ID: 321374
Sample Name: Fennec Pharma
.docx
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 02:12:58
Date: 21/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

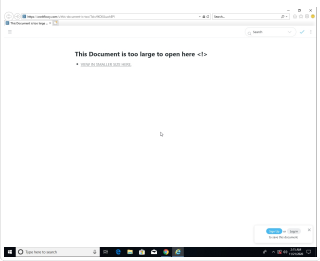
Analysis Report Fennec Pharma .docx

Overview

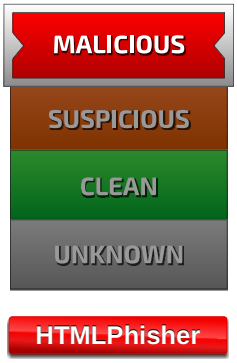
General Information

Sample Name:	Fennec Pharma .docx
Analysis ID:	321374
MD5:	e935876bc1daf07.
SHA1:	2f0444a05ac3eca..
SHA256:	494148b0b3b417..

Most interesting Screenshot:



Detection

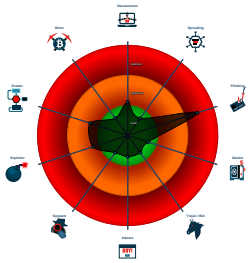


Score:	64
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Yara detected HtmlPhish_10
- Phishing site detected (based on im…
- Phishing site detected (based on log…
- Allocates a big amount of memory (p…
- Found a high number of Window / Us…
- HTML body contains low number of …
- HTML title does not match URL
- IP address seen in connection with o…
- JA3 SSL client fingerprint seen in co…
- Sample execution stops while proce…

Classification



Startup

- **System is w10x64**
- WINWORD.EXE (PID: 488 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE' /Automation -Embedding MD5: 0B9AB9B9C4DE429473D6450D4297A123)
  - splwow64.exe (PID: 6640 cmdline: C:\Windows\splwow64.exe 12288 MD5: 8D59B31FF375059E3C32B17BF31A76D5)
- iexplore.exe (PID: 6300 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6344 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6300 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

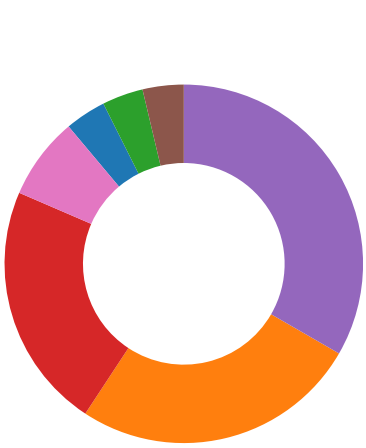
Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\dfce06801e1a85d6d06f1fdd4475dacd[1].htm	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Phishing:

Yara detected HtmlPhish_10

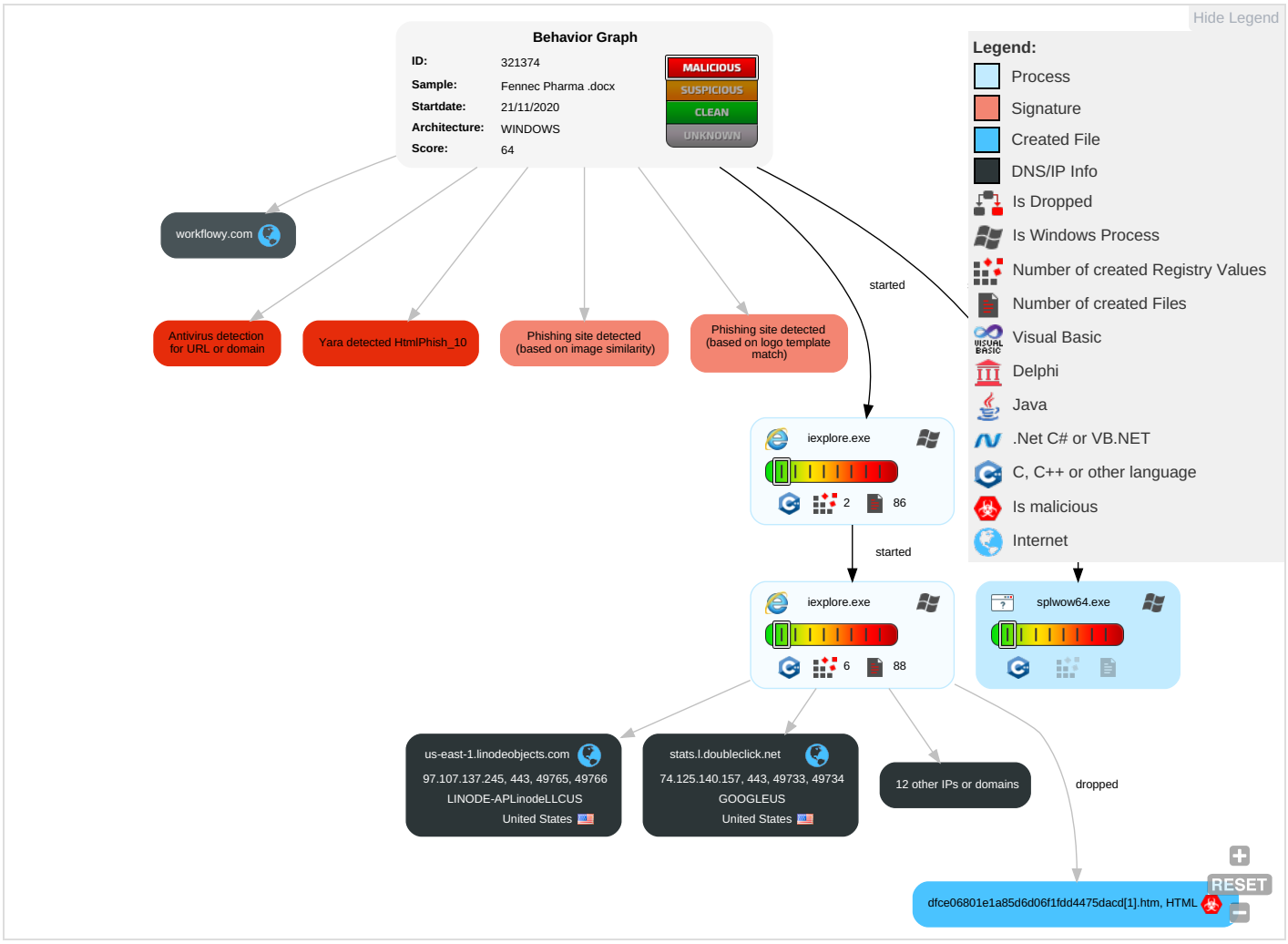
Phishing site detected (based on image similarity)

Phishing site detected (based on logo template match)

Mitre Att&ck Matrix

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

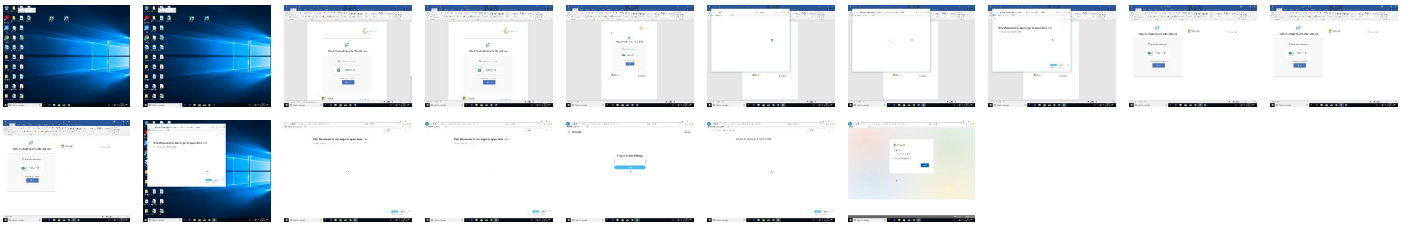
Behavior Graph

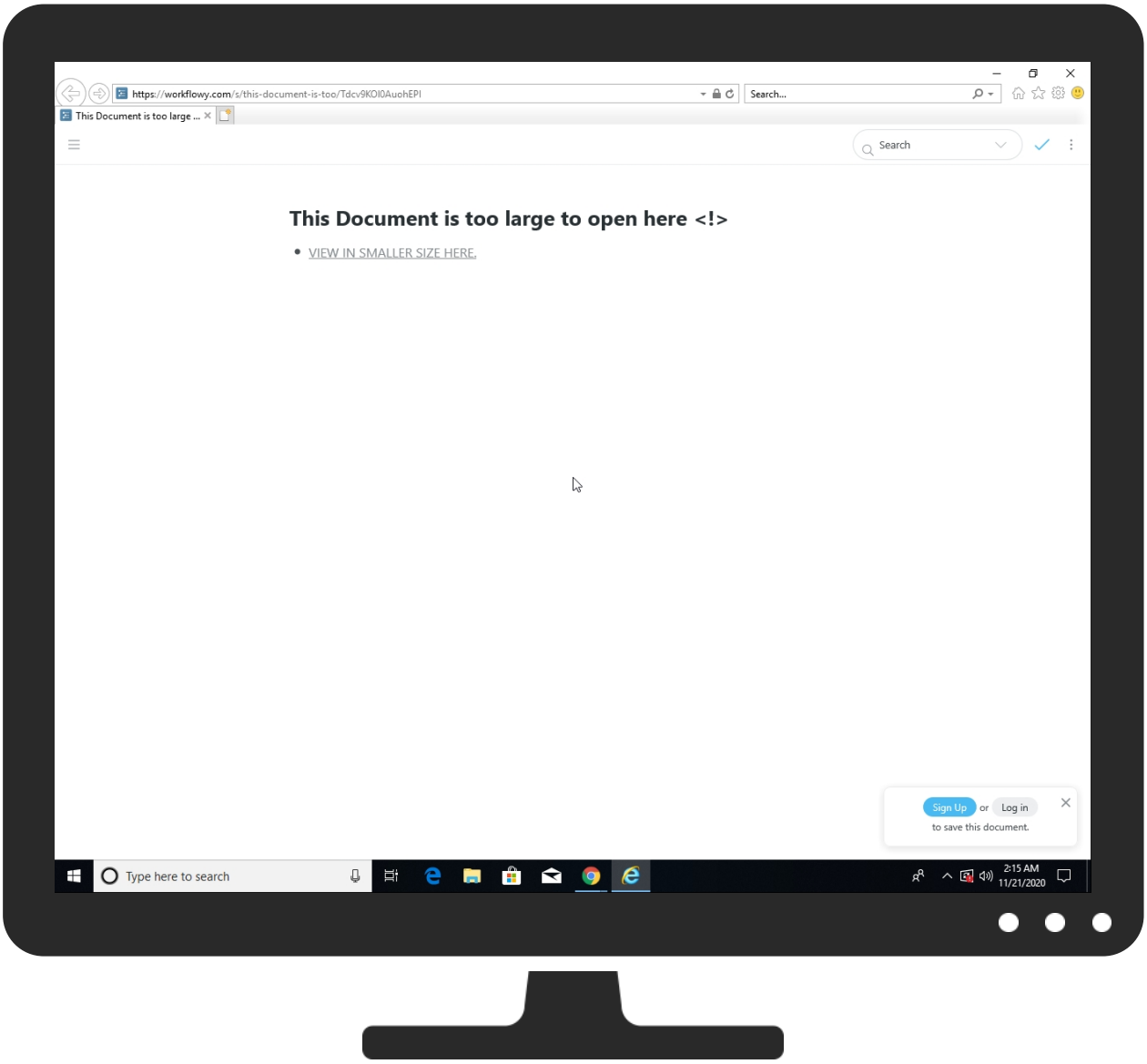


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Fennec Pharma .docx	0%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
us-east-1.linodeobjects.com	0%	Virustotal		Browse
bam-cell.nr-data.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link

