false
Reputation:	high, very likely benign file
Preview:	.PNG.....IHDR.....R....sRGB.....gAMA.....a.....pHYs.....o.d...-PLTE.....(..5..X..h.....J4.I...IIDAT.[c`..&.(.....F....cX.(@.j.+@..K.(..2L....1.{.....c`]L 9.&2.I...I..E.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{7E9128F8-3101-11EB-ADCF-ECF4BBB5915B}.dat	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{7E9128F8-3101-11EB-ADCF-ECF4BBB5915B}.dat	
Size (bytes):	33368
Entropy (8bit):	1.864989891924485
Encrypted:	false
SSDEEP:	48:IvuGcpU7Gwp0uKG/apnu5drGIpHu5TQGvnZpEu5TFkvGoIVqpqu5TFwk+Go4Uc5Z:MyKVK/pi9JwaZ0Sx3jVjkaAS3
MD5:	5AD6516FF8A5095810C6B125EB4ED533
SHA1:	AA3E036DB54125EC37123ECCD65C19C07DD3AC11
SHA-256:	2BF484CC7472693B1634384C6B036C6B33DAF45DB82CEB85DF58610766238C70
SHA-512:	6E7FE61FB7BC8780CA6C499B9E99B7E7B505083924CC9D3C366B67388888021D63C3C3F732FCA2EC07FD8390BABBD30453660DE5A59DAC7349B87C666EBE1FD
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\{7E9128FA-3101-11EB-ADCF-ECF4BBB5915B}.dat	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	37792
Entropy (8bit):	1.9445020966375004
Encrypted:	false
SSDEEP:	192:MdXKWbeJ07uFcR3pRWkJR6zR9Y/7a07Iht740N7K3G71dhJC60xbF0FBOiRs:MEYKCuizHuzC/EHxZxt0kBOD
MD5:	CB438622373D31144D1666EF28CBA93E
SHA1:	649578FAAA3A8FC3A937A4D0E37A05BC01DCC845
SHA-256:	1B40D3037C4657122705604D0A52B3E910268124B46935C89C37080EE1452062
SHA-512:	418C374E0988B846368C691FA873D0A069F6036F57395949CCD255E887DD19865920E674E5CEDEF63D670FCAD2D21740E2531E2764C91D9CEC07CD53A1431FE
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\{94493AEE-3101-11EB-ADCF-ECF4BBB5915B}.dat	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5669672934425503
Encrypted:	false
SSDEEP:	48:IvGGcpUxGwpNQG4pPghGrapgSOxrGQpZkGWG7HpCnsTGIpG:MaKrbQJCeSuF/f0n4A
MD5:	DDAAB1CD3E4810DAFA6CA5BCD019D225
SHA1:	FB0A316FB7882B28F481EC6A006AFFA4F0A3EFA6
SHA-256:	4A14CA138515F76A470ACB7FBAE3C5AC9A0CF2333144B4043A8CBB0930C0BD9C
SHA-512:	5853859D68FFAE626FB1ADD86FF9860B388E6B94E09472C41D1BF22F1CD19710730B0230CE2CE61D9352A2232F55B337350DB526190FBB9C34403EBA13E7D4C9
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\lr5drzg\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:HtRkmavaCcpjlWTUzjEZLEMIT57DwPoQNAnDKlfXGA:HteUCmlnaE/7D4FNAnulfT
MD5:	74C0320B82593DB8ADBCAD8F8604E714
SHA1:	368A1B538D68D527946B5266D871CE5D8FE8B29C
SHA-256:	4A632D3FEFD8E0D41DDB1E8BFF2A9C3749D440CFED835A5E9DA0E8B19D83810C

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\lr5drzg\imagestore.dat	
SHA-512:	7ED3EDCA4A85CBDF3AEBA0E9D0E9F09C864387BD6C22AF73BFE1B1B43B42AB89EC0719570B4DC0536DC451A8F45C415D29F887E7F5909FB2132852F32884E7 2
Malicious:	false
Reputation:	low
Preview:	$.h.t.t.p.s.:././.l.i.n.k.t.r...e.e./.s.t.a.t.i.c./.f.a.v.i.c.o.n...p.n.g......PNG........IHDR.............(-.S....gAMA......a.....sRGB........ cHRM..z&..............u0...`..:....p..Q<....PLTE...9.9.9 .9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.....m[...4tRNS....F....{c..'.y..(..Z....@..I.......L..........u.L.@.....bKGD5..k....pHYs... H...H.F.k>....IDAT..e....P.C'.(([A)R..*...os..s..=.,BD.m.........`.u...K6......k.k.^...*0.fv]..*x.p....T.n..Q....x'..$.+..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\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\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+jjjjjjjjDhhhhv:fJzAqoDZZIKQEnhhhhv
MD5:	92D02EB7F5FF234BBC392920BD1D461E
SHA1:	583E1B2FDCD303E720F440401C5A5CC2ABA3880A
SHA-256:	2D83244F48AD4EE1CDD191C983C0468E168EE4BF2F6618794B4440120FE9A999
SHA-512:	F81A0AB5F28D9FB529B916E3669019571DB6ABCD9CD7ECBECD572510A1508E4FE711D753ACEA92E684D5282B55963C39C89E211661885B38EC01F3699E4D3D/ 2
Malicious:	false
Reputation:	low
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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz...?..........x... ...k.@.....k.....Q.G.....B..v.A.p......UZ.BIh.(.P.@..#........Yr..x............f$....>.....l..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.@

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\37aee9ee.023bc762744cd0548817[1].js</th></tr>
<tr><td>Process:</td><td>C:\Program Files (x86)\Internet Explorer\iexplore.exe</td></tr>
<tr><td>File Type:</td><td>ASCII text, with very long lines, with no line terminators</td></tr>
<tr><td>Category:</td><td>downloaded</td></tr>
<tr><td>Size (bytes):</td><td>244165</td></tr>
<tr><td>Entropy (8bit):</td><td>4.68737820103819</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>3072:c8Er84Awjj03k4PV03C4PcpiXoLyEZn+3+6DvzZtpSBm6sRTbgQLcn4CQrixrbMp:c8NZgWPZn+3+6D9+s</td></tr>
<tr><td>MD5:</td><td>240379080B94CB962C365F3634D48E4E</td></tr>
<tr><td>SHA1:</td><td>887A81FE5C5AED45B9B849AD1E414AB6C5CD9F4F</td></tr>
<tr><td>SHA-256:</td><td>18C0E02037833073A6C1312310F391C55A47DD81974B36B99406D24555B982CD</td></tr>
<tr><td>SHA-512:</td><td>F00EB0D140EF538BCF896C248C59B2F13AF035E2D24A9257C9D3B4F52CDB48678C2F20B5946E31FDA39F7FE246D0F1D46B656EFAAA9576BD0D29DE7896847D/ A</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Reputation:</td><td>low</td></tr>
<tr><td>IE Cache URL:</td><td>http://https://linktr.ee/_next/static/chunks/37aee9ee.023bc762744cd0548817.js</td></tr>
<tr><td>Preview:</td><td>(window.webpackJsonp=window.webpackJsonp||[]).push([[3],{lanT:function(d,$){!function(){var d=this||self;function $($,e){$=$.split(".");var n,t=d;$[0]in t||"undefined"==t ypeof t.execScript||t.execScript("var "+$[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,$,e){return Array.prototype.index Of.call(d,$,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</td></tr>
</table>

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\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:fBnA1gQwrD32FI
MD5:	2099A0B679B578D738056778DA5C2EA8
SHA1:	8AE37F705D9D752CEB47339AA10ABDAE84D18098
SHA-256:	7E7F002B8581918FFDEA2637DE6C963C9B7B0DDB0ACAD2816ACBFE073E798658

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\4674618e.7a549f670d4ea1a99faf[1].js	
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\Temporary Internet Files\Content.IE5\5JC0A1KN\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
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\Temporary Internet Files\Content.IE5\5JC0A1KN\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\Temporary Internet Files\Content.IE5\5JC0A1KN\[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
SSDEEP:	48:lD58v1xAh/lPr66wpV5qsYauV5q7J21g2td5BArYG4z8wZDSg7+wg:cAtlPr6z35CaY5WJ2q2tdLo4zn7Ng
MD5:	A6BE4B9281D74675B3DA1027F8749D31
SHA1:	71EDA9C31E7308EB544ADAFCE0185D8CBD899D0B
SHA-256:	FBA14C65B1FBDBA974804F2AB94C932EEB7D17BE0B7DCAECD0D13A4D84064C2E

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\[profile][1].js	
SHA-512:	F9606B9BEE222CCF8C973BFA8BAF185FBA1B0C273F04B4C19BEE186C2DEC3DA3F7C8E42688ABD5C3337248AD5EB78FFD16FDFC82ED34BA1BDBDF8C58D388 1996
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\Temporary Internet Files\Content.IE5\5JC0A1KN\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:	3:0SYWFFWlIYCKWMRI5XwDKLRIHDfFRWdFWLRI9j9v7fqzrZqcd39vvE2V8tSDUYAC:0IFFY+56ZRWHMqh7izlpdtEy8tLNin
MD5:	E24D6CEBCF543FA75829419AB80905DA
SHA1:	DC20C556ABA7A4507D8F4191F873789F622A6B02
SHA-256:	B49FA2E8F3A97F3B225021A86390A6CF496FBF66F4F5C99716A4012B92ECE554
SHA-512:	8017D8D13464C7ABE9FC68141CBA5286963102F5399A6F6770CF91CF10298207D09BEAD46969D3FC74D2474B32DA7FB2A5588C1367A9800724B4A62FEF7718C0
Malicious:	false
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\Temporary Internet Files\Content.IE5\5JC0A1KN\css2[2].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\Temporary Internet Files\Content.IE5\5JC0A1KN\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:	40829385A7CBED6EE8863779377E10531C03E016DF116BF8BDB52B3CE750BAFB40B75219197EDF2C027FFE7A13B3FBBCC9AC533C5122C6FFAB531159A00770D 6
Malicious:	false
IE Cache URL:	http://https://linktr.ee/_next/static/chunks/ddbbc6a8.91a110ad55746e11f584.js