Source	Detection	Scanner	Label	Link
http://https://jamif-cdn3d.us-east-1.linodeobjects.com/dfce06801e1a85d6d06f1fdd4475dacd.html	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://https://jamif-cdn3d.us-east-1.linodeobjects.com/dfce06801e1a85d6d06f1fdd4475dacd.html	100%	UrlScan	phishing brand: generic microsoft	Browse
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://fontawesome.comhttps://fontawesome.comFont	0%	Avira URL Cloud	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	Avira URL Cloud	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://ukrainianpolicy.ru/Dee23ope11nov/next.php	0%	Avira URL Cloud	safe	
http://https://www.google.%/ads/ga-audiences?	0%	URL Reputation	safe	
http://https://www.google.%/ads/ga-audiences?	0%	URL Reputation	safe	
http://https://www.google.%/ads/ga-audiences?	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://promisesaplus.com/#point-59	0%	URL Reputation	safe	
http://https://promisesaplus.com/#point-59	0%	URL Reputation	safe	
http://https://promisesaplus.com/#point-59	0%	URL Reputation	safe	
http://https://promisesaplus.com/#point-57	0%	URL Reputation	safe	
http://https://promisesaplus.com/#point-57	0%	URL Reputation	safe	
http://https://promisesaplus.com/#point-57	0%	URL Reputation	safe	
http://https://promisesaplus.com/#point-54	0%	URL Reputation	safe	
http://https://promisesaplus.com/#point-54	0%	URL Reputation	safe	
http://https://promisesaplus.com/#point-54	0%	URL Reputation	safe	
http://https://getbootstrap.com)	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
workflowy.com	54.84.56.113	true	false		high
us-east-1.linodeobjects.com	97.107.137.245	true	false	• 0%, Virustotal, Browse	unknown
s3.amazonaws.com	52.217.4.102	true	false		high
stats.l.doubleclick.net	74.125.140.157	true	false		high
cdnjs.cloudflare.com	104.16.19.94	true	false		high
ka-f.fontawesome.com	unknown	unknown	false		high
code.jquery.com	unknown	unknown	false		high
kit.fontawesome.com	unknown	unknown	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
js-agent.newrelic.com	unknown	unknown	false		high
maxcdn.bootstrapcdn.com	unknown	unknown	false		high
jamif-cdn3d.us-east-1.linodeobjects.com	unknown	unknown	false		unknown
bam-cell.nr-data.net	unknown	unknown	false	• 0%, Virustotal, Browse	unknown
stats.g.doubleclick.net	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://jamif-cdn3d.us-east-1.linodeobjects.com/dfce06801e1a85d6d06f1fdd4475dacd.html	true	• 100%, UrlScan, Browse • SlashNext: Fake Login Page type: Phishing & Social Engineering	unknown
http://https://workflowy.com/signup/?next=/s/this-document-is-too/Tdcv9KOl0AuohEPI	false		high
http://https://workflowy.com/s/this-document-is-too/Tdcv9KOl0AuohEPI#/7686a5f8c6e6	false		high
http://https://workflowy.com/s/this-document-is-too/Tdcv9KOl0AuohEPI	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://workflowy.com/referrals/	document_view.min[1].js.7.dr	false		high
http://https://shell.suite.office.com:1443	CAFA8CBC-8827-49EF-9BA3-5B2EB2C2B7DA.0.dr	false		high
http://https://stats.g.doubleclick.net/g/collect	js[1].js.7.dr	false		high
http://https://code.jquery.com/jquery-3.2.1.slim.min.js	dfce06801e1a85d6d06f1fdd4475dacd[1].htm.7.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	CAFA8CBC-8827-49EF-9BA3-5B2EB2C2B7DA.0.dr	false		high
http://https://cdn.entity.	CAFA8CBC-8827-49EF-9BA3-5B2EB2C2B7DA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	CAFA8CBC-8827-49EF-9BA3-5B2EB2C2B7DA.0.dr	false		high
http://https://web.archive.org/web/20100324014747/blindsignals.com/index.php/2009/07/jquery-delay/	jquery-3.3.1[1].js.7.dr	false		high
http://https://rpsticket.partnerservices.getmicrosoftkey.com	CAFA8CBC-8827-49EF-9BA3-5B2EB2C2B7DA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	CAFA8CBC-8827-49EF-9BA3-5B2EB2C2B7DA.0.dr	false		high
http://https://fontawesome.comhttps://fontawesome.comFont	free-fa-solid-900[1].eot.7.dr, free-fa-regular-400[1].eot.7.dr	false	• Avira URL Cloud: safe	unknown
http://https://html.spec.whatwg.org/multipage/forms.html#concept-fe-disabled	jquery-3.3.1[1].js.7.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	CAFA8CBC-8827-49EF-9BA3-5B2EB2C2B7DA.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	CAFA8CBC-8827-49EF-9BA3-5B2EB2C2B7DA.0.dr	false		high
http://https://api.aadrm.com/	CAFA8CBC-8827-49EF-9BA3-5B2EB2C2B7DA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://infra.spec.whatwg.org/#strip-and-collapse-ascii-whitespace	jquery-3.3.1[1].js.7.dr	false		high
http://https://fontawesome.com	free-v4-shims.min[1].css.7.dr, free-fa-solid-900[1].eot.7.dr	false		high
http://https://workflowy.com/s/this-document-is-too/Tdcv9KOl0AuohEPI	{4F0DC65E-2BE2-11EB-90E4-ECF4BB862DED}.dat.6.dr, ~WRS{FABF639E-4792-4112-BF52-2B5E333F7251}.tmp.0.dr	false		high
http://https://github.com/twbs/bootstrap/graphs/contributors)	bootstrap.min[1].js.7.dr	false		high
http://https://github.com/jrburke/requirejs/wiki/Updating-existing-libraries#wiki-anon	jquery-3.3.1[1].js.7.dr	false		high
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	CAFA8CBC-8827-49EF-9BA3-5B2EB2C2B7DA.0.dr	false		high
http://https://api.microsoftstream.com/api/	CAFA8CBC-8827-49EF-9BA3-5B2EB2C2B7DA.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	CAFA8CBC-8827-49EF-9BA3-5B2EB2C2B7DA.0.dr	false		high
http://https://cr.office.com	CAFA8CBC-8827-49EF-9BA3-5B2EB2C2B7DA.0.dr	false		high
http://https://bugzilla.mozilla.org/show_bug.cgi?id=687787	jquery-3.3.1[1].js.7.dr	false		high
http://https://stats.g.doubleclick.net/j/collect	analytics[1].js.7.dr	false		high
http://https://bugs.chromium.org/p/chromium/issues/detail?id=470258	jquery-3.3.1[1].js.7.dr	false		high
http://https://kit.fontawesome.com/585b051251.js	dfce06801e1a85d6d06f1fdd4475dacd[1].htm.7.dr	false		high
http://https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/js/bootstrap.min.js	dfce06801e1a85d6d06f1fdd4475dacd[1].htm.7.dr	false		high
http://www.reddit.com/	msapplication.xml4.6.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	CAFA8CBC-8827-49EF-9BA3-5B2EB2C2B7DA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	CAFA8CBC-8827-49EF-9BA3-5B2EB2C2B7DA.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	CAFA8CBC-8827-49EF-9BA3-5B2EB2C2B7DA.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://store.office.cn/addinstemplate	CAFA8CBC-8827-49EF-9BA3-5B2EB2C2B7DA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://workflowy.com/s/this-document-is-too/Tdcv9KOl0AuohEPI#/7686a5f8c6e6	{4F0DC65E-2BE2-11EB-90E4-ECF4BB862DED}.dat.6.dr, ~DF36F3C25722F1499C.TMP.6.dr	false		high
http://https://wus2-000.pagecontentsync.	CAFA8CBC-8827-49EF-9BA3-5B2EB2C2B7DA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	CAFA8CBC-8827-49EF-9BA3-5B2EB2C2B7DA.0.dr	false		high
http://https://jamif-cdn3d.us-east-1.linodeobjects.com/dfce06801e1a85d6d06f1fdd4475dacd.html	{4F0DC65E-2BE2-11EB-90E4-ECF4BB862DED}.dat.6.dr, ~DF36F3C25722F1499C.TMP.6.dr	true	• 100%, UrlScan, Browse • SlashNext: Fake Login Page type: Phishing & Social Engineering	unknown
http://https://www.odwebp.svc.ms	CAFA8CBC-8827-49EF-9BA3-5B2EB2C2B7DA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://jsperf.com/getall-vs-sizzle/2	jquery-3.3.1[1].js.7.dr	false		high
http://https://api.powerbi.com/v1.0/myorg/groups	CAFA8CBC-8827-49EF-9BA3-5B2EB2C2B7DA.0.dr	false		high
http://https://web.microsoftstream.com/video/	CAFA8CBC-8827-49EF-9BA3-5B2EB2C2B7DA.0.dr	false		high
http://https://graph.windows.net	CAFA8CBC-8827-49EF-9BA3-5B2EB2C2B7DA.0.dr	false		high
http://https://jquery.com/	jquery-3.3.1[1].js.7.dr	false		high
http://https://stats.g.doubleclick.net/j/collect?	ga[1].js.7.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	CAFA8CBC-8827-49EF-9BA3-5B2EB2C2B7DA.0.dr	false		high
http://https://github.com/twbs/bootstrap/blob/master/LICENSE)	bootstrap.min[1].css.7.dr, bootstrap.min[1].js.7.dr	false		high
http://https://stats.g.doubleclick.net/g/collect?v=2&	js[1].js.7.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	CAFA8CBC-8827-49EF-9BA3-5B2EB2C2B7DA.0.dr	false		high
http://weather.service.msn.com/data.aspx	CAFA8CBC-8827-49EF-9BA3-5B2EB2C2B7DA.0.dr	false		high
http://https://sizzlejs.com/	jquery-3.3.1[1].js.7.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	CAFA8CBC-8827-49EF-9BA3-5B2EB2C2B7DA.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	CAFA8CBC-8827-49EF-9BA3-5B2EB2C2B7DA.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	CAFA8CBC-8827-49EF-9BA3-5B2EB2C2B7DA.0.dr	false		high
http://https://ka-f.fontawesome.com	585b051251[1].js.7.dr	false		high
http://https://bugs.jquery.com/ticket/12359	jquery-3.3.1[1].js.7.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	CAFA8CBC-8827-49EF-9BA3-5B2EB2C2B7DA.0.dr	false		high
http://https://workflowy.com/media/i/favicon.ico	imagestore.dat.7.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	CAFA8CBC-8827-49EF-9BA3-5B2EB2C2B7DA.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://clients.config.office.net/user/v1.0/android/policies	CAFA8CBC-8827-49EF-9BA3-5B2EB2C2B7DA.0.dr	false		high
http://www.amazon.com/	msapplication.xml.6.dr	false		high
http://https://workflowy.com/s/this-document-is-too/Tdcv9KOl0AuohEPInThis	{4F0DC65E-2BE2-11EB-90E4-ECF4BB862DED}.dat.6.dr	false		high
http://https://entitlement.diagnostics.office.com	CAFA8CBC-8827-49EF-9BA3-5B2EB2C2B7DA.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	CAFA8CBC-8827-49EF-9BA3-5B2EB2C2B7DA.0.dr	false		high
http://www.twitter.com/	msapplication.xml5.6.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	CAFA8CBC-8827-49EF-9BA3-5B2EB2C2B7DA.0.dr	false		high
http://https://fontawesome.com/license/free	free-v4-shims.min[1].css.7.dr	false		high
http://https://ukrainianpolicy.ru/Dee23ope11nov/next.php	dfce06801e1a85d6d06f1fdd4475dacd[1].htm.7.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.google.%/ads/ga-audiences?	ga[1].js.7.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://https://github.com/jquery/jquery/pull/557)	jquery-3.3.1[1].js.7.dr	false		high
http://https://bugs.chromium.org/p/chromium/issues/detail?id=378607	jquery-3.3.1[1].js.7.dr	false		high
http://https://graph.windows.net/	CAFA8CBC-8827-49EF-9BA3-5B2EB2C2B7DA.0.dr	false		high
http://https://devnull.onenote.com	CAFA8CBC-8827-49EF-9BA3-5B2EB2C2B7DA.0.dr	false		high
http://https://messaging.office.com/	CAFA8CBC-8827-49EF-9BA3-5B2EB2C2B7DA.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	CAFA8CBC-8827-49EF-9BA3-5B2EB2C2B7DA.0.dr	false		high
http://https://skyapi.live.net/Activity/	CAFA8CBC-8827-49EF-9BA3-5B2EB2C2B7DA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.nytimes.com/	msapplication.xml3.6.dr	false		high
http://https://drafts.csswg.org/cssom/#resolved-values	jquery-3.3.1[1].js.7.dr	false		high
http://https://bugs.chromium.org/p/chromium/issues/detail?id=589347	jquery-3.3.1[1].js.7.dr	false		high
http://https://visio.uservoice.com/forums/368202-visio-on-devices	CAFA8CBC-8827-49EF-9BA3-5B2EB2C2B7DA.0.dr	false		high
http://https://code.jquery.com/jquery-3.1.1.min.js	dfce06801e1a85d6d06f1fdd4475dacd[1].htm.7.dr	false		high
http://https://onedrive.live.com/embed?	CAFA8CBC-8827-49EF-9BA3-5B2EB2C2B7DA.0.dr	false		high
http://https://augloop.office.com	CAFA8CBC-8827-49EF-9BA3-5B2EB2C2B7DA.0.dr	false		high
http://https://html.spec.whatwg.org/multipage/syntax.html#attributes-2	jquery-3.3.1[1].js.7.dr	false		high
http://https://promisesaplus.com/#point-59	jquery-3.3.1[1].js.7.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://promisesaplus.com/#point-57	jquery-3.3.1[1].js.7.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.7.dr	false		high
http://https://promisesaplus.com/#point-54	jquery-3.3.1[1].js.7.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://workflowy.com/s/this-doRoot	{4F0DC65E-2BE2-11EB-90E4-ECF4BB862DED}.dat.6.dr	false		high
http://https://code.jquery.com/jquery-3.3.1.js	dfce06801e1a85d6d06f1fdd4475dacd[1].htm.7.dr	false		high
http://https://html.spec.whatwg.org/multipage/scripting.html#selector-disabled	jquery-3.3.1[1].js.7.dr	false		high
http://https://api.diagnostics.office.com	CAFA8CBC-8827-49EF-9BA3-5B2EB2C2B7DA.0.dr	false		high
http://https://jquery.org/license	jquery-3.3.1[1].js.7.dr	false		high
http://https://store.office.de/addinstemplate	CAFA8CBC-8827-49EF-9BA3-5B2EB2C2B7DA.0.dr	false		high
http://https://getbootstrap.com)	bootstrap.min[1].css.7.dr, bootstrap.min[1].js.7.dr	false	• Avira URL Cloud: safe	low
http://https://api.powerbi.com/v1.0/myorg/datasets	CAFA8CBC-8827-49EF-9BA3-5B2EB2C2B7DA.0.dr	false		high