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\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\Temporary Internet Files\Content.IE5\5JC0A1KN\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\Temporary Internet Files\Content.IE5\5JC0A1KN\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:ExffRGjwLhrYRc7zsHkwBmaclBmGL0BTMWwMWIeazfIvJks8if:EBRIoYO7fwFgfKTMWLdYks8G
MD5:	40B4095B5B68A142C856F388CCB756F2
SHA1:	31905340609587E1A7C5D4A92D08A2FA3B404DB1
SHA-256:	E2FBB88B4D15A9F7702CA58EBBE8D1D927FFD2667E585E70A5F3D51ACB1A37D2
SHA-512:	3FAB812739B50D25209FE4EC6A72D2441ECE9D4A9347DFD0A47CEC27CCB07676ED8B9958E4985831A896166492DB33D9D88951C88F1FD0BB1858908209058259
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),o=!1}finally{o&&delete n[r]}return 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\Temporary Internet Files\Content.IE5\T4O403JZ\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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\89963fc67fc7243243e5d1e66f0a4763d3fc8a2b_CSS.244c3afbbfc751a1196f[1].js	
Preview:	(window.webpackJsonp=window.webpackJsonp||[]).push([[8],[]]);

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\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-T i<....[....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\Temporary Internet Files\Content.IE5\T4O403JZ\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}h tml{font-family:sans

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\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
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\Temporary Internet Files\Content.IE5\T4O403JZ\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,accessibleNameRequired:!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","structure","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":function(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\Temporary Internet Files\Content.IE5\T4O403JZ\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\Temporary Internet Files\Content.IE5\T4O403JZ\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\Temporary Internet Files\Content.IE5\T4O403JZ\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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\f[1].txt	
Encrypted:	false
SSDEEP:	384:fvrS22Cz5Pre2C2xOMJ+siVS9yS8ksf92xeE1zeuzitwXMyFJTVen5r:X/zyM1yS9yS8k+92NLv4
MD5:	5D2FEECA4ABE16EC87F73BB1E452D943
SHA1:	35AD3FD46E181554318E6710149C262A78A56523
SHA-256:	30B509528A09195B7A7080345419048FD35269803CDFEAB438A98C2176A1D9D0
SHA-512:	ADBC86E5FAB01B8522308E4F63394B2B7CD3F07B5B4DBED76969E49DDB065BA9FFC8D906AAE4EB86EFE7EFB0DCBC9F58DFE8CE6AAC817072193C4CB71415 33E1
Malicious:	false
IE Cache URL:	http://https://www.googleadservices.com/pagead/conversion_async.js
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,v alue: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 globa l&&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 Sy mbol&&"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\Temporary Internet Files\Content.IE5\T4O403JZ\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:	E2C9E41DF9465B44E4FED8E7CFB79AB20B5602A64FF6803DA21D942DBF01FFB484BA9C68329513080CF198B6ADD9258D53DD2FF7D77E90754ABAA1F00D6FF8 8
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 .9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.....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....%tEXtda te: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.0B B..>....VtEXtThumb::URI.file:///mntlog/favico

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\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:	5E4CE1913035AD431E9D0DF3E755A18BCB53731688EEE1E54204CBA7E7F623DEA481C48FDB1F658D824D234169CD02C0B7A6F9643C26AE935368781B9396FBC B
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_GL OBAL_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\Temporary Internet Files\Content.IE5\T4O403JZ\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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\free-v4-shims.min[1].css	
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 F ree";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{co ntent:"\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\Temporary Internet Files\Content.IE5\T4O403JZ\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
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-var iant: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;po sition: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\Temporary Internet Files\Content.IE5\T4O403JZ\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):	66223
Entropy (8bit):	3.522225210694822
Encrypted:	false
SSDEEP:	384:3c4tBf6Q9C2OC9F1ZHr+xoFznknxDt1H34TFo:M4td6Q9P76CMxDtN4TFo
MD5:	CB55EA8477F9AC04643AE3DC6EADEBC2
SHA1:	20E0E4C796C7D83D7AAAD7B5268E185B0A917BB3
SHA-256:	9BAF800E00217EAB0294179FAFC781BB9921F536EA0BB02776A0D7FC94777638
SHA-512:	9930F5098155822A932BD791679C35DE3D73D0F34A4FE0DC01537696697B37FC37EBC1650D647E89E1415A8DB353F848714A15BA04276846A92BF7ECFFAD941A
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: bas eline. }. . 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\Temporary Internet Files\Content.IE5\T4O403JZ\urlblockindex[1].bin	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	data
Category:	downloaded
Size (bytes):	16
Entropy (8bit):	1.6216407621868583
Encrypted:	false
SSDEEP:	3:PF/l:
MD5:	FA518E3DFAE8CA3A0E495460FD60C791
SHA1:	E4F30E49120657D37267C0162FD4A08934800C69
SHA-256:	775853600060162C4B4E5F883F9FD5A278E61C471B3EE1826396B6D129499AA7
SHA-512:	D21667F3FB081D39B579178E74E9BB1B6E9A97F2659029C165729A58F1787DC0ADADD980CD026C7A601D416665A81AC13A69E49A6A2FE2FDD0967938AA645C0

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\urlblockindex[1].bin	
Malicious:	false
IE Cache URL:	http://https://r20swj13mr.microsoft.com/ieblocklist/v1/urlblockindex.bin
Preview:	.p.J2.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC_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:	FFDFBE3A5D9AADDD25C475C9BF0A79CE955A240389241E3794C371D4F80685D7BBD02CA8790C8121DA1F5297360BCDB5F5B73B72D78B331F68AEDBAF82CFE F5
Malicious:	false
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\Temporary Internet Files\Content.IE5\XNHC0JWC_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\Temporary Internet Files\Content.IE5\XNHC0JWC\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/oOkKQB3l+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\Temporary Internet Files\Content.IE5\XNHC0JWC\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:	6D178A6671E6C1E4148770A4FD6351FD237628A48748047006B350E3FBD2BDFD0257BD908BAA26606D3326FE2F7D1E80B505E533716D9EFE8490A6EEC99D83B0
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\Temporary Internet Files\Content.IE5\XNHC0JWC\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
Preview:	(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"

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\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-.61 1,3.184,3.184,0,0,0-1.15-.217,2.919,2.919,0,0,0-2.223.9,3.37,3.37,0,0,0-.847,2.416,3.216,3.216,0,0,0,.813,2.338,2.936,2.936,0,0,0,2.209.837M65.4,8.343a2.952,2.9 52,0,0,1,.5.039,2.1,2.1,0,0,1,.375.1v2.358a2.04,2.04,0,0,0-.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\polyfills-561c4794932226d48fd0[1].js	
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:	7DA3E2C167F148CB915F00A10A6A0E2AFE6117C0AD809493BF695DEB59D85A5B2192F50072F8CFF13A2B97A583E568733332E34290EB5CD6B33802C3379CE4AF
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\Temporary Internet Files\Content.IE5\XNHC0JWC\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
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.....l.@: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.... ...$...7hmtx..D....l...rl'..loca..H.....<...jmaxp..K..... ....name..K,....."3[U.post..L<.....#Ge.prep..Q.....h...x.-..DCa.....?LU.].d .4..J.f.H`&.J .@m!.)..."@.....4%#KV... .....^P.....Ib;@.1g.Y..l....g...{.....rg.y.u/...../...x.....~m..rX)BJ(a;.e.J.)Vl.4..R.....J.G.qg...9.l^y..4..-.`.*.>.....ll%[...B.....UU}...>.=.)"AD...HI.....7.....q.....N.&~..B)..WE.?..?....x.\|...dY.EO....msl.m.m.m.m.f.qh..M..#..=.H..K.L....-E...fI.ABj.Mv..m6.q+..j..h.B`6.Xe.p.R.X.S...<...f.....g....;.(....1.,.....qw..o..d.d.d.....TKj...$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\Temporary Internet Files\Content.IE5\XNHC0JWC\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.....l.@: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\Temporary Internet Files\Content.IE5\XNHC0JWC\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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\qkBIXvYC6trAT55ZBi1ueQVIjQTDJp2qFw[1].woff	
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...I.....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.... ...$...7hmtx..E....P...r...loca..Hd.....<..4maxp..Kt..... ....name..K...."...D6.[]post..L.....#Ge.prep..Qx.....h...x.-..DCa.....?LU.].d .4..J.f.H `&...J@[...H.)@.....4%#KV... .....^P.....Ib;@.1g.Y..I.m..1...s{.....rg.y.u/...../...x.....~m..rX)BJ(a;.e.J.)Vl.4..R.....J.G.qg...9.l^y..4..-.`.*.>.....Il%[...B...[.UU}.....=.."AD...HI.. .].....q.....N.&~..B)..WE.?..?....x.|...$[.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\Temporary Internet Files\Content.IE5\XNHC0JWC\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
SSDEEP:	384:YqD/yN4jvqgVU+cElyWo+3dRlttWWgTJfocPuyXoC6+fObTJjKbgSbH+A:nry8lNcElyT+3fVWbTJfocmEos2b9+gw
MD5:	98B3968B9D045714CFA9AB7A80EE45A5
SHA1:	BE1DA834578FA6D99B71C3A6B3FC655996196E26
SHA-256:	828C641A1D8771BB4DD56B570C1C9C0AA83F0ABDAC8BEA3E8C7B97C3A1B676C9
SHA-512:	26189CCB03CAD8CD9CB586C55CF0DEA83DBA25C2094AA58F0D2CD913B808369FACED255177F637D444404CC3525357584903D71441BDB72BDFB01BD4846D1A A
Malicious:	false
IE Cache URL:	http://https://fonts.gstatic.com/s/karla/v14/qkBIXvYC6trAT55ZBi1ueQVIjQTDppqqFw.woff
Preview:	wOFF.....QX.....`.....GDEF...I.....H.@:GPOS..... .....Qg.GSUB.....f...na.h.OS/2.....Z...`.^eSTAT...I...<...L....cmap.....F.....pQsgasp.....glyf.....2...Q.5 .N.head..D....6...6.=.zhhea..D.... ...$...7hmtx..D....K...r....loca..HH.....<....maxp..KX..... ....name..Kt.....87U\fpost..L.....#Ge.prep..QP.....h...x.-..DCa.....?LU.].d .4..J. f.HD.LM*@(.m!.)..."@.....4%#KV... .....^P.....Ib;@.1gW.[l.]...g...{.....rg.y.u/...../...x.....~m..rX)BJ(a;.e.J.)Vl.4..R.....J.G.qg...9.l^y..4..-.`.*.>.....Il%[...B.6.;.UU}...>.=.) "AD...HI.....q.....N.&~..B)..WE.?..?l...x.|Q...X...I.l...m.m.m.m.6...(m..>V..` ....*R...[.....i..@...q.6po].CK..n.%B...F..aa..{..... .....X...3x...%.8...K..'e....~2B....%...Q.J....G... P.)O,..*.ZP`..N.\.....>...X>o... ../2#+...9..\.`X..,\.!.6O!.9..z..s..;$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\Temporary Internet Files\Content.IE5\XNHC0JWC\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.. ..... ...$.=. hmtx.....p.E..loca.....:N..Smaxp..... ... ....name...<.....Tlvpost...@...P.....prep.....`...`.Ex+.....x.-....A.....<.2.....,#....k..]WfP:.O.....tV.W.Ha. 2.....9.7.%..<..r.....&.<.....x.\..L.Q...{o.]..k..l{6.....lf...4+.....w.....&.H...T.....$.....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.;!.l...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\Temporary Internet Files\Content.IE5\ZAE7RW1P\07D9KDVU.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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\07D9KDVU.htm	
SHA-512:	A05A7979B53ADFE694C2BA886E7AA89BF4D7E4F4EB0D684B00349DF71D4F3B463C14D18C6DB085CC57A74A82860FCD05E7286AB31A6C037C5B80A6D43EBE31F5
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_10, Description: Yara detected HtmlPhish_10, Source: C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\07D9KDVU.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" content="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="	

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\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\Temporary Internet Files\Content.IE5\ZAE7RW1P\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\Temporary Internet Files\Content.IE5\ZAE7RW1P\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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\YS99cwPS1yJGdXcJU31Y_62xa7aqirVCeh6yn[1].jpg	
SHA-256:	19937CE1BB80110BFF3B21817076DB673CBB2B7357263F05B03D5DCEC5C7F8B6
SHA-512:	778D16E08E5914E3B62FAC7AE0EC153DEA6AFD5F0DE15330DA9E1540BC73515F8023F1228A8C185B787224999978 46EDFED5BDD5DE3D8A1BACA57CEEAD583AE7
Malicious:	false
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@.I..#.....o%*.....[.....=..y...i.....yUR.....)..v.C.....+y*....|..?@..*..... <.....9[\.....Wu.....I....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\Temporary Internet Files\Content.IE5\ZAE7RW1P_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
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\Temporary Internet Files\Content.IE5\ZAE7RW1P\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+tIeFLkjdPg
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\Temporary Internet Files\Content.IE5\ZAE7RW1P\favicon[1].ico	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 4-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	237
Entropy (8bit):	6.1480026084285395
Encrypted:	false
SSDEEP:	6:6v/lhPIF6R/C+u1fXNg1XQ3yslRtNO+cKvAElRApGCp:6v/7b/C1fm1ZslRTvAElR47
MD5:	9FB559A691078558E77D6848202F6541
SHA1:	EA13848D33C2C7F4F4BAA39348AEB1DBFAD3DF31
SHA-256:	6D8A01DC7647BC218D003B58FE04049E24A9359900B7E0CEBAE76EDF85B8B914
SHA-512:	0E08938568CD123BE8A20B87D9A3AAF5CB05249DE7F8286FF99D3FA35FC7AF7A9D9797DD6EFB6D1E722147DCFB74437DE520395234D0009D452FB96A8ECE23B

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\favicon[1].ico	
Malicious:	false
IE Cache URL:	http://www.bing.com/favicon.ico
Preview:	.PNG.....IHDR.....R....sRGB.....gAMA.....a.....pHYs.....o.d...-PLTE.....(..5..X..h.....J4.I...IIDAT.[c`..&.(.....F....cX.(@.j.+@..K.(..2L....1.{.....c`]L 9.&2.l...I..E.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\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\Temporary Internet Files\Content.IE5\ZAE7RW1P\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\Temporary Internet Files\Content.IE5\ZAE7RW1P\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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\jquery-3.3.1[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 under the MIT license. * https://jquery.org/license. *. * Date: 2018-01-20T17:24Z. */.(function(global, factory) {..."use strict";...if (typeof module === "object" && typeof module.exports === "object") {....// For CommonJS and CommonJS-like environments where a proper `window`...// is present, execute the factory and get jQuery....// For environments 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\Temporary Internet Files\Content.IE5\ZAE7RW1P\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
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\Temporary Internet Files\Content.IE5\ZAE7RW1P\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
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\Temporary Internet Files\Content.MSO\3EA4068F.png	
Process:	C:\Program Files\Microsoft Office\Office14\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
SHA-256:	5697E0FFEA9EF65FDAAFE0FBC36673FF1C06E7DD6BAF28DF5F06BF53E0393EE8
SHA-512:	046BA1E28B6152D2471EBE8DF24FFE8644CC40A06BA5E78ED45896A9C0ED2BF788F7ED40BB7FE189660503F701B3F0F7161ADECB1FE39A2DDC13A1340F8D3BEE
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\3EA4068F.png	
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\Temp\Cab4633.tmp	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Microsoft Cabinet archive data, 58936 bytes, 1 file
Category:	dropped
Size (bytes):	58936
Entropy (8bit):	**7.994797855729196**
Encrypted:	**true**
SSDEEP:	768:A2CCXehkvodpN73AJjDzh85ApA37vK5clxQh+aLE/sSkoWYrgEHqCinmXdBDz2mi:i/LAvEZrGclx0hoW6qCLdNz2pj
MD5:	E4F1E21910443409E81E5B55DC8DE774
SHA1:	EC0885660BD216D0CDD5E6762B2F595376995BD0
SHA-256:	CF99E08369397577BE949FBF1E4BF06943BC8027996AE65CEB39E38DD3BD30F5
SHA-512:	2253849FADBCDF2B10B78A8B41C54E16DB7BB300AAA1A5A151EDA2A7AA64D5250AED908C3B46AFE7262E66D957B255F6D57B6A6BB9E4F9324F2C22E9BF0882 46
Malicious:	false
Preview:	MSCF....8.....,.....I.....S.....LQ.v .authroot.stl..0(/.5..CK..8T....c_.d...:(.....].M$[v.4CH)-.%.QIR..$t)Kd...D.....3.n..u.....|..=H4.U=...X..qn.+S..^J.....y.n.v.XC... 3a.!.....]...c(...p..]..M.....4.....i...}C.@.[..#xUU..*D..agaV..2.|.g...Y..j.^..@.Q.....n7R...`.../..s...f...+...c..9+[.|0.'..2!.s....a.....w.t:..L!.s....`.O>.`#..'.pfi7.U.....s..^...wz.A.g.Y.... ....g.....:7{.O.....N.....C..?....P0$.Y..?m....Z0.g3.>W0&.y](....].`>... ..R.qB..f.....y.cEB.V=.....hy}....t6b.q./~.p.....60...eCS4.o.....d..}.<,nh..;.....)....e..\|....Cxj...f.8.Z..&..G..... ..b.....OGQ.V..q..Y.....q...0..V.Tu?.Z..r...J...>R.ZsQ...dn.0.<...o.K....\|.....Q...'....X..C.....a;.*..Nq..x.b4..1,}.'.....z.N.N...Uf.q'.>}.....o\.cD"0.'.Y.....SV..g...Y.....o.=.....k..u. .s.kV?@....M...S.n^.:G.....U.e.v..>...q.'..$.)3..T...r.!.m.....6...r,lH.B <.ht..8.s..u[.N.dL.%...q....g..;T..l..5...\.....g...`...........A$:.....