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
54.84.56.113	unknown	United States		14618	AMAZON-AESUS	false
97.107.137.245	unknown	United States		63949	LINODE-APLinodeLLCUS	false
74.125.140.157	unknown	United States		15169	GOOGLEUS	false
52.217.4.102	unknown	United States		16509	AMAZON-02US	false
104.16.19.94	unknown	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	321374
Start date:	21.11.2020
Start time:	02:12:58
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 36s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Fennec Pharma .docx
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Potential for more IOCs and behavior
Number of analysed new started processes analysed:	27
Number of new started drivers analysed:	0

Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal64.phis.winDOCX@6/77@12/6
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .docx • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Browse link: https://workflowy.com/s/this-document-is-too/Tdcv9KOl0AuohEPI • Scroll down • Close Viewer • Browsing link: https://workflowy.com/signup?next=/s/this-document-is-too/Tdcv9KOl0AuohEPI • Browsing link: https://workflowy.com/login?next=/s/this-document-is-too/Tdcv9KOl0AuohEPI • Browsing link: https://workflowy.com/s/this-document-is-too/Tdcv9KOl0AuohEPI#/7686a5f8c6e6 • Browsing link: https://jamif-cdn3d.us-east-1.linodeobjects.com/dfce06801e1a85d6d06f1fdd4475dacd.html

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 104.43.139.144, 168.61.161.212, 104.43.193.48, 52.109.88.8, 52.109.8.25, 52.109.12.21, 51.104.139.180, 2.20.84.85, 88.221.62.148, 172.217.22.40, 151.101.2.110, 151.101.66.110, 151.101.130.110, 151.101.194.110, 162.247.243.147, 162.247.243.146, 20.54.26.129, 51.104.144.132, 92.122.213.194, 92.122.213.247, 152.199.19.161, 172.217.23.168, 172.217.18.106, 172.217.23.131, 172.217.23.174, 209.197.3.24, 209.197.3.15, 216.58.212.138, 104.18.22.52, 104.18.23.52, 172.64.202.28, 172.64.203.28 • Excluded domains from analysis (whitelisted): gstaticadssl.l.google.com, cds.s5x3j6q5.hwcdn.net, prod-w.nexus.live.com.akadns.net, arc.msn.com.nsatc.net, ka-f.fontawesome.com.cdn.cloudflare.net, tls12.newrelic.com.cdn.cloudflare.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, go.microsoft.com, www.googletagmanager.com, nexus.officeapps.live.com, ssl-google-analytics.l.google.com, officeclient.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, www.google-analytics.com, kit.fontawesome.com.cdn.cloudflare.net, fonts.googleapis.com, fs.microsoft.com, www-google-analytics.l.google.com, ie9comview.vo.msecnd.net, fonts.gstatic.com, ajax.googleapis.com, prod.configsvc1.live.com.akadns.net, db3p-ris-pf-prod-atm.trafficmanager.net, www-googletagmanager.l.google.com, ris-prod.trafficmanager.net, f4.shared.global.fastly.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, skypedataprdcolcus16.cloudapp.net, skypedataprdcolcus15.cloudapp.net, ssl.google-analytics.com, ris.api.iris.microsoft.com, config.officeapps.live.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, cds.j3z9t3p6.hwcdn.net, europe.configsvc1.live.com.akadns.net, cs9.wpc.v0cdn.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtDeviceIoControlFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
02:14:21	API Interceptor	1065x Sleep call for process: splwow64.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
74.125.140.157	activate_36059.EXE	Get hash	malicious	Browse	
	http://https://onedriveonlinemicrosoft.typeform.com/to/EM15DyjP	Get hash	malicious	Browse	
	DriverUpdate-setup-751d8317-4511-4738-aaab-007b6c6dcb5d.exe	Get hash	malicious	Browse	
	http://https://changeanduncertaintyontrustandcyberthreats.splashthat.com/	Get hash	malicious	Browse	
	http://https://isvconstructions.com.au/iso/?p=LFsAXVB1up6wUN57xRREGPHm	Get hash	malicious	Browse	
	http://https://simplebooklet.com/payment1	Get hash	malicious	Browse	
	http://https://bitly.com/34g6lib	Get hash	malicious	Browse	
	http://https://jetsgmbhcom-my.sharepoint.com:443/:b:/g/personal/g_petrova_jetsgmbh_com/Eflus5lYFHBKhp-a3eq9etsBroqnbi9FaLH1uKjHJLoO3Q?e=4%3amUSYs9&at=9	Get hash	malicious	Browse	
	http://pfasdd.fr/abige/	Get hash	malicious	Browse	
	http://https://joom.ag/iFjC	Get hash	malicious	Browse	
	http://ohshub.com/excavation-and-trenching-safety-handout-quiz-answers/	Get hash	malicious	Browse	
	http://https://joom.ag/iFjC	Get hash	malicious	Browse	
	http://https://bit.ly/32VsT8i	Get hash	malicious	Browse	
	http://https://ozobot.com/educate/classroom	Get hash	malicious	Browse	
	http://https://tinyurl.com/yye5b9wx	Get hash	malicious	Browse	
	http://https://youallhavetoactfast.webnode.com/	Get hash	malicious	Browse	
	4524754_tgp.docx	Get hash	malicious	Browse	
	http://https://outlookmicrosoftwo.wixsite.com/upgrade	Get hash	malicious	Browse	
	http://https://www.brighttalk.com/webcast/18362/432178	Get hash	malicious	Browse	
	KutoolsforExcelSetup.exe	Get hash	malicious	Browse	
54.84.56.113	Fennec Pharma .docx	Get hash	malicious	Browse	
	Fennec Pharma.xlsx	Get hash	malicious	Browse	
	Fennec Pharma.xlsx	Get hash	malicious	Browse	
104.16.19.94	http://https://j.mp/38NwiZZ	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://lokalny-biznes.eu/modules/mod_simplefileuploadv1.3/elements/reactivation/indextest.php?youll=enwht11p10sc0&picture=call&please=gave	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://https://pinpoint-insights.com/interx/tracker?op=click&id=107b4.3e3b&url=https%3A%2F%2Fpinpoint-insights.com%2Finterx%2Funsubscribe%3Fid%3D107b4.3e3b%26type%3Dnormal&_hC=D7C07475	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/flickity/1.0.0/flickity.min.css
	http://https://pinpoint-insights.com/interx/tracker?op=click&id=107b4.3e3b&url=https%3A%2F%2Fpinpoint-insights.com%2Finterx%2Funsubscribe%3Fid%3D107b4.3e3b%26type%3Dnormal&_hC=D7C07475	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/flickity/1.0.0/flickity.min.css

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
workflowy.com	Fennec Pharma.xlsx	Get hash	malicious	Browse	• 54.84.56.113
	Fennec Pharma.xlsx	Get hash	malicious	Browse	• 54.84.56.113
s3.amazonaws.com	Fennec Pharma.xlsx	Get hash	malicious	Browse	• 52.217.43.14
	http://https://app.clio.com/link/AxWtfjmmzhja	Get hash	malicious	Browse	• 52.216.134.237
	http://WWW.ALYSSA-J-MILANO.COM	Get hash	malicious	Browse	• 52.216.130.21
	http://https://olhonabrasa.com.br/secure/zimbra/access/zimbra/index.php	Get hash	malicious	Browse	• 52.216.18.35
	http://https://s3.amazonaws.com/atlasox/uni/BAv1106876.msi	Get hash	malicious	Browse	• 54.231.40.66
	http://https://download.winzipdriverupdater.com/wzdu/wzdu53.exe	Get hash	malicious	Browse	• 52.217.106.206
	http://https://ref320.way.live/fx04	Get hash	malicious	Browse	• 52.217.81.190
	Report-doc.11.03.xlsb	Get hash	malicious	Browse	• 52.216.128.181

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://www.google.com/url?q=https://talibllc--c.documentforce.com/sfc/dist/version/download/?oid%3D00D4W0000092RKF%26ids%3D0684W000007pR1HQAU%26d%3D%252Fa%252F4W000000Putz%252Fms_BmovqE_WXkJYztxhvReEhZJLVdobKujH1zudqg3s%26operationContext%3DDELIVERY%26viewId%3D05H4W000000luGyUAI%26dpt%3D&sa=D&ust=1604432432908000&usg=AOvVaw2LctXUh7R_FyT0gHvTDxLU	Get hash	malicious	Browse	• 52.217.103.70
	http://https://chddid13.way.live/1497640082	Get hash	malicious	Browse	• 52.216.249.150
	http://https://messageso.webs.com/	Get hash	malicious	Browse	• 52.216.207.197
cdnjs.cloudflare.com	Fennec Pharma.xlsx	Get hash	malicious	Browse	• 104.16.19.94
	http://https://elharless.github.io/stamapdevmo/tak.html?bbre=oadfis48sd	Get hash	malicious	Browse	• 104.16.18.94
	http://https://albanesebros.sendx.io/lp/shared-doc.html	Get hash	malicious	Browse	• 104.16.19.94
	http://https://xerox879784379923.azureedge.net??#ZGluYS5qb25nZWtyeWdAYWxhc2thYWlyLmNvbQ	Get hash	malicious	Browse	• 104.16.19.94
	http://https://faxfax.zizera.com/remittanceadvice	Get hash	malicious	Browse	• 104.16.18.94
	http://https://flyboyfurnishings.com/firstam/RD-FITT	Get hash	malicious	Browse	• 104.16.18.94
	http://ec.autohonda.it	Get hash	malicious	Browse	• 104.16.19.94
	http://https://mcmms.typeform.com/to/Vtnb9OBC	Get hash	malicious	Browse	• 104.16.19.94
	http://www.portal.office.com.s3-website.us-east-2.amazonaws.com#p.steinberger@wafra.com	Get hash	malicious	Browse	• 104.16.19.94
	http://https://storage.googleapis.com/storesll0f4bb6d9b7f964569155d2bb42628/a83416219a20d87f4dabde9f057f93b5.html#p.steinberger@wafra.com	Get hash	malicious	Browse	• 104.16.19.94
	http://https://largemail.r1.rpost.net/files/7xU97qcFgCvB3Uv1wDC4qvS2ZriLfublohKWA5V3/ln/en-us	Get hash	malicious	Browse	• 104.16.18.94
	http://https://eagleeyeproduce-my.sharepoint.com/:o:/p/mckrayp/EtopxtQDn3pOqhvY4g_gG3ABKX9ornSoGNhGOLIXyaU89Q?e=Ee0wW2	Get hash	malicious	Browse	• 104.16.19.94
	http://https://certified1.box.com/s/2ta9r7cyn5g09fblryd9xqqpnfxbjqej	Get hash	malicious	Browse	• 104.16.19.94
	http://s1022.t.en25.com/e/er?s=1022&lid=2184&elqTrackId=BEDFF87609C7D9DEAD041308DD8FFFB8&lb_email=bkirwer%40farbestfoods.com&elq=b095bd096fb54161953a2cf8316b5d13&elqaid=3115&elqat=1	Get hash	malicious	Browse	• 104.16.18.94
	http://https://trondiamond.co/OMMOM/OM9u8	Get hash	malicious	Browse	• 104.16.18.94
	http://https://go.pardot.com/e/395202/siness-insights-dashboard-html/bnmpz6/1446733421?h=AwLDfNsCVbkjEN13pzY-7AXMPolL_XMigGsJSppGaiM	Get hash	malicious	Browse	• 104.16.19.94
	http://https://app.box.com/s/gdf36roak3w2fc52cgfbxuq651p0zehy	Get hash	malicious	Browse	• 104.16.18.94
	http://septterror.tripod.com/the911basics.html	Get hash	malicious	Browse	• 104.16.19.94
	http://https://my.freshbooks.com/#/link/eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJzeXN0ZW1pZCI6OTQ3OTM1LCJ1c2VyaWQiOjYzNDYyNywidHlwZSI6Imludm9pY2UiLCJvYmplY3RpZCI6Mjg4MjQ0OSwiZXhwIjoxNjM3MjY5MTgxLCJsZXZlbCI6MH0.DGVcXxdiwtgxTUka4TzPi_o6GS8zH-kvvTnFJZxapLg?companyName=Amanda&invoiceNumber=00007767&ownerEmail=avigilante%40maxburst.com&type=primary	Get hash	malicious	Browse	• 104.16.18.94
	http://45.95.168.116	Get hash	malicious	Browse	• 104.16.19.94
stats.l.doubleclick.net	Fennec Pharma .docx	Get hash	malicious	Browse	• 74.125.140.156
	activate_36059.EXE	Get hash	malicious	Browse	• 74.125.140.157
	Fennec Pharma.xlsx	Get hash	malicious	Browse	• 74.125.140.154
	Fennec Pharma.xlsx	Get hash	malicious	Browse	• 74.125.140.154
	http://www.openair.com	Get hash	malicious	Browse	• 74.125.140.154
	http://https://largemail.r1.rpost.net/files/7xU97qcFgCvB3Uv1wDC4qvS2ZriLfublohKWA5V3/ln/en-us	Get hash	malicious	Browse	• 108.177.15.155
	http://s1022.t.en25.com/e/er?s=1022&lid=2184&elqTrackId=BEDFF87609C7D9DEAD041308DD8FFFB8&lb_email=bkirwer%40farbestfoods.com&elq=b095bd096fb54161953a2cf8316b5d13&elqaid=3115&elqat=1	Get hash	malicious	Browse	• 108.177.15.155
	http://global.krx.co.kr/board/GLB0205020100/bbs#view=649	Get hash	malicious	Browse	• 108.177.15.155
	http://https://www.canva.com/design/DAEN9RlD8Vk/acBvt6UoL-DafjXmQk38pA/view?utm_content=DAEN9RlD8Vk&utm_campaign=designshare&utm_medium=link&utm_source=publishsharelink	Get hash	malicious	Browse	• 108.177.15.156
	http://WWW.ALYSSA-J-MILANO.COM	Get hash	malicious	Browse	• 108.177.15.156
	http://www.marcusevans.com	Get hash	malicious	Browse	• 108.177.15.154
	http://septterror.tripod.com/the911basics.html	Get hash	malicious	Browse	• 108.177.15.155

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://tgcdevgroup-my.sharepoint.com/:b:/g/personal/jmoore_tgcgroup_net/EcgJdwLEdb9OriDBRaw9slAB4_8AMjn68ZCbL_ahHtwjlA?e=4%3a8pEDtO&at=9	Get hash	malicious	Browse	• 108.177.15.157
	http://45.95.168.116	Get hash	malicious	Browse	• 108.177.15.156
	http://https://www.canva.com/design/DAEN3YdYVHw/zaVHWoDx-9G9l20JXWSBtg/view?utm_content=DAEN3YdYVHw&utm_campaign=designshare&utm_medium=link&utm_source=sharebutton	Get hash	malicious	Browse	• 108.177.15.155
	http://https://www.canva.com/design/DAENqED8UzU/0m_RcAQIILTwa79MyPG8KA/view?utm_content=DAENqED8UzU&utm_campaign=designshare&utm_medium=link&utm_source=sharebutton	Get hash	malicious	Browse	• 108.177.119.155
	http://www.ericbess.com/ericblog/2008/03/03/wp-codebox/#examples	Get hash	malicious	Browse	• 108.177.119.154
	http://https://www.vedansha.com/doc/office/LatestLOGOOfficeEncoded/LatestLOGOOfficeEncoded/RedirectPage/marc.loney@navitas.com	Get hash	malicious	Browse	• 108.177.119.154
	http://https://olhonabrasa.com.br/secure/zimbra/access/zimbra/index.php	Get hash	malicious	Browse	• 108.177.15.154
	http://https://www.canva.com/design/DAEN4Gk1aAs/uErgK6sn3gPozGMXWtYgqA/view?utm_content=DAEN4Gk1aAs&utm_campaign=designshare&utm_medium=link&utm_source=sharebutton	Get hash	malicious	Browse	• 108.177.15.157

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AMAZON-AESUS	Fennec Pharma .docx	Get hash	malicious	Browse	• 54.84.56.113
	Fennec Pharma.xlsx	Get hash	malicious	Browse	• 54.84.56.113
	Fennec Pharma.xlsx	Get hash	malicious	Browse	• 54.84.56.113
	http://https://albanesebros.sendx.io/lp/shared-doc.html	Get hash	malicious	Browse	• 3.213.165.33
	http://www.openair.com	Get hash	malicious	Browse	• 34.202.206.65
	http://https://faxfax.zizera.com/remittanceadvice	Get hash	malicious	Browse	• 184.73.218.177
	http://webnavigator.co	Get hash	malicious	Browse	• 34.235.7.64
	http://https://mcmms.typeform.com/to/Vtnb9OBC	Get hash	malicious	Browse	• 34.200.62.85
	yQDGREHA9h.exe	Get hash	malicious	Browse	• 54.235.83.248
	mcsrXx9lfD.exe	Get hash	malicious	Browse	• 54.235.83.248
	SecuriteInfo.com.Trojan.PackedNET.461.20928.exe	Get hash	malicious	Browse	• 23.21.42.25
	Defender-update-kit-x86x64.exe	Get hash	malicious	Browse	• 54.225.153.147
	http://https://largemail.r1.rpost.net/files/7xU97qcFgCvB3Uv1wDC4qvS2ZriLfublohKWA5V3/ln/en-us	Get hash	malicious	Browse	• 54.225.66.103
	ORDER.exe	Get hash	malicious	Browse	• 54.235.142.93
	http://s1022.t.en25.com/e/er?s=1022&lid=2184&elqTrackId=BEDFF87609C7D9DEAD041308DD8FFFB8&lb_email=bkirwer%40farbestfoods.com&elq=b095bd096fb54161953a2cf8316b5d13&elqaid=3115&elqat=1	Get hash	malicious	Browse	• 52.1.99.77
	Bill # 2.xlsx	Get hash	malicious	Browse	• 23.21.42.25
	http://https://ubereats.app.link/cwmLFZfMz5?%243p=a_custom_354088&%24deeplink_path=promo%2Fapply%3FpromoCode%3DRECONFORT7&%24desktop_url=tracking.spectrumemp.com/el?aid=8feeb968-bdd0-11e8-b27f-22000be0a14e&rid=50048635&pid=285843&cid=513&dest=overlordscan.com/cmV0by5tZXR6bGVyQGlzb2x1dGlvbnMuY2g=%23#kkowfocjoyuynaip#	Get hash	malicious	Browse	• 35.170.181.205
	BANK ACCOUNT INFO!.exe	Get hash	malicious	Browse	• 107.22.223.163
	PO1.xlsx	Get hash	malicious	Browse	• 174.129.214.20
	http://https://rebrand.ly/zkp0y	Get hash	malicious	Browse	• 54.227.164.140
AMAZON-02US	activate_36059.EXE	Get hash	malicious	Browse	• 13.224.93.99
	Fennec Pharma.xlsx	Get hash	malicious	Browse	• 52.217.43.14
	http://https://albanesebros.sendx.io/lp/shared-doc.html	Get hash	malicious	Browse	• 13.224.93.76
	http://www.openair.com	Get hash	malicious	Browse	• 13.224.93.99
	http://https://faxfax.zizera.com/remittanceadvice	Get hash	malicious	Browse	• 34.255.187.247
	http://https://flyboyfurnishings.com/firstam/RD-FITT	Get hash	malicious	Browse	• 13.224.93.52
	http://webnavigator.co	Get hash	malicious	Browse	• 52.210.174.128
	http://https://mcmms.typeform.com/to/Vtnb9OBC	Get hash	malicious	Browse	• 13.224.93.121