C:\Users\user\AppData\Local\Temp\Cab46A2.tmp	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Microsoft Cabinet archive data, 58936 bytes, 1 file
Category:	dropped
Size (bytes):	58936
Entropy (8bit):	**7.994797855729196**
Encrypted:	**true**
SSDEEP:	768:A2CCXehkvodpN73AJjDzh85ApA37vK5clxQh+aLE/sSkoWYrgEHqCinmXdBDz2mi:i/LAvEZrGclx0hoW6qCLdNz2pj
MD5:	E4F1E21910443409E81E5B55DC8DE774
SHA1:	EC0885660BD216D0CDD5E6762B2F595376995BD0
SHA-256:	CF99E08369397577BE949FBF1E4BF06943BC8027996AE65CEB39E38DD3BD30F5
SHA-512:	2253849FADBCDF2B10B78A8B41C54E16DB7BB300AAA1A5A151EDA2A7AA64D5250AED908C3B46AFE7262E66D957B255F6D57B6A6BB9E4F9324F2C22E9BF0882 46
Malicious:	false
Preview:	MSCF....8.....,.....I.....S.....LQ.v .authroot.stl..0(/.5..CK..8T....c_.d...:(.....].M$[v.4CH)-.%.QIR..$t)Kd...D.....3.n..u.....|..=H4.U=...X..qn.+S..^J.....y.n.v.XC... 3a.!.....]...c(...p..]..M.....4.....i...}C.@.[..#xUU..*D..agaV..2.|.g...Y..j.^..@.Q.....n7R...`.../..s...f...+...c..9+[.|0.'..2!.s....a.....w.t:..L!.s....`.O>.`#..'.pfi7.U.....s..^...wz.A.g.Y.... ....g.....:7{.O.....N.....C..?....P0$.Y..?m....Z0.g3.>W0&.y](....].`>... ..R.qB..f.....y.cEB.V=.....hy}....t6b.q./~.p.....60...eCS4.o.....d..}.<,nh..;.....)....e..\|....Cxj...f.8.Z..&..G..... ..b.....OGQ.V..q..Y.....q...0..V.Tu?.Z..r...J...>R.ZsQ...dn.0.<...o.K....\|.....Q...'....X..C.....a;.*..Nq..x.b4..1,}.'.....z.N.N...Uf.q'.>}.....o\.cD"0.'.Y.....SV..g...Y.....o.=.....k..u. .s.kV?@....M...S.n^.:G.....U.e.v..>...q.'..$.)3..T...r.!.m.....6...r,lH.B <.ht..8.s..u[.N.dL.%...q....g..;T..l..5...\.....g...`...........A$:.....

C:\Users\user\AppData\Local\Temp\Tar4634.tmp	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	152533
Entropy (8bit):	6.31602258454967
Encrypted:	false
SSDEEP:	1536:SIPLlYy2pRSjgCyrYBb5HQop4Ydm6CWku2PtIz0jD1rfJs42t6WP:S4LIpRScCy+fdmcku2PagwQA
MD5:	D0682A3C344DFC62FB18D5A539F81F61
SHA1:	09D3E9B899785DA377DF2518C6175D70CCF9DA33
SHA-256:	4788F7F15DE8063BB3B2547AF1BD9CDBD0596359550E53EC98E532B2ADB5EC5A
SHA-512:	0E884D65C738879C7038C8FB592F53DD515E630AEACC9D9E5F9013606364F092ACF7D832E1A8DAC86A1F0B0E906B2302EE3A840A503654F2B39A65B2FEA04EC
Malicious:	false
Preview:	0..S...*.H.....S.0..S....1.0...`.H.e.....0..C...+.....7.....C.0..C.0...+.....7.....201012214904Z0...+.....0..C.0..*.....`...@.,..0..0.r1...0...+.....7..~1.....D...0...+.....7..i1...0... +.....7<..0 ..+.....7...1.....@N...%.=.,..0$..+.....7...1.....`@V'..%..*..S.Y.00..+.....7..b1". .].L4.>..X...E.W..'.....-@w0Z..+.....7...1L.JM.i.c.r.o.s.o.f.t. .R.o.o.t. .C.e.r.t.i.f.i.c.a.t.e. .A.u.t.h.o.r.i.t.y...0..,.....[./..ulv..%1...0...+.....7..h1.....6.M...0...+.....7..~1.....0...+.....7...1...0...+.....0 ..+.....7...1...O..V.....b0$..+.....7...1...>.)....s,.=$.~R.'..00..+. ....7..b1". [x.....[....3x:_....7.2...Gy.cS.0D..+.....7...16.4V.e.r.i.S.i.g.n. .T.i.m.e. .S.t.a.m.p.i.n.g. .C.A...0.....4...R....2.7.. ...1..0...+.....7..h1.....o&...0...+.....7..i1...0...+.....7<..0 ..+.....7...1...lo...^....[...J@0$..+.....7...1...J\u".F....9.N...`...00..+.....7..b1". ...@.....G..d..m..$.....X...}0B..+.....7...14.2M.i.c.r.o.s.o.f.t. .R.o.o.t. .A.u.t.h.o

C:\Users\user\AppData\Local\Temp\Tar46A3.tmp

C:\Users\user\AppData\Local\Temp\Tar46A3.tmp	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	152533
Entropy (8bit):	6.31602258454967
Encrypted:	false
SSDEEP:	1536:SIPLlYy2pRSjgCyrYBb5HQop4Ydm6CWku2PtIz0jD1rfJs42t6WP:S4LIpRScCy+fdmcku2PagwQA
MD5:	D0682A3C344DFC62FB18D5A539F81F61
SHA1:	09D3E9B899785DA377DF2518C6175D70CCF9DA33
SHA-256:	4788F7F15DE8063BB3B2547AF1BD9CDBD0596359550E53EC98E532B2ADB5EC5A
SHA-512:	0E884D65C738879C7038C8FB592F53DD515E630AEACC9D9E5F9013606364F092ACF7D832E1A8DAC86A1F0B0E906B2302EE3A840A503654F2B39A65B2FEA04EC
Malicious:	false
Preview:	0..S...*.H.....S.0..S....1.0...`.H.e.....0..C...+.....7.....C.0..C.0...+.....7.....20101221490 4Z0...+.....0..C.0..*.....`...@.,..0..0.r1...0...+.....7..~1.....D...0...+.....7..i1...0... +.....7<..0 ..+.....7...1.....@N...%.=.,..0$..+.....7...1.....`@V'..%..*..S.Y.00..+.....7..b1". .].L4.>..X...E.W..'.....-@w0Z..+.....7...1L.JM.i.c.r.o.s.o.f.t. .R.o.o.t. .C.e.r.t.i.f.i.c.a.t.e. .A.u.t.h.o.r.i.t.y...0..,.....[./..uIv..%1...0...+.....7..h1.....6.M...0...+.....7..~1.....0...+.....7...1...0...+.....0 ..+.....7...1...O..V.....b0$..+.....7...1...>.)....s,.=$.~R.'..00..+. ....7..b1". [x.....[....3x:_....7.2...Gy.cS.0D..+.....7...16.4V.e.r.i.S.i.g.n. .T.i.m.e. .S.t.a.m.p.i.n.g. .C.A...0.....4...R....2.7.. ...1..0...+.....7..h1.....o&...0...+.....7..i1...0...+.....7<..0 ..+.....7...1...lo...^....[...J@0$..+.....7...1...J\u".F....9.N...`...00..+.....7..b1". ...@.....G..d..m..$.....X...}0B..+.....7...14.2M.i.c.r.o.s.o.f.t. .R.o.o.t. .A.u.t.h.o

C:\Users\user\AppData\Local\Temp\~DF07EE94C78C24348B.TMP	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	2.4993228309949833
Encrypted:	false
SSDEEP:	96:LywrbP6HDmvCrbP6HDX4TrbP6HDlw0bP6HDcSaSDbP6HDllRbP6HDn:Ly/jmvdjX4GjlwXjRvajllUjn
MD5:	1C7AB6E8645C1FB34F4C75555EBC3C7E
SHA1:	80D7E65995713E6221BD5277F6CFBDA872FDEF9F
SHA-256:	D355B274297736C9B29E2500BDAD8673C76B7E2E9CD077DC6D7C3D871EBCF5CD
SHA-512:	CB8CE4273297BFD48B4D67445669CC5A5C13AFB519EA6833DD2474F1B51F3F7CEC7BE3C90D3B75717C23A6FDAD840EFA56E1E6F1DB0BE0DF086F03C1816A0 09
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... .....N.....(.....Ye P.....Ee.....h.....<....8-d`.....\.f.....=...P..!0.....g.....k.....>.....I.....e.... .....m.....M.....`.....f.....N.....0.....g.....p.....O.....P.....e.....r.....Q.. .....`.....f.....R.....0.....g.....u.....S.....T.....e.....w.....U.....`.....f.....