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://t.e.vailresorts.com/r/?id=hda0e43a,3501a2a,3501f68&VRI_v73=c2F1bWlsLnNoYWhAYXJtLmNvbQ==&cmpid=EML_SNOWALRT_OTHR_000_NW_00_00000_000000_000000_20200110_v01&p1=www.snow.com%40g-em.xyz	Get hash	malicious	Browse	• 52.12.33.145
	vOKMFxiCYt.exe	Get hash	malicious	Browse	• 3.138.72.189
	http://microsoftonlineofficeteam.weebly.com	Get hash	malicious	Browse	• 35.163.165.143
	ACH & WIRE REMITTANCE ADVICE.xlsx	Get hash	malicious	Browse	• 52.33.162.26
	ACH & WIRE REMITTANCE ADVICE.xlsx	Get hash	malicious	Browse	• 143.204.201.83
	http://www.portal.office.com.s3-website.us-east-2.amazonaws.com#p.steinberger@wafra.com	Get hash	malicious	Browse	• 52.219.102.33
	http://https://protect-us.mimecast.com/s/eKI8CjRMnyCnG2lvSW3aOv?domain=document-efw5.zizera.com	Get hash	malicious	Browse	• 143.204.201.92
	http://https://t.e.vailresorts.com	Get hash	malicious	Browse	• 35.164.67.102
	http://https://largemail.r1.rpost.net/files/7xU97qcFgCvB3Uv1wDC4qvS2ZriLfublohKWA5V3/ln/en-us	Get hash	malicious	Browse	• 52.58.5.168
	http://https://t.e.vailresorts.com/r/?id=hda0e43a,3501a2a,3501f68&VRI_v73=YnJlbmRhLmNvcGVsYW5kQHN0ZXViZW50cnVzdC5jb20=&cmpid=EML_SNOWALRT_OTHR_000_NW_00_00000_000000_000000_20200110_v01&p1=www.snow.com%40h-is.xyz	Get hash	malicious	Browse	• 35.164.67.102
	http://s1022.t.en25.com/e/er?s=1022&lid=2184&elqTrackId=BEDFF87609C7D9DEAD041308DD8FFFB8&lb_email=bkirwer%40farbestfoods.com&elq=b095bd096fb54161953a2cf8316b5d13&elqaid=3115&elqat=1	Get hash	malicious	Browse	• 13.224.100.124
	http://https://ubereats.app.link/cwmLFZfMz5?%243p=a_custom_354088&%24deeplink_path=promo%2Fapply%3FpromoCode%3DRECONFORT7&%24desktop_url=tracking.spectrumemp.com/el?aid=8feeb968-bdd0-11e8-b27f-22000be0a14e&rid=50048635&pid=285843&cid=513&dest=overlordscan.com/cmV0by5tZXR6bGVyQGlzb2x1dGlvbnMuY2g=%23#kkowfocjoyuynaip#	Get hash	malicious	Browse	• 13.224.93.92
GOOGLEUS	Fennec Pharma .docx	Get hash	malicious	Browse	• 74.125.140.156
	activate_36059.EXE	Get hash	malicious	Browse	• 172.217.16.193
	Fennec Pharma.xlsx	Get hash	malicious	Browse	• 74.125.140.154
	Fennec Pharma.xlsx	Get hash	malicious	Browse	• 74.125.140.154
	http://https://elharless.github.io/stamapdevmo/tak.html?bbre=oadfis48sd	Get hash	malicious	Browse	• 172.217.21.193
	http://www.openair.com	Get hash	malicious	Browse	• 172.217.16.194
	http://https://faxfax.zizera.com/remittanceadvice	Get hash	malicious	Browse	• 142.250.74.194
	http://ec.autohonda.it	Get hash	malicious	Browse	• 172.217.23.161
	ING.apk	Get hash	malicious	Browse	• 172.217.23.170
	bot.apk	Get hash	malicious	Browse	• 216.58.212.174
	ING_.apk	Get hash	malicious	Browse	• 216.58.212.174
	http://https://mcmms.typeform.com/to/Vtnb9OBC	Get hash	malicious	Browse	• 172.217.22.34
	NQQWym075C.exe	Get hash	malicious	Browse	• 34.102.136.180
	vOKMFxiCYt.exe	Get hash	malicious	Browse	• 34.102.136.180
	com.fdhgkjhrtjkjbx.model.apk	Get hash	malicious	Browse	• 216.58.212.163
	http://www.portal.office.com.s3-website.us-east-2.amazonaws.com#p.steinberger@wafra.com	Get hash	malicious	Browse	• 172.217.16.193
	http://https://storage.googleapis.com/storesll0f4bb6d9b7f964569155d2bb42628/a83416219a20d87f4dabde9f057f93b5.html#p.steinberger@wafra.com	Get hash	malicious	Browse	• 172.217.16.193
	http://https://docs.google.com/document/d/e/2PACX-1vS19QxlBmfgZPBsUyM3LjkhvVA-TJ0Z_P3J8f_cqg7VN4_zRcrthLeTjZzAubcBh9YWnC0ty3FtmofH/pub	Get hash	malicious	Browse	• 172.217.16.193
	http://https://sites.google.com/site/id500800931/googledrive/share/downloads/storage?FID=6937265496484	Get hash	malicious	Browse	• 172.217.16.193
	http://https://docs.google.com/document/d/e/2PACX-1vSF_0NxJ4W_JaHZNaHV7imTfN6FtP563leR3WEEVqre35gDV9YM55P9l-6Y-B1gmL7J7GW--QSF89LQ/pub	Get hash	malicious	Browse	• 172.217.16.193
LINODE-APLinodeLLCUS	Fennec Pharma.xlsx	Get hash	malicious	Browse	• 45.79.137.127
	http://https://t.e.vailresorts.com/r/?id=h1bac782d,59eb410,55e61f1&VRI_v73=96008558&cmpid=EML_OPENDAYS_RESO_000_OK_SR_REN1Y_000000_TG0001_20201118_V00_EX001_LOCA_ANN_00000_000	Get hash	malicious	Browse	• 45.79.189.238
	BYRkah8GsZ.exe	Get hash	malicious	Browse	• 178.79.134.144
	Quotation Request-RFQ#2020-11-19.exe	Get hash	malicious	Browse	• 139.162.21.249
	SWIFT_HSBC Bank.exe	Get hash	malicious	Browse	• 45.33.2.79

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://customer.cartech.com/inventory_manufacturing.cfm	Get hash	malicious	Browse	• 96.126.117.62
	ShippingDoc.jar	Get hash	malicious	Browse	• 23.239.31.129
	baf6b9fcec491619b45c1dd7db56ad3d.exe	Get hash	malicious	Browse	• 104.200.21.25
	LQehPYZp3c.exe	Get hash	malicious	Browse	• 198.74.50.235
	45g7l63ZII.exe	Get hash	malicious	Browse	• 45.56.111.241
	35xLEdpG78.exe	Get hash	malicious	Browse	• 45.56.111.241
	GLN3AV6KhN.exe	Get hash	malicious	Browse	• 139.162.1.137
	2ocLlNcGe8.exe	Get hash	malicious	Browse	• 45.56.111.241
	XgDDVAxhZU.exe	Get hash	malicious	Browse	• 176.58.123.25
	p8LV1eVFyO.exe	Get hash	malicious	Browse	• 104.200.21.25
	6TQMq6JTWW.exe	Get hash	malicious	Browse	• 176.58.104.168
	feJbFA6woA.exe	Get hash	malicious	Browse	• 96.126.123.244
	hlDQ6vR2zn.exe	Get hash	malicious	Browse	• 45.56.127.13
	WeV32WScnY.exe	Get hash	malicious	Browse	• 139.162.1.137
	qkN4OZWFG6.exe	Get hash	malicious	Browse	• 45.33.30.74

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
9e10692f1b7f78228b2d4e424db3a98c	http://https://saadellefurniture.com.au/CD/out/	Get hash	malicious	Browse	• 54.84.56.113 • 74.125.140.157 • 97.107.137.245 • 104.16.19.94
	Fennec Pharma.xlsx	Get hash	malicious	Browse	• 54.84.56.113 • 74.125.140.157 • 97.107.137.245 • 104.16.19.94
	http://https://albanesebros.sendx.io/lp/shared-doc.html	Get hash	malicious	Browse	• 54.84.56.113 • 74.125.140.157 • 97.107.137.245 • 104.16.19.94
	http://https://xerox879784379923.azureedge.net??#ZGluYS5qb25nZWtyeWdAYWxhc2thYWlyLmNvbQ	Get hash	malicious	Browse	• 54.84.56.113 • 74.125.140.157 • 97.107.137.245 • 104.16.19.94
	http://https://flyboyfurnishings.com/firstam/RD-FITT	Get hash	malicious	Browse	• 54.84.56.113 • 74.125.140.157 • 97.107.137.245 • 104.16.19.94
	http://ec.autohonda.it	Get hash	malicious	Browse	• 54.84.56.113 • 74.125.140.157 • 97.107.137.245 • 104.16.19.94
	http://webnavigator.co	Get hash	malicious	Browse	• 54.84.56.113 • 74.125.140.157 • 97.107.137.245 • 104.16.19.94
	http://www.947947.mirramodaintima.com.br/#aHR0cHM6Ly9lbXl0dXJrLmNvbS9zZC9JSy9vZjEvRmlkZWwuVG9ycmVzQHNlYXJzaGMuY29t	Get hash	malicious	Browse	• 54.84.56.113 • 74.125.140.157 • 97.107.137.245 • 104.16.19.94
	http://https://t.e.vailresorts.com/r/?id=hda0e43a,3501a2a,3501f68&VRI_v73=c2F1bWlsLnNoYWhAYXJtLmNvbQ==&cmpid=EML_SNOWALRT_OTHR_000_NW_00_00000_000000_000000_20200110_v01&p1=www.snow.com%40g-em.xyz	Get hash	malicious	Browse	• 54.84.56.113 • 74.125.140.157 • 97.107.137.245 • 104.16.19.94
	http://microsoftonlineofficeteam.weebly.com	Get hash	malicious	Browse	• 54.84.56.113 • 74.125.140.157 • 97.107.137.245 • 104.16.19.94
	ACH & WIRE REMITTANCE ADVICE.xlsx	Get hash	malicious	Browse	• 54.84.56.113 • 74.125.140.157 • 97.107.137.245 • 104.16.19.94
	SecuriteInfo.com.Trojan.GenericKD.35280757.18070.dll	Get hash	malicious	Browse	• 54.84.56.113 • 74.125.140.157 • 97.107.137.245 • 104.16.19.94
	http://https://docs.google.com/document/d/e/2PACX-1vS19QxlBmfgZPBsUyM3LjkhvVA-TJ0Z_P3J8f_cqg7VN4_zRcrthLeTjZzAubcBh9YWnC0ty3FtmofH/pub	Get hash	malicious	Browse	• 54.84.56.113 • 74.125.140.157 • 97.107.137.245 • 104.16.19.94
	http://rwiqipwvnklaqkuu.ltiliqhting.com/asci/SmFjcXVlbGluZS5TY2hyYWRlckByYWJvYmFuay5jb20=	Get hash	malicious	Browse	• 54.84.56.113 • 74.125.140.157 • 97.107.137.245 • 104.16.19.94