C:\Users\user\AppData\Local\Temp\~DF393BF7B86FA4A2BC.TMP	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	44273
Entropy (8bit):	1.6947841223581
Encrypted:	false
SSDEEP:	384:Lygvy9vVzq18fE0Q+c06Ks0UthELBeoW0:bvnft
MD5:	B3F13E07A92CABBCB09DCE115AF40042
SHA1:	543D6785E50206236E9E6B1E5ABA82BAFD725D7E
SHA-256:	888268E10B1AFC6C0324256323648DCDA3EC947DE17AFF2DE7AA17498CEB6FAE
SHA-512:	6BE251AF97297A68DE3E112A1C58FC5D11F1AF8FC56FDDF3793E47DBFBA1B3D709E485C9D32B15BEB60F0DBA8BA088CD7012649E03390ED93BC7730AD56676 E0
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... .....`+FA.....K.j.j.a.q.f.a.j.N.2.c .0.u.z.g.v.1.l.4.q.y.5.n.f.W.e.....8.....X..... ....

C:\Users\user\AppData\Local\Temp\~DF991194E5623C2CC5.TMP	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13077
Entropy (8bit):	0.7983133744462331
Encrypted:	false
SSDEEP:	24:3NlLONlLONlIkNlIkNlouqXNlou6G83XNlWu5TOswTMKPMSMTaYwYo:LypvPuqIu6G42u5TFwTMaMSMTaYwYo
MD5:	C161751BC8849F7BC90754848A12A543
SHA1:	7F17220CBDBBA7AB5C92FF7925C6DB2E1C7833B2

C:\Users\user\AppData\Local\Temp\~DF991194E5623C2CC5.TMP	
SHA-256:	DE2A13DF01A67B3E80A6407AA5313989C858B8B9DCBF8A2CCF1C197829C6AA67
SHA-512:	705864E96056A663707DE1C619155468597A8D4C980552A6C4B8B1522DC31E1B08638159D97326D9BAE382050534C97AA2AF1ABFA2B5EE97E059D7EC687F0C7C
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\Desktop\~$Direct Deposit.xlsx	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	165
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fV:vBFFGS
MD5:	797869BB881CFBCDAC2064F92B26E46F
SHA1:	61C1B8FBF505956A77E9A79CE74EF5E281B01F4B
SHA-256:	D4E4008DD7DFB936F22D9EF3CC569C6F88804715EAB8101045BA1CD0B081F185
SHA-512:	1B8350E1500F969107754045EB84EA9F72B53498B1DC05911D6C7E771316C632EA750FBCE8AD3A82D664E3C65CC5251D0E4A21F750911AE5DC2FC3653E49F58
Malicious:	false
Preview:	.user ..A.l.b.u.s. . . . .

Static File Info

General

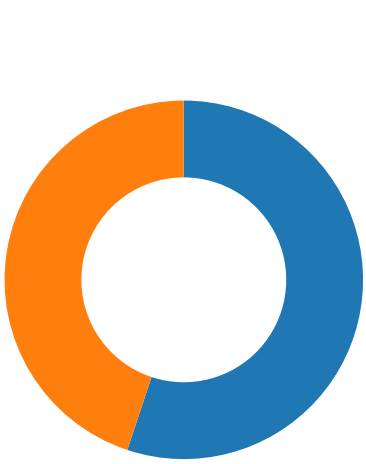
File type:	Microsoft Excel 2007+
Entropy (8bit):	7.875577413292684
TrID:	• Excel Microsoft Office Open XML Format document (40004/1) 83.33% • ZIP compressed archive (8000/1) 16.67%
File name:	Direct Deposit.xlsx
File size:	53638
MD5:	69e51c55e817ad606af9c380ff76ea90
SHA1:	0385a74d84fbf8964d363fb979ecf6afe14b5eba
SHA256:	c38e8675fe9efcc6c74ac66c182c58d458b091d14ababda785b3144e3fbbfe6f
SHA512:	a4053c28b7697e1ecf5a0f9b63e39217e5c179318f21ea6a502a270109460250c89a6000e57cf84d16c5396ad0a2e34017609f369262fbc49c127f589fd6b255
SSDEEP:	1536:LFxJ4QsSxCGi2JGHCv3wcQMcK6Xvl/R1ZtdVF++:JcQxC0JurUcTsJz
File Content Preview:	PK.....!..``p.....[Content_Types].xml ...(..... ....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 14:40:19.407871962 CET	49165	443	192.168.2.22	151.101.130.133
Nov 27, 2020 14:40:19.416356087 CET	49166	443	192.168.2.22	151.101.130.133
Nov 27, 2020 14:40:19.426901102 CET	443	49165	151.101.130.133	192.168.2.22
Nov 27, 2020 14:40:19.426983118 CET	49165	443	192.168.2.22	151.101.130.133
Nov 27, 2020 14:40:19.435072899 CET	49165	443	192.168.2.22	151.101.130.133
Nov 27, 2020 14:40:19.435399055 CET	443	49166	151.101.130.133	192.168.2.22
Nov 27, 2020 14:40:19.435465097 CET	49166	443	192.168.2.22	151.101.130.133
Nov 27, 2020 14:40:19.435805082 CET	49166	443	192.168.2.22	151.101.130.133
Nov 27, 2020 14:40:19.454021931 CET	443	49165	151.101.130.133	192.168.2.22
Nov 27, 2020 14:40:19.454646111 CET	443	49166	151.101.130.133	192.168.2.22
Nov 27, 2020 14:40:19.455615997 CET	443	49165	151.101.130.133	192.168.2.22
Nov 27, 2020 14:40:19.455643892 CET	443	49165	151.101.130.133	192.168.2.22
Nov 27, 2020 14:40:19.455662966 CET	443	49165	151.101.130.133	192.168.2.22
Nov 27, 2020 14:40:19.455703020 CET	49165	443	192.168.2.22	151.101.130.133
Nov 27, 2020 14:40:19.455734015 CET	49165	443	192.168.2.22	151.101.130.133
Nov 27, 2020 14:40:19.456166029 CET	443	49166	151.101.130.133	192.168.2.22
Nov 27, 2020 14:40:19.456192970 CET	443	49166	151.101.130.133	192.168.2.22
Nov 27, 2020 14:40:19.456212044 CET	443	49166	151.101.130.133	192.168.2.22
Nov 27, 2020 14:40:19.456217051 CET	49165	443	192.168.2.22	151.101.130.133
Nov 27, 2020 14:40:19.456270933 CET	49166	443	192.168.2.22	151.101.130.133
Nov 27, 2020 14:40:19.456310987 CET	49166	443	192.168.2.22	151.101.130.133
Nov 27, 2020 14:40:19.456319094 CET	49166	443	192.168.2.22	151.101.130.133
Nov 27, 2020 14:40:19.463102102 CET	49165	443	192.168.2.22	151.101.130.133
Nov 27, 2020 14:40:19.470566988 CET	49166	443	192.168.2.22	151.101.130.133
Nov 27, 2020 14:40:19.482426882 CET	443	49165	151.101.130.133	192.168.2.22
Nov 27, 2020 14:40:19.482605934 CET	49165	443	192.168.2.22	151.101.130.133
Nov 27, 2020 14:40:19.489979982 CET	443	49166	151.101.130.133	192.168.2.22
Nov 27, 2020 14:40:19.490045071 CET	49166	443	192.168.2.22	151.101.130.133
Nov 27, 2020 14:40:21.080722094 CET	49165	443	192.168.2.22	151.101.130.133
Nov 27, 2020 14:40:21.100692034 CET	443	49165	151.101.130.133	192.168.2.22
Nov 27, 2020 14:40:21.100743055 CET	443	49165	151.101.130.133	192.168.2.22
Nov 27, 2020 14:40:21.100780010 CET	443	49165	151.101.130.133	192.168.2.22
Nov 27, 2020 14:40:21.100785017 CET	49165	443	192.168.2.22	151.101.130.133
Nov 27, 2020 14:40:21.100804090 CET	49165	443	192.168.2.22	151.101.130.133
Nov 27, 2020 14:40:21.100819111 CET	443	49165	151.101.130.133	192.168.2.22
Nov 27, 2020 14:40:21.100847006 CET	49165	443	192.168.2.22	151.101.130.133
Nov 27, 2020 14:40:21.100852013 CET	443	49165	151.101.130.133	192.168.2.22
Nov 27, 2020 14:40:21.100883961 CET	49165	443	192.168.2.22	151.101.130.133
Nov 27, 2020 14:40:21.100918055 CET	49165	443	192.168.2.22	151.101.130.133
Nov 27, 2020 14:40:21.237369061 CET	49165	443	192.168.2.22	151.101.130.133
Nov 27, 2020 14:40:21.254740000 CET	49166	443	192.168.2.22	151.101.130.133
Nov 27, 2020 14:40:21.257589102 CET	443	49165	151.101.130.133	192.168.2.22
Nov 27, 2020 14:40:21.257662058 CET	443	49165	151.101.130.133	192.168.2.22
Nov 27, 2020 14:40:21.257702112 CET	443	49165	151.101.130.133	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 14:40:21.257735014 CET	443	49165	151.101.130.133	192.168.2.22
Nov 27, 2020 14:40:21.257755041 CET	49165	443	192.168.2.22	151.101.130.133
Nov 27, 2020 14:40:21.257790089 CET	49165	443	192.168.2.22	151.101.130.133
Nov 27, 2020 14:40:21.257796049 CET	49165	443	192.168.2.22	151.101.130.133
Nov 27, 2020 14:40:21.261977911 CET	49171	443	192.168.2.22	151.101.130.133
Nov 27, 2020 14:40:21.262479067 CET	49172	443	192.168.2.22	151.101.130.133
Nov 27, 2020 14:40:21.263005018 CET	49173	443	192.168.2.22	151.101.130.133
Nov 27, 2020 14:40:21.264019966 CET	49174	443	192.168.2.22	151.101.130.133
Nov 27, 2020 14:40:21.267435074 CET	49165	443	192.168.2.22	151.101.130.133
Nov 27, 2020 14:40:21.274677038 CET	443	49166	151.101.130.133	192.168.2.22
Nov 27, 2020 14:40:21.274734020 CET	443	49166	151.101.130.133	192.168.2.22
Nov 27, 2020 14:40:21.274771929 CET	443	49166	151.101.130.133	192.168.2.22
Nov 27, 2020 14:40:21.274802923 CET	49166	443	192.168.2.22	151.101.130.133
Nov 27, 2020 14:40:21.274811983 CET	443	49166	151.101.130.133	192.168.2.22
Nov 27, 2020 14:40:21.274816036 CET	49166	443	192.168.2.22	151.101.130.133
Nov 27, 2020 14:40:21.274849892 CET	443	49166	151.101.130.133	192.168.2.22
Nov 27, 2020 14:40:21.274856091 CET	49166	443	192.168.2.22	151.101.130.133
Nov 27, 2020 14:40:21.274888039 CET	443	49166	151.101.130.133	192.168.2.22
Nov 27, 2020 14:40:21.274893045 CET	49166	443	192.168.2.22	151.101.130.133
Nov 27, 2020 14:40:21.274925947 CET	443	49166	151.101.130.133	192.168.2.22
Nov 27, 2020 14:40:21.274929047 CET	49166	443	192.168.2.22	151.101.130.133
Nov 27, 2020 14:40:21.274971008 CET	49166	443	192.168.2.22	151.101.130.133
Nov 27, 2020 14:40:21.274974108 CET	443	49166	151.101.130.133	192.168.2.22
Nov 27, 2020 14:40:21.275016069 CET	443	49166	151.101.130.133	192.168.2.22
Nov 27, 2020 14:40:21.275018930 CET	49166	443	192.168.2.22	151.101.130.133
Nov 27, 2020 14:40:21.275054932 CET	443	49166	151.101.130.133	192.168.2.22
Nov 27, 2020 14:40:21.275060892 CET	49166	443	192.168.2.22	151.101.130.133
Nov 27, 2020 14:40:21.275093079 CET	443	49166	151.101.130.133	192.168.2.22
Nov 27, 2020 14:40:21.275095940 CET	49166	443	192.168.2.22	151.101.130.133
Nov 27, 2020 14:40:21.275131941 CET	443	49166	151.101.130.133	192.168.2.22
Nov 27, 2020 14:40:21.275135994 CET	49166	443	192.168.2.22	151.101.130.133
Nov 27, 2020 14:40:21.275175095 CET	49166	443	192.168.2.22	151.101.130.133
Nov 27, 2020 14:40:21.275558949 CET	443	49166	151.101.130.133	192.168.2.22
Nov 27, 2020 14:40:21.275603056 CET	443	49166	151.101.130.133	192.168.2.22
Nov 27, 2020 14:40:21.275640965 CET	443	49166	151.101.130.133	192.168.2.22
Nov 27, 2020 14:40:21.275655031 CET	49166	443	192.168.2.22	151.101.130.133
Nov 27, 2020 14:40:21.275682926 CET	49166	443	192.168.2.22	151.101.130.133
Nov 27, 2020 14:40:21.276573896 CET	443	49166	151.101.130.133	192.168.2.22
Nov 27, 2020 14:40:21.276612043 CET	443	49166	151.101.130.133	192.168.2.22
Nov 27, 2020 14:40:21.276645899 CET	49166	443	192.168.2.22	151.101.130.133
Nov 27, 2020 14:40:21.276679039 CET	443	49166	151.101.130.133	192.168.2.22
Nov 27, 2020 14:40:21.276731968 CET	49166	443	192.168.2.22	151.101.130.133
Nov 27, 2020 14:40:21.276737928 CET	49166	443	192.168.2.22	151.101.130.133
Nov 27, 2020 14:40:21.277537107 CET	443	49166	151.101.130.133	192.168.2.22
Nov 27, 2020 14:40:21.277580023 CET	443	49166	151.101.130.133	192.168.2.22
Nov 27, 2020 14:40:21.277618885 CET	443	49166	151.101.130.133	192.168.2.22
Nov 27, 2020 14:40:21.277618885 CET	49166	443	192.168.2.22	151.101.130.133
Nov 27, 2020 14:40:21.277688026 CET	49166	443	192.168.2.22	151.101.130.133
Nov 27, 2020 14:40:21.277704954 CET	49166	443	192.168.2.22	151.101.130.133
Nov 27, 2020 14:40:21.278505087 CET	443	49166	151.101.130.133	192.168.2.22
Nov 27, 2020 14:40:21.278538942 CET	443	49166	151.101.130.133	192.168.2.22
Nov 27, 2020 14:40:21.278604984 CET	49166	443	192.168.2.22	151.101.130.133
Nov 27, 2020 14:40:21.279247999 CET	49166	443	192.168.2.22	151.101.130.133
Nov 27, 2020 14:40:21.281148911 CET	443	49171	151.101.130.133	192.168.2.22
Nov 27, 2020 14:40:21.281363964 CET	443	49172	151.101.130.133	192.168.2.22
Nov 27, 2020 14:40:21.281469107 CET	49172	443	192.168.2.22	151.101.130.133