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://37.1.220.206/bTcpkT?subacc=manualen2015&subacc2=m.inmanuals.com&subacc3=inmanuals.com&keyword=Fall%20Trivia%20Questions%20And%20Answers&site=	Get hash	malicious	Browse	• 54.84.56.113 • 74.125.140.157 • 97.107.137.245 • 104.16.19.94
	http://https://bakrisoil.com/wp-content/cd.php?e=gjeffries@hughesellard.com	Get hash	malicious	Browse	• 54.84.56.113 • 74.125.140.157 • 97.107.137.245 • 104.16.19.94
	Payment conflict- aptiv 082920134110.htm	Get hash	malicious	Browse	• 54.84.56.113 • 74.125.140.157 • 97.107.137.245 • 104.16.19.94
	http://https://aanqylta.com/42/ac/7f/42ac7faefbb3c959ec74f8c07898a6eb.js	Get hash	malicious	Browse	• 54.84.56.113 • 74.125.140.157 • 97.107.137.245 • 104.16.19.94
	http://https://docs.google.com/document/d/e/2PACX-1vSF_0NxJ4W_JaHZNaHV7imTfN6FtP563leR3WEEVqre35gDV9YM55P9l-6Y-B1gmL7J7GW--QSF89LQ/pub	Get hash	malicious	Browse	• 54.84.56.113 • 74.125.140.157 • 97.107.137.245 • 104.16.19.94
	http://https://t.e.vailresorts.com	Get hash	malicious	Browse	• 54.84.56.113 • 74.125.140.157 • 97.107.137.245 • 104.16.19.94
3faf2df7ab96c36419c31725cb1fa7d6	http://septterror.tripod.com/the911basics.html	Get hash	malicious	Browse	• 52.217.4.102
	http://https://olhonabrasa.com.br/secure/zimbra/access/zimbra/index.php	Get hash	malicious	Browse	• 52.217.4.102
	http://https://svlxltppmh.objects-us-east-1.dream.io/link.html#qs=r-aggieaidcjkdfieaefhkbhbaekgeckfaehehfabababackadbbaccacbidacfheaiebhiacb	Get hash	malicious	Browse	• 52.217.4.102
	http://app.eq.intuit.com/e/er?s=113755760&lid=62441&elqTrackId=4b615073902b48dc9d66fc98052408f2&elq=cbdf3bcb965644b38a2e3ce069e60868&elqaid=27000&elqat=1	Get hash	malicious	Browse	• 52.217.4.102
	http://151.80.37.64/exploit/description/34365	Get hash	malicious	Browse	• 52.217.4.102
	http://email.b.kajabimail.net/c/eJwlUEtrwzAY-zXJZSTY_mLHPuTQBx2DwV6wjl7C59fixklK4o51v34ZAyEdBEKSbQgAoMxDwwgjlFJGVVWDLGkp5WYnd5IpIZTYS5lVRJc9nlGHAUMsR5fyrgFVi0pxLal1q1ZWAxgORKD3SlGex6ZL6bJksMnYYQUO-DONhQ4xFt5pWg63_9DSTMPqO73SdtPV2_N0PB1ph8dvf7p_X_DjFM0YPR5fl8cX8xSkei4KairNPTDwQCrhhNJG1ZY7LxlzEo1FSThymcFh6cOlNTGYvk0zmj6Mnxns03x1uftb1FoXw5ebb22wTUEBFCFU0CqfG2siullP17S-YK_JdBFHe4m4pGCWv-Z5at5CcncP-4wB5UQx8gsXp2u0	Get hash	malicious	Browse	• 52.217.4.102
	PO AJ155.xlsx.html	Get hash	malicious	Browse	• 52.217.4.102
	http://geelongmartialarts.com/timetable/	Get hash	malicious	Browse	• 52.217.4.102
	http://https://peraichi.com/landing_pages/expergy1	Get hash	malicious	Browse	• 52.217.4.102
	http://https://luacclibrary-my.sharepoint.com/:b:/g/personal/polson_luacc_com/EfAoFE3NqkFOtaxmNOJG-7cBczwxxIkQeEoohauxLQl30g?e=RpwCpr	Get hash	malicious	Browse	• 52.217.4.102
	http://https://luacclibrary-my.sharepoint.com/:b:/g/personal/polson_luacc_com/EfAoFE3NqkFOtaxmNOJG-7cBczwxxIkQeEoohauxLQl30g?e=RpwCpr	Get hash	malicious	Browse	• 52.217.4.102
	http://https://pellalibrary.s3.us-east-2.amazonaws.com/redirect.html	Get hash	malicious	Browse	• 52.217.4.102
	http://slimware.com	Get hash	malicious	Browse	• 52.217.4.102
	http://https://ref320.way.live/fx04	Get hash	malicious	Browse	• 52.217.4.102
	http://https://u7456750.ct.sendgrid.net/ls/click?upn=lUSUFKorb51gKWUmtJS0SUAaMaat8JGkwiwrkX8swkynuckR14hSzV2yHmMU8fyrZlj2J4EvFZDC47QQd31H2fALJB9Qi6Lfd7rmFhLkmVBJkaMOjkDoZYzoBhYbycxMV8R-2FEOsIqSc8JOmtFPLeIvgplWzYuqQ82vRY97rfv5AWMeGD61lwL1AeVQOwtBM-2FPyDocDNWBc-2F2BfzdJ2wvXBZIVIvobYfdIve-2BldJs7BMbsSMbTw5M9KpL-2B7aSATPgTT0BSHkOBE5X8jTa2BVKMJ0-2FcG4qPdH6ly85YXDKYMbaMu5GiSD4TPZVPfzwSC2onD8emo1zO1lKQr4iO-2F8xAccitDHiD43l6fEg14UWQHw-3DZFm1_GCYjay1OXPdBLKXxEX9Ib1Ow9nCAa6dczU4ILWaYrl7rCU2QinUi3GIcLzsbvdEmF-2BeD9PTudAX458IMPTFSnAb6ttoaOHulatODILcch6TYq-2Fn-2BwEwCLnX1LC8AU86jOkJkpggjd4TlyPmJG6xN-2BRL74BtzxC7VJTmRlqsQWFANODrbTLMNUjYTjXRBO21FvxTt7n9Jhf-2FuwIsMzJPcVA-3D-3D	Get hash	malicious	Browse	• 52.217.4.102

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://u17481766.ct.sendgrid.net/ls/click?upn=PkfwU1WgH-2Byme0WKBjBdm5v4r4hDbgElBrLwHBahCnfkVWJRMoWDpmB-2BBsizyDw-2FF2JS7W17bZQQK13rYiiNJ4EtZPAXowi-2Bq6xtGB9CxHOWKVwqh9G1ep6UNE6zIoHrnTXvMvCw4d8hk9U1CQHPLLRgSSzEQ-2FhdksTFLXBnAw1TeY3sOMRyhu1CgpJxjPja45N5paVHIbtbAaqUEfIWmHIZDfI69yZX7e-2BVHXvIfx7RXsiMQIUJi06D2eZPCRthhxSDQuLN0AI19dNrDmgkzZQbovZQ5sKXIpJEGwlZ8bY-3Dendb_iPqbxG6-2Bi15Gs56F-2B4973ZUXSS-2BM8ZTRSw-2FGxc25rci5TZ50eWy6QvH4CtHo1Wk6U1Ca4R7ZvMqDo96awxs1aMxX7kQatVQRjwP9uxVCvUizbx2duQlr-2FxpyCxoNZSZE8wwC5pjFuHw4XtVEpCUWWoKZCUzxr8Ma3a-2Bg7U4NZjr-2FPRkuq1HYD4ACx-2FMy6a7UbEcz3U9-2BjqZ9zzlGN285tWcFbaXydtJa1HUW12Vgl8o-3D	Get hash	malicious	Browse	• 52.217.4.102
	http://https://s3.us-east-2.amazonaws.com/www1.microsoft.com/inAAi33.html?8ecb955250c4269c374b34c7ba11ae94a5dc1533b6a019e7f2b778630d5a8b97?%20a83416219a20d87f4dabde9f057f93b5	Get hash	malicious	Browse	• 52.217.4.102
	http://https://shahebwouwihw0h3oa8982es7s0eps30tpn2i.s3.ap-northeast-2.amazonaws.com/index.html#jeff.small@windstream.com	Get hash	malicious	Browse	• 52.217.4.102
	http://https://shahebwouwihw0h3oa8982es7s0eps30tpn2i.s3.ap-northeast-2.amazonaws.com/index.html#jeff.small@windstream.com	Get hash	malicious	Browse	• 52.217.4.102
	http://https://shahebwouwihw0h3oa8982es7s0eps30tpn2i.s3.ap-northeast-2.amazonaws.com/index.html#jeff.small@windstream.com	Get hash	malicious	Browse	• 52.217.4.102

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\PTS75JZM\workflowy[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4788
Entropy (8bit):	5.051165812167868
Encrypted:	false
SSDEEP:	96:OpNpzF7FNpzF7FIRNpzF7FIRyKNpzF7FIRyKpjNpzF7FIRyKpjNpTzF7FIRyKpjF:ODr8KMMUzT
MD5:	A1411AA07780568CD5711800F7F09AC3
SHA1:	86D7F27E0BE5C896CE8A857FB6E389935FE07864
SHA-256:	5778769699A20C2F3879E281094E1E7FC60C5F8E5F01D5B9943B00540DA2DADC
SHA-512:	C999600D4F3BA6F521CB12CA75D729F8E74E85FC2C515A9005657E5CDBBED3FC3346AD6D9FA87517D43BFBBE5D4DC158430EFB246279AA5986FDCD6B278BEF4
Malicious:	false
Reputation:	low
Preview:	<root></root><root><item name="mostRecentlyOpenedWindowId" value="1605953660628-0.22457293537327844" ltime="335802720" htime="30851055" /></root><root><item name="mostRecentlyOpenedWindowId" value="1605953660628-0.22457293537327844" ltime="335802720" htime="30851055" /><item name="userstorage.user_id" value="-1" ltime="339842720" htime="30851055" /><item name="userstorage.format_version" value="3" ltime="339842720" htime="30851055" /></root><root><item name="mostRecentlyOpenedWindowId" value="1605953660628-0.22457293537327844" ltime="335802720" htime="30851055" /><item name="userstorage.user_id" value="-1" ltime="339842720" htime="30851055" /><item name="userstorage.format_version" value="3" ltime="339842720" htime="30851055" /><item name="userstorage.appcache_id" value="2020-11-21 01:14:18.436031" ltime="339882720" htime="30851055" /></root><root><item name="mostRecentlyOpenedWindowId" value="1605953660628-0.22457293537327844" ltime="335802720" htime="30851055" /><item name="userstora