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 14:40:18.427153111 CET	52197	53	192.168.2.22	8.8.8.8
Nov 27, 2020 14:40:18.464200974 CET	53	52197	8.8.8.8	192.168.2.22
Nov 27, 2020 14:40:19.364111900 CET	53099	53	192.168.2.22	8.8.8.8
Nov 27, 2020 14:40:19.399446964 CET	53	53099	8.8.8.8	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 14:40:19.972465992 CET	52838	53	192.168.2.22	8.8.8.8
Nov 27, 2020 14:40:19.992125988 CET	61200	53	192.168.2.22	8.8.8.8
Nov 27, 2020 14:40:19.999469042 CET	53	52838	8.8.8.8	192.168.2.22
Nov 27, 2020 14:40:20.009304047 CET	49548	53	192.168.2.22	8.8.8.8
Nov 27, 2020 14:40:20.019232035 CET	53	61200	8.8.8.8	192.168.2.22
Nov 27, 2020 14:40:20.036438942 CET	53	49548	8.8.8.8	192.168.2.22
Nov 27, 2020 14:40:20.068449974 CET	55627	53	192.168.2.22	8.8.8.8
Nov 27, 2020 14:40:20.095695019 CET	53	55627	8.8.8.8	192.168.2.22
Nov 27, 2020 14:40:20.600987911 CET	56009	53	192.168.2.22	8.8.8.8
Nov 27, 2020 14:40:20.628142118 CET	53	56009	8.8.8.8	192.168.2.22
Nov 27, 2020 14:40:20.636822939 CET	61865	53	192.168.2.22	8.8.8.8
Nov 27, 2020 14:40:20.672513962 CET	53	61865	8.8.8.8	192.168.2.22
Nov 27, 2020 14:40:20.680344105 CET	55171	53	192.168.2.22	8.8.8.8
Nov 27, 2020 14:40:20.707406998 CET	53	55171	8.8.8.8	192.168.2.22
Nov 27, 2020 14:40:20.717700005 CET	52496	53	192.168.2.22	8.8.8.8
Nov 27, 2020 14:40:20.754762888 CET	53	52496	8.8.8.8	192.168.2.22
Nov 27, 2020 14:40:21.235043049 CET	57564	53	192.168.2.22	8.8.8.8
Nov 27, 2020 14:40:21.260066986 CET	63009	53	192.168.2.22	8.8.8.8
Nov 27, 2020 14:40:21.262288094 CET	53	57564	8.8.8.8	192.168.2.22
Nov 27, 2020 14:40:21.271922112 CET	59319	53	192.168.2.22	8.8.8.8
Nov 27, 2020 14:40:21.275470018 CET	53070	53	192.168.2.22	8.8.8.8
Nov 27, 2020 14:40:21.303564072 CET	53	63009	8.8.8.8	192.168.2.22
Nov 27, 2020 14:40:21.307475090 CET	53	59319	8.8.8.8	192.168.2.22
Nov 27, 2020 14:40:21.318475008 CET	53	53070	8.8.8.8	192.168.2.22
Nov 27, 2020 14:40:21.654658079 CET	59770	53	192.168.2.22	8.8.8.8
Nov 27, 2020 14:40:21.690645933 CET	53	59770	8.8.8.8	192.168.2.22
Nov 27, 2020 14:40:22.929302931 CET	61523	53	192.168.2.22	8.8.8.8
Nov 27, 2020 14:40:22.930310965 CET	62791	53	192.168.2.22	8.8.8.8
Nov 27, 2020 14:40:22.930934906 CET	50667	53	192.168.2.22	8.8.8.8
Nov 27, 2020 14:40:22.932298899 CET	54129	53	192.168.2.22	8.8.8.8
Nov 27, 2020 14:40:22.932908058 CET	65329	53	192.168.2.22	8.8.8.8
Nov 27, 2020 14:40:22.933104038 CET	60718	53	192.168.2.22	8.8.8.8
Nov 27, 2020 14:40:22.956418991 CET	53	61523	8.8.8.8	192.168.2.22
Nov 27, 2020 14:40:22.957878113 CET	53	50667	8.8.8.8	192.168.2.22
Nov 27, 2020 14:40:22.959160089 CET	53	54129	8.8.8.8	192.168.2.22
Nov 27, 2020 14:40:22.959789038 CET	53	65329	8.8.8.8	192.168.2.22
Nov 27, 2020 14:40:22.959937096 CET	53	60718	8.8.8.8	192.168.2.22
Nov 27, 2020 14:40:22.974114895 CET	53	62791	8.8.8.8	192.168.2.22
Nov 27, 2020 14:40:24.273576021 CET	49157	53	192.168.2.22	8.8.8.8
Nov 27, 2020 14:40:24.300529003 CET	53	49157	8.8.8.8	192.168.2.22
Nov 27, 2020 14:40:49.110542059 CET	57391	53	192.168.2.22	8.8.8.8
Nov 27, 2020 14:40:49.137872934 CET	53	57391	8.8.8.8	192.168.2.22
Nov 27, 2020 14:40:49.833499908 CET	61858	53	192.168.2.22	8.8.8.8
Nov 27, 2020 14:40:49.860601902 CET	53	61858	8.8.8.8	192.168.2.22
Nov 27, 2020 14:40:50.117335081 CET	57391	53	192.168.2.22	8.8.8.8
Nov 27, 2020 14:40:50.153256893 CET	53	57391	8.8.8.8	192.168.2.22
Nov 27, 2020 14:40:50.834748030 CET	61858	53	192.168.2.22	8.8.8.8
Nov 27, 2020 14:40:50.870675087 CET	53	61858	8.8.8.8	192.168.2.22
Nov 27, 2020 14:40:51.131644011 CET	57391	53	192.168.2.22	8.8.8.8
Nov 27, 2020 14:40:51.167340040 CET	53	57391	8.8.8.8	192.168.2.22
Nov 27, 2020 14:40:51.849190950 CET	61858	53	192.168.2.22	8.8.8.8
Nov 27, 2020 14:40:51.884670973 CET	53	61858	8.8.8.8	192.168.2.22
Nov 27, 2020 14:40:51.992436886 CET	62500	53	192.168.2.22	8.8.8.8
Nov 27, 2020 14:40:52.031461000 CET	53	62500	8.8.8.8	192.168.2.22
Nov 27, 2020 14:40:53.144251108 CET	57391	53	192.168.2.22	8.8.8.8
Nov 27, 2020 14:40:53.191870928 CET	53	57391	8.8.8.8	192.168.2.22
Nov 27, 2020 14:40:53.861709118 CET	61858	53	192.168.2.22	8.8.8.8
Nov 27, 2020 14:40:53.888786077 CET	53	61858	8.8.8.8	192.168.2.22
Nov 27, 2020 14:40:57.154036999 CET	57391	53	192.168.2.22	8.8.8.8
Nov 27, 2020 14:40:57.191637039 CET	53	57391	8.8.8.8	192.168.2.22
Nov 27, 2020 14:40:57.870990992 CET	61858	53	192.168.2.22	8.8.8.8
Nov 27, 2020 14:40:57.898030996 CET	53	61858	8.8.8.8	192.168.2.22
Nov 27, 2020 14:41:30.373641014 CET	51652	53	192.168.2.22	8.8.8.8
Nov 27, 2020 14:41:30.409018993 CET	53	51652	8.8.8.8	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 14:41:33.414036036 CET	62762	53	192.168.2.22	8.8.8.8
Nov 27, 2020 14:41:33.457375050 CET	53	62762	8.8.8.8	192.168.2.22
Nov 27, 2020 14:41:34.039638996 CET	56905	53	192.168.2.22	8.8.8.8
Nov 27, 2020 14:41:34.155416012 CET	54609	53	192.168.2.22	8.8.8.8
Nov 27, 2020 14:41:34.170015097 CET	58101	53	192.168.2.22	8.8.8.8
Nov 27, 2020 14:41:34.192523956 CET	64329	53	192.168.2.22	8.8.8.8
Nov 27, 2020 14:41:34.194860935 CET	64881	53	192.168.2.22	8.8.8.8
Nov 27, 2020 14:41:34.197932959 CET	53	58101	8.8.8.8	192.168.2.22
Nov 27, 2020 14:41:34.198559046 CET	55327	53	192.168.2.22	8.8.8.8
Nov 27, 2020 14:41:34.198658943 CET	53	54609	8.8.8.8	192.168.2.22
Nov 27, 2020 14:41:34.211898088 CET	59150	53	192.168.2.22	8.8.8.8
Nov 27, 2020 14:41:34.216372013 CET	53	56905	8.8.8.8	192.168.2.22
Nov 27, 2020 14:41:34.219463110 CET	53	64329	8.8.8.8	192.168.2.22
Nov 27, 2020 14:41:34.221692085 CET	53	64881	8.8.8.8	192.168.2.22
Nov 27, 2020 14:41:34.225419998 CET	53	55327	8.8.8.8	192.168.2.22
Nov 27, 2020 14:41:34.248560905 CET	53	59150	8.8.8.8	192.168.2.22
Nov 27, 2020 14:41:34.596393108 CET	63439	53	192.168.2.22	8.8.8.8
Nov 27, 2020 14:41:34.623431921 CET	53	63439	8.8.8.8	192.168.2.22
Nov 27, 2020 14:41:34.635889053 CET	65040	53	192.168.2.22	8.8.8.8
Nov 27, 2020 14:41:34.682734013 CET	53	65040	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 27, 2020 14:40:19.364111900 CET	192.168.2.22	8.8.8.8	0x6dcc	Standard query (0)	linktr.ee	A (IP address)	IN (0x0001)
Nov 27, 2020 14:40:21.275470018 CET	192.168.2.22	8.8.8.8	0xb72c	Standard query (0)	d1fdloi71m ui9q.cloud front.net	A (IP address)	IN (0x0001)
Nov 27, 2020 14:41:30.373641014 CET	192.168.2.22	8.8.8.8	0x39c4	Standard query (0)	linktr.ee	A (IP address)	IN (0x0001)
Nov 27, 2020 14:41:33.414036036 CET	192.168.2.22	8.8.8.8	0x17bf	Standard query (0)	secure-excel-file.glitch.me	A (IP address)	IN (0x0001)
Nov 27, 2020 14:41:34.039638996 CET	192.168.2.22	8.8.8.8	0x5fd2	Standard query (0)	ibuykenya.com	A (IP address)	IN (0x0001)
Nov 27, 2020 14:41:34.170015097 CET	192.168.2.22	8.8.8.8	0xb34b	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)
Nov 27, 2020 14:41:34.192523956 CET	192.168.2.22	8.8.8.8	0x7191	Standard query (0)	kit.fontawesome.com	A (IP address)	IN (0x0001)
Nov 27, 2020 14:41:34.194860935 CET	192.168.2.22	8.8.8.8	0xd240	Standard query (0)	maxcdn.bootstrapcdn.com	A (IP address)	IN (0x0001)
Nov 27, 2020 14:41:34.198559046 CET	192.168.2.22	8.8.8.8	0x6e99	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
Nov 27, 2020 14:41:34.211898088 CET	192.168.2.22	8.8.8.8	0x1058	Standard query (0)	secure.aadcdn.microsoftonline-p.com	A (IP address)	IN (0x0001)
Nov 27, 2020 14:41:34.596393108 CET	192.168.2.22	8.8.8.8	0x6ce5	Standard query (0)	ka-f.fontawesome.com	A (IP address)	IN (0x0001)
Nov 27, 2020 14:41:34.635889053 CET	192.168.2.22	8.8.8.8	0x60a4	Standard query (0)	i.ibb.co	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 27, 2020 14:40:19.399446964 CET	8.8.8.8	192.168.2.22	0x6dcc	No error (0)	linktr.ee		151.101.130.133	A (IP address)	IN (0x0001)
Nov 27, 2020 14:40:19.399446964 CET	8.8.8.8	192.168.2.22	0x6dcc	No error (0)	linktr.ee		151.101.66.133	A (IP address)	IN (0x0001)
Nov 27, 2020 14:40:19.399446964 CET	8.8.8.8	192.168.2.22	0x6dcc	No error (0)	linktr.ee		151.101.2.133	A (IP address)	IN (0x0001)
Nov 27, 2020 14:40:19.399446964 CET	8.8.8.8	192.168.2.22	0x6dcc	No error (0)	linktr.ee		151.101.194.133	A (IP address)	IN (0x0001)
Nov 27, 2020 14:40:21.303564072 CET	8.8.8.8	192.168.2.22	0x54dd	No error (0)	pagead.l.doubleclick.net		172.217.168.2	A (IP address)	IN (0x0001)
Nov 27, 2020 14:40:21.318475008 CET	8.8.8.8	192.168.2.22	0xb72c	No error (0)	d1fdloi71m ui9q.cloud front.net		143.204.214.108	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 27, 2020 14:40:21.318475008 CET	8.8.8.8	192.168.2.22	0xb72c	No error (0)	d1fdloi71m ui9q.cloud front.net		143.204.214.143	A (IP address)	IN (0x0001)
Nov 27, 2020 14:40:21.318475008 CET	8.8.8.8	192.168.2.22	0xb72c	No error (0)	d1fdloi71m ui9q.cloud front.net		143.204.214.26	A (IP address)	IN (0x0001)
Nov 27, 2020 14:40:21.318475008 CET	8.8.8.8	192.168.2.22	0xb72c	No error (0)	d1fdloi71m ui9q.cloud front.net		143.204.214.224	A (IP address)	IN (0x0001)
Nov 27, 2020 14:41:30.409018993 CET	8.8.8.8	192.168.2.22	0x39c4	No error (0)	linktr.ee		151.101.194.133	A (IP address)	IN (0x0001)
Nov 27, 2020 14:41:30.409018993 CET	8.8.8.8	192.168.2.22	0x39c4	No error (0)	linktr.ee		151.101.130.133	A (IP address)	IN (0x0001)
Nov 27, 2020 14:41:30.409018993 CET	8.8.8.8	192.168.2.22	0x39c4	No error (0)	linktr.ee		151.101.66.133	A (IP address)	IN (0x0001)
Nov 27, 2020 14:41:30.409018993 CET	8.8.8.8	192.168.2.22	0x39c4	No error (0)	linktr.ee		151.101.2.133	A (IP address)	IN (0x0001)
Nov 27, 2020 14:41:33.457375050 CET	8.8.8.8	192.168.2.22	0x17bf	No error (0)	secure-excel-file.glitch.me		52.205.236.122	A (IP address)	IN (0x0001)
Nov 27, 2020 14:41:33.457375050 CET	8.8.8.8	192.168.2.22	0x17bf	No error (0)	secure-excel-file.glitch.me		34.231.129.212	A (IP address)	IN (0x0001)
Nov 27, 2020 14:41:34.197932959 CET	8.8.8.8	192.168.2.22	0xb34b	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Nov 27, 2020 14:41:34.216372013 CET	8.8.8.8	192.168.2.22	0x5fd2	No error (0)	ibuykenya.com		50.87.153.159	A (IP address)	IN (0x0001)
Nov 27, 2020 14:41:34.219463110 CET	8.8.8.8	192.168.2.22	0x7191	No error (0)	kit.fontawesome.com	kit.fontawesome.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Nov 27, 2020 14:41:34.221692085 CET	8.8.8.8	192.168.2.22	0xd240	No error (0)	maxcdn.bootstrapcdn.com	cds.j3z9t3p6.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Nov 27, 2020 14:41:34.225419998 CET	8.8.8.8	192.168.2.22	0x6e99	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Nov 27, 2020 14:41:34.225419998 CET	8.8.8.8	192.168.2.22	0x6e99	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Nov 27, 2020 14:41:34.248560905 CET	8.8.8.8	192.168.2.22	0x1058	No error (0)	secure.aadcdn.microsoftonline-p.com	secure.aadcdn.microsoftonline-p.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Nov 27, 2020 14:41:34.623431921 CET	8.8.8.8	192.168.2.22	0x6ce5	No error (0)	ka-f.fontawesome.com	ka-f.fontawesome.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Nov 27, 2020 14:41:34.682734013 CET	8.8.8.8	192.168.2.22	0x60a4	No error (0)	i.ibb.co		145.239.131.55	A (IP address)	IN (0x0001)
Nov 27, 2020 14:41:34.682734013 CET	8.8.8.8	192.168.2.22	0x60a4	No error (0)	i.ibb.co		145.239.131.60	A (IP address)	IN (0x0001)
Nov 27, 2020 14:41:34.682734013 CET	8.8.8.8	192.168.2.22	0x60a4	No error (0)	i.ibb.co		145.239.131.51	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	192.168.2.22	49200	50.87.153.159	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Nov 27, 2020 14:41:34.399375916 CET	1904	OUT	GET /vendor/doctrine/styles.css HTTP/1.1 Accept: text/css, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: ibuykenya.com DNT: 1 Connection: Keep-Alive
Nov 27, 2020 14:41:34.581810951 CET	2107	IN	HTTP/1.1 200 OK Date: Fri, 27 Nov 2020 13:41:34 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 14:40:19.455643892 CET	151.101.130.133	443	192.168.2.22	49165	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	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					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 14:40:19.456192970 CET	151.101.130.133	443	192.168.2.22	49166	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	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					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 14:40:21.393652916 CET	143.204.214.108	443	192.168.2.22	49179	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	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					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 14:40:21.398046970 CET	143.204.214.108	443	192.168.2.22	49180	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	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					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 14:40:21.417036057 CET	172.217.168.2	443	192.168.2.22	49175	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	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					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		