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{4F0DC65C-2BE2-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	33368
Entropy (8bit):	1.8741027890396582
Encrypted:	false
SSDEEP:	192:rcZjZ82A9W79t7MLf7gJ06M8c6N+gwc6bbtMJBK3:rclLAULoLO078c6N+gwc6bZWB2
MD5:	612D47B043A6F99869C8166C6234DB9F

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{4F0DC65C-2BE2-11EB-90E4-ECF4BB862DED}.dat	
SHA1:	CC9E2DD5C3BFCEB8CDE91787774380028A8FA73D
SHA-256:	137E4D24187FA5669AC36120A7D029BF2A43FEC5398B8257F4FFF22BC926F9F0
SHA-512:	1916238EBBD752C310676FD843BBDEB9A0C17329DDE3E2E93BF0ED939E715305BF07720D9A91C603532A8DD3B5969A4D951938C1AAD8AFC51A7D260684F831D
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\{4F0DC65E-2BE2-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	77016
Entropy (8bit):	2.357943532602179
Encrypted:	false
SSDEEP:	384:rw4T7+hQkBH2C/H4I/y5gN1B/IOqoKAsJMpC/UoI/ybJvvDqzdoZWs4ZDKIeZKLG:6TRTH5ZEDgyYmID1s8qF
MD5:	0C64EE521BF80D2C7401794E8C9FD4A0
SHA1:	C7659C6E14A8E511CB5CE6FEFC0ACCE659EB584E
SHA-256:	CEAB1E12A4DCA7CC5B4CA27E5E4FC2ECE726739D2F7AA8DC4757EBB9876D909E
SHA-512:	68423A17D194C217482AAF30460CD4EA02B2F73E32E3E0DBA8023897582AB83F66A9D8530BA66E7CB15C9389FB13CA7E977031A015EB768EDA9E63E359B1F74E
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\{66CF5440-2BE2-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5655625465053649
Encrypted:	false
SSDEEP:	48:IwHGcpreGwpaQG4pQQGrapbSUcrGQpK+AG7HpRTcsTGIpG:rtZWQQ6uBSUcFA+bTA4A
MD5:	B23D46E0160885AAA2CF8D50DA7AF7C5
SHA1:	106C793AC223C1FA684A538872C4840A4F0B8ACF
SHA-256:	D09FE89E2890AE13B41CE5D8D38FE5F17CB838A1BF8EB18D8352B7830F6A47C7
SHA-512:	EE3DBCF262680A520360A2FA1AB24AB1A53682E8749A93F541F67749466161AC574A48632B842099359165890492525 82FE3304A2DD072D91C4AC4033965E1AE
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.076314076493388
Encrypted:	false
SSDEEP:	12:TMHdNMNxOEBIcNnWimI002EtM3MHdNMNxOEBIcNnWimI00ObVbkEtMb:2d6NxOsSZHKd6NxOsSZ76b
MD5:	0D1CE7CFB70A639950470DD6D9EDFA75
SHA1:	0CF866AB69C26892C3D2FF5683FA9EF441BF4FA4
SHA-256:	6F9993CE21ADB584C829D81A5C3F3326BBEA40BE900CAF8EFB74C554DC2F4A51
SHA-512:	87C5D1A1687D7D0FC8C9E50B8C6EAFA68F424CC4B95AB9861020A4E68E837F98B1569D3B84790AFE37BB5DFB0442C2BA18A1C0E5A866162D816C4FF585619B2D
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x25fcabf8,0x01d6bfef</date><accdate>0x25fcabf8,0x01d6bfef</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x25fcabf8,0x01d6bfef</date><accdate>0x25fcabf8,0x01d6bfef</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Twitter.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.130768873225171
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kUUdUcNnWimI002EtM3MHdNMNxe2kUUdUcNnWimI00Obkak6EtMb:2d6NxrCuSSZHKd6NxrCuSSZ7Aa7b
MD5:	3E43A6231447D2B59221FBF314045102
SHA1:	C260944B4D9731E958F59404D21149553517D86C
SHA-256:	33CF304569F26CA0B3A131E619F9BD8822D9EAFC11A4A80AE6117687AA480E6D
SHA-512:	41CD3177EDE6FAE0D34B81CACAD26D3FDA8ECC9D3A5933188C666624D02A5CF04955045E17E0D1CEE8185E9B0D485254AB63F148501CB86DC4708989BE1D5(1
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x25f584dc,0x01d6bfef</date><accdate>0x25f584dc,0x01d6bfef</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x25f584dc,0x01d6bfef</date><accdate>0x25f584dc,0x01d6bfef</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Amazon.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	662
Entropy (8bit):	5.094000737602587
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLBIcNnWimI002EtM3MHdNMNxvLBc+pNnWimI00ObmZEtMb:2d6NxvRSZHKd6Nxva+bSZ7mb
MD5:	88AA2C233ABC26358F4FDBB809F20860
SHA1:	C5E399462C3A56154F454633E6555EA30CE7C253
SHA-256:	D353729C5062EFF5255E6D7EDDBB823D648FB0E45D02D736F2228B461759FDDC
SHA-512:	85C7A3AAB629EA1FC9B82FCA10C4C51BDEF37DD5E9BF68560FA0493A5694B77639BB835EFA9A1E37ECF70291575A402ABFD4141D85F3659385AD97E0E11F4B0
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x25fcabf8,0x01d6bfef</date><accdate>0x25fcabf8,0x01d6bfef</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x25fcabf8,0x01d6bfef</date><accdate>0x25ff0e5d,0x01d6bfef</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Wikipedia.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	647
Entropy (8bit):	5.145683581944715
Encrypted:	false
SSDEEP:	12:TMHdNMNxiHblNnWimI002EtM3MHdNMNxiHblNnWimI00Obd5EtMb:2d6NxibXSZHKd6NxibXSZ7Jjb
MD5:	E4AED45902F15E24E3A85DFC2657D601
SHA1:	00CF72D4059684686CD3B6095632EAC239B5589A
SHA-256:	96A2CFC816D7381AF8AD764FB1E06BA2713B2B0A33710D4FF158843BDC49C529
SHA-512:	EA137AA5150719C9ED5FDC171891BEFC738AD60517DBE4900FFFE611D58B48C4B9EAEC1BA8D18CC4EDB1C3713E00BBBF366F200A63BB2FA028247B810EA79(89
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x25fa4985,0x01d6bfef</date><accdate>0x25fa4985,0x01d6bfef</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x25fa4985,0x01d6bfef</date><accdate>0x25fa4985,0x01d6bfef</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Live.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.092800088505762
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwT+T+pNnWimI002EtM3MHdNMNxhGwT+T+pNnWimI00Ob8K075EtMb:2d6NxQU+T+bSZHKd6NxQU+T+bSZ7YKa/
MD5:	376076773DA51336CD5DE6FA30809F63
SHA1:	E9C2EB29373C758E9ADBC87CEB85605E27D6EBE3
SHA-256:	DE5C95F6E5EA9C2DC14F2FEA7E7C471946E3B53ABFC6A412BC47730E826A7BFC
SHA-512:	682C488EAE092FD03F40E56B6BD55DD6EB3BD344A7041F6EC2DE1E20704FCA178F7476E1654C266AB075D2A0317F573797799F01011E7794C8328C6614854249
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x25ff0e5d,0x01d6bfef</date><accdate>0x25ff0e5d,0x01d6bfef</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x25ff0e5d,0x01d6bfef</date><accdate>0x25ff0e5d,0x01d6bfef</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Youtube.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.13276838300934
Encrypted:	false
SSDEEP:	12:TMHdNMNx0nHblNnWimI002EtM3MHdNMNx0nHblNnWimI00ObxEtMb:2d6Nx0HbXSZHKd6Nx0HbXSZ7nb
MD5:	5B993EF372D077595AD6085F9235D9EE
SHA1:	0B0CCBB0145089AEE27879FC96B7E8456FEC855D
SHA-256:	1AFCBD7669DFA10395810A9C89B41F0449889F0FAEDE12275E2ECF8238B072EC
SHA-512:	EA0A235B997E4FA2F11AFDF1F90DBB275D30BE773CC161DF44CAE3BC92752184F706BC1BD67E7A1E6A14B3BDBC00354F8D7153F459E19DFD0F1CA49D9FC2C69
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x25fa4985,0x01d6bfef</date><accdate>0x25fa4985,0x01d6bfef</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x25fa4985,0x01d6bfef</date><accdate>0x25fa4985,0x01d6bfef</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Reddit.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.169860041021384
Encrypted:	false
SSDEEP:	12:TMHdNMNxxHblNnWimI002EtM3MHdNMNxxHblNnWimI00Ob6Kq5EtMb:2d6NxtbXSZHKd6NxtbXSZ7ob
MD5:	959A5B6E3EAB7F04AB81A5C162FE9EFD
SHA1:	D689DEA25FCBBB176A3340E5FB204EEDDECAD4B3
SHA-256:	E7421243D9AB8C0DD29F3A176BFA5BDA4B3E5BB2898A1B442E57FB42473D5E3A
SHA-512:	3A66820B9FE052BF6A27214D43B691D3206A931FEE8F0601719EB3C33B87054420B20B69605DB16D6CA8B91FF7907AE8EF465CED13E4985EB2B1AAB41FED2965
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x25fa4985,0x01d6bfef</date><accdate>0x25fa4985,0x01d6bfef</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x25fa4985,0x01d6bfef</date><accdate>0x25fa4985,0x01d6bfef</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\NYTimes.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	659
Entropy (8bit):	5.116591306222555
Encrypted:	false
SSDEEP:	12:TMHdNMNxcHPBNnWimI002EtM3MHdNMNxcHPBNnWimI00ObVEtMb:2d6Nx2SZHKd6Nx2SZ7Db
MD5:	507472780BF01D274A97B4023FF197B4
SHA1:	FD6A368D9F2FA44B39E5A7FABE0D0069014CA661
SHA-256:	942CD07EB541A31C84D16C56B77439F77CD28BBC96E1F20D57DAFABF7110101D
SHA-512:	0EFFC6E1E615A244308CD09CD787CD35130827FD31AF2D4018927BB4662B948271AF3859B0808B3BFC26951F0324502C8C7D707D56B69E4194A3DFC2AD5DB5C
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x25f7e74b,0x01d6bfef</date><accdate>0x25f7e74b,0x01d6bfef</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x25f7e74b,0x01d6bfef</date><accdate>0x25f7e74b,0x01d6bfef</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Facebook.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.118449838663188
Encrypted:	false
SSDEEP:	12:TMHdNMNxfnHPBNnWimI002EtM3MHdNMNxfnHvlNnWimI00Obe5EtMb:2d6NxDSZHKd6NxXXSZ7ijb
MD5:	82BC853FCA11C07891806B87C7357BDC
SHA1:	8697B2D2C83E4B20BA2511A2A7CF026FF7B84EC5
SHA-256:	DAE6528FB732ED8035465E4C6994154D3AC342A058BE40E59CA53D36571BF4E6
SHA-512:	0CCE07D41BF9273B4F246B6768839649B022CB6AD81B520D3EDAB37A63E6BB4A59A5A1217744E47F0368FB0A38C53B12B686BB9D9652F6AFECA75E96BC363F86
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x25f7e74b,0x01d6bfef</date><accdate>0x25f7e74b,0x01d6bfef</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x25f7e74b,0x01d6bfef</date><accdate>0x25fa4985,0x01d6bfef</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Google.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\ynfz0jx\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	370820
Entropy (8bit):	4.812040217571223
Encrypted:	false
SSDEEP:	1536:UD48rp0/IBXhIyuE/7rbkQblJ0AAxNPKIJ+:P8e/IBXjPAjSIJ+
MD5:	3C08B3C998BD88EB113BE57E3EFA631B
SHA1:	A1FDD6669BCDC4ABF8DCDA098AC1DCE1C14631D1
SHA-256:	63E4FEBE0BF47EDC0534691B22B590438BB993049B6997EA0A97412762F932DD
SHA-512:	15ADAF11A7CCE483BD6DA69EBB801AADE0F0EF3486D32B7CA2C1974AA7E7D10B4D9FC4D8866E09296E7008F6869D1233AF05D9EAFDD66F189C8BA9ACEBEEEA3
Malicious:	false
Reputation:	low
Preview:	).h.t.t.p.s.:././.w.o.r.k.f.l.o.w.y...c.o.m./.m.e.d.i.a./.i./.f.a.v.i.c.o.n...i.c.o.> ..... .(.....(..... ....