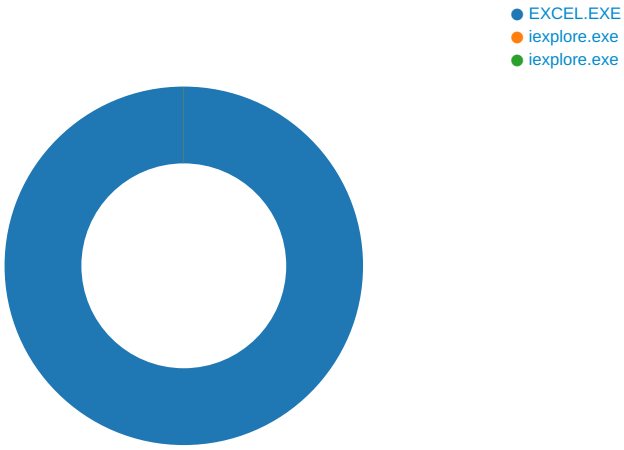
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Nov 27, 2020 14:40:21.419492006 CET	172.217.168.2	443	192.168.2.22	49178	CN=www.googleadservices.com, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, 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	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					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 14:41:33.667021036 CET	52.205.236.122	443	192.168.2.22	49191	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	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					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 14:41:33.667241096 CET	52.205.236.122	443	192.168.2.22	49192	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	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					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 14:41:34.261502981 CET	104.16.19.94	443	192.168.2.22	49206	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Oct 21 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Thu Oct 21 01:59:59 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					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 14:41:34.261945963 CET	104.16.19.94	443	192.168.2.22	49207	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Oct 21 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Thu Oct 21 01:59:59 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					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 14:41:34.738064051 CET	145.239.131.55	443	192.168.2.22	49212	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 Mar 17 17:40:46 CET 2016	Thu Dec 31 07:53:44 CET 2020 Wed Mar 17 17:40:46 CET 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					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 14:41:34.738440990 CET	145.239.131.55	443	192.168.2.22	49213	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 Mar 17 17:40:46 CET 2016	Thu Dec 31 07:53:44 CET 2020 Wed Mar 17 17:40:46 CET 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					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



Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 2448 Parent PID: 584

General

Start time:	14:39:39
Start date:	27/11/2020
Path:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding
Imagebase:	0x13fdb0000
File size:	27641504 bytes
MD5 hash:	5FB0A0F93382ECD19F5F499A5CAA59F0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\42EA.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	1400FEC83	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image002.pn~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.rcv	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.ht~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\42EA.tmp	success or wait	1	14036B818	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.css	C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs~..	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.htm	C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht~s~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.htm	C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht~s~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image002.png	C:\Users\user\AppData\Local\Temp\imgs_files\image002.pn~s~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xml	C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~s~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs_	C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.css..	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht_	C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.htmss	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht_	C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.htmss	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image003.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image003.pngss	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm_	C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xmlss	success or wait	1	7FEEAC59AC0	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$Direct Deposit.xlsx	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	13FFFF526	WriteFile
C:\Users\user\Desktop\~$Direct Deposit.xlsx	unknown	110	05 00 41 00 6c 00 62 00 75 00 73 00 20 00	..A.l.b.u.s.	success or wait	1	13FFFF591	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\3EA4068F.png	0	42269	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\3EA4068F.png	0	42269	success or wait	1	7FEEAC59AC0	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F4395	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F4422	success or wait	1	7FEEAC59AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	|c2	binary	7C 63 32 00 90 09 00 00 02 00 00 00 00 00 00 00 52 00 00 00 01 00 00 00 28 00 00 00 1E 00 00 00 64 00 69 00 72 00 65 00 63 00 74 00 20 00 64 00 65 00 70 00 6F 00 73 00 69 00 74 00 2E 00 78 00 6C 00 73 00 78 00 00 00 64 00 69 00 72 00 65 00 63 00 74 00 20 00 64 00 65 00 70 00 6F 00 73 00 69 00 74 00 00 00	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3771420242.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F4395	F4395	binary	04 00 00 00 90 09 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 BB 9A E9 41 0E C5 D6 01 95 43 0F 00 95 43 0F 00 00 00 00 00 B8 02 00 00 56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3771420242.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F4422	F4422	binary	04 00 00 00 90 09 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 BB 9A E9 41 0E C5 D6 01 22 44 0F 00 22 44 0F 00 00 00 00 00 B8 02 00 00 56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAC59AC0	unknown

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

Analysis Process: iexplore.exe PID: 1748 Parent PID: 584

General

Start time:	14:40:06
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:	0x13f3b0000
File size:	814288 bytes
MD5 hash:	4EB098135821348270F27157F7A84E65
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

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: 2352 Parent PID: 1748

General

Start time:	14:40:06
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:1748 CREDAT:275457 /prefetch:2
Imagebase:	0xaa0000
File size:	815304 bytes
MD5 hash:	8A590F790A98F3D77399BE457E01386A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

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

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

Disassembly