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\CAFA8CBC-8827-49EF-9BA3-5B2EB2C2B7DA	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	129952
Entropy (8bit):	5.378320969999905

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\CAFA8CBC-8827-49EF-9BA3-5B2EB2C2B7DA	
Encrypted:	false
SSDEEP:	1536:/cQceNWiA3gZwLpQ9DQW+zAUH34ZldpKWXboOilXPErLL8TT:1mQ9DQW+zBX8u
MD5:	D86F4803BA8228417BFBF171DA3F47FC
SHA1:	0DCA3676E47AD0A7AC76F01C26F1316C0D0536CF
SHA-256:	1EA52AD6C45B4F9E3BBFA6333D63502593B3C201A24D79BED49760EAC34FFA0E
SHA-512:	D07CAB5158BE0413F22DBB5E27EE64106A0937744A8A16E2169497A3F777EF8C585940547F1A046228A8BAF87C7DE4BC0D85F3C475AAC9CA91F9FA4ED3EB05C A
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2020-11-21T01:13:47">.. Build: 16.0.13517.30525-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:u rl>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\2D18C2DB.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	PNG image data, 96 x 96, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	2528
Entropy (8bit):	7.859207022816853
Encrypted:	false
SSDEEP:	48:GBZrR8Yz0A9399D99Yfc5xL4edUuKfNSCg6G3jQpHl40gFmc:GBZr2YztBYU5d6ueqj8+0gwc
MD5:	0FE6ADC78BBEBE98184DF48B55373859
SHA1:	C2029F1E8DAAB504C75BA6CE808B10D93F4FDA7F
SHA-256:	EB307607E7F37A674C545B5E05C88117888A393D8FAACED70C765142CBC97028
SHA-512:	54D5BE5CA569AA474A05C84B65B56687AA3D76CBE048A4622C50AAA0AF608CB9ECB99779953DF2CA82FFA2D9D6349AAFCB57ECCFF8BD2934C1F5BD4C597F2 E5F
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR...`...`.....w8....IDATx^....e..?..w..P.j.Y-..-*.TQ#...(...R$D0Q.--.Pw.w.p.m)....&..iDB4.MH..... .;.+B1bP..E8.v.3..Aoggf.....I..v..y..~..w._'$W..H..'.....$...1)P 0G0.c.hL%hf{.F@.....EqB8..p...Tr+.....!.....QGB...o`.;.d/..B.`v.(%w.!.**....>..O.dWG.!...# ".....N%.:.....m..K.....p+F~...Nm..~...-..~...%..*..b..1r.u...6.....CH..~..b1...D5w y...?9.p2/}4..9....r4..M.vW."[1r....I..V..P.B...6.H`....s....P...D.ph,@..Aj.....9F...".....P....(...T`...:....0..P_..m.>R7P.^.Q>...?.b=..y..@Y.....f..:..~.X..Xt.\.[..;}hW{'.v.R}5.u.k.. ./../. ..i.....~.Y;..".R.nq.W.....iL..r~h.....&..O.@.m..=...M.^....@.m.....}.....*...CV`..k^...,n....Ts..2.....$..1....._.....Y..6..<.....3X..r.^.Fg.\..@.....[...`.....F..t .[.<LJ~I.vP..;....h .E.&W.).*.R;...P.."LmG9.*"'.C...C.K....J..Q..K....R...z'...P..m..Cu..mU._..et.....).@%7<..o...S....<...>].h..]..f..y9.[..V...P.J.M.z|..!....aj8g.~ ..a.F...@.v...=j....j....Y.(.....="a.J.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\2F482720.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	PNG image data, 48 x 48, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	2058
Entropy (8bit):	7.880249272589655
Encrypted:	false
SSDEEP:	48:KQ4hL12ktJW/Lk9fyqIbJH3c7nGR/GT6g7uzwdK:KQ4JFgktyqId3mG9GzU
MD5:	9C2FBA52C04789512F6A65063D4E133D
SHA1:	7DB79BE522470FD497E3B773573B9AAA0BC16859
SHA-256:	830F7BA5968E6EBF92275418B4AC0622CC85867B1A8729DA7B571992052C7DB3
SHA-512:	544B72B9CB4E706ACE15FF19B5D916C5A39CE54A30F62086E27699FBFDF809417E33A096173D2A1610CB22AACDB30F5D631E63F38EC87F27C5E2332178AFF98
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR...0...0.....W.....IDAThC.ZMLTW.>.fHe..wE0Z..@SM...SM.YU..\2D..EQ\i.+..Bh.....Q..t!...6..$.jk.....$..m...;o.}..b..`.}.....s.5.P](..n.(Y...b.E..".%....d.."...M.E.. .....w..%.%A.V..%.D>.L..I.I|...].K..K.d{....R..b.g...J\.K.4.j.....$.>....#..&A.f".h.T+..X_..I(.....z*.\d3..&.'....~.o&...7.o.....@.Lh..'.wH.I.....#-R.kA3s3.z.....D..m.....)..a....)R.. ..1hjv..7....Kl...Y....z... i2.....T..~U.....R....k&...P...../.9..m'.Cgjn.....W...n8...w._..U.&....=z9'M .`z.E.TQ\A0G.. HPu.3...4..a.....M.C.7...G.2T:.(...j..5..@.5^.....N.N.....MD[a..G.. {C.u...../.1....:{.6...].8 ]..6.H@...J.e/.4.4...E....*S).....7...j.L...|..4..0....8...8.C.....LF'A.i.c... i:..d^..k..Q..6....^.+..9.!H..w..Y.M.....@.{..B.':O`.h ;.-..FW.<I.s.^8J.J...He^e..I.- ..Kc.f.&...K..7.[.W'5b..r..Z..T.].s.y...o@.L,Y/.....<,....}W..hA.....e6.gdB...G.)...../8.R..+.1P....s...s`...N.2..b57kd5.G4....<..Y.r.jb..lK.h8v=v.b.q._f...J&...>..!r{.....'...C.N...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\47E6D66C.wmf	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	Targa image data - Map - RLE 65536 x 65536 x 0 "\004"
Category:	dropped
Size (bytes):	860
Entropy (8bit):	3.319067512243173
Encrypted:	false
SSDEEP:	24:i0L+vddHEKm3QXXzYD6Zc6psBuXSobG/G:n3o06i6mw8e
MD5:	A6055AB777E6107F2348E54069050C7A

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\47E6D66C.wmf	
SHA1:	EE1F98386F89EC41A36438835EA9E1AF67DFA737
SHA-256:	F74F05036173A87CF0BF0D2B2F2F78571C2030CC6790A8CF0D187D0F72BDFFF6
SHA-512:	726DD47E3FE40743CC2DA64593BE891F90AD5CCF5C6D1E8337D04B1EF51954ED68EDAAF026C4630C8BAE41E012BE3502814C19480CD2760F703B300ECE10ABC
Malicious:	false
Preview:	.....@."Calibri.....-.....-.....-.....2.U..... .6.....Dr.....-.....-.....$..... .....-.....-.....7c.....-.....-.....$.....-.....-.....'.....&.....{.....@."Calibri.....-.....-..... ..-.....2.....&.....OpenX.F.B.G.....2.....&..... .N.....{.....@. Calibri.....-.....-.....-.....-.....@.!.....'.....-..... .....'....."System.....`.....st.1..`.....-.....-.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\75F7C857.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	PNG image data, 510 x 280, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	11108
Entropy (8bit):	7.813787831094833
Encrypted:	false
SSDEEP:	192:JRD9c21QPq/mm1PZWJAkC/XMT42x4IxcoJfVgYeuPNy3AMcvrnmc6urw058J2SVI:zWwJ1PZ0AjPMb4gcon71y3FJ22Q
MD5:	7A3FD376C29289D2BDE569B6FC88387A
SHA1:	4B4DD1F44164EF4E9356297CC9A7A8B04430D69D
SHA-256:	ED58EB28375D1515BB2C6197F1CDCF063521F3FF84478FFC8234F962EEC223CC
SHA-512:	1775AFAAABB8A4971DD4C4B234E5ABA53445D068CA649C7EBDEEB582F61326C8BEFB0C7969DE8B0BC22BEEF64C553225A831D9ECA7F90BD4F6FA72580467BDA2
Malicious:	false
Preview:	.PNG.....IHDR.....r.....tEXtSoftware.Adobe ImageReadyq.e<...(iTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c138 79.159824, 2016/09/14-01:09:01 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmp:CreatorTool="Adobe Photoshop CC 2017 (Macintosh)" xmpMM:InstanceID="xmp.iid:5C5F8CD8998E11E8A8318B31A92F73C1" xmpMM:DocumentID="xmp.did:5C5F8CD9998E11E8A8318B31A92F73C1"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:5C5F8CD6998E11E8A8318B31A92F73C1" stRef:documentID="xmp.did:5C5F8CD7998E11E8A8318B31A92F73C1"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>n.AL..'.IDATx...$E..kI.,..d...p...$..."(....x.....s.$J." ..\2...%g.(....=.}F.....}....?.O....U..:5d.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\93CABA2E.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	PNG image data, 172 x 40, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	5572
Entropy (8bit):	7.920865999861533
Encrypted:	false
SSDEEP:	96:L3wpVn/Lf65V9ZwgsLtoa2D3rqqvMaxNziK8EiNEmdylAQMgaN4gD0WlMoHbJiiv:LA/aYlLtT2DbqqvMaxNzujHzbJzv
MD5:	BD7344C330BCB32B4F97670132E93812
SHA1:	C002D5CD0241EC15F2A8765FCD250E2568E304A2
SHA-256:	F1760B2EF1795DEFBE9F2918D19DE19AA09333FD56C079E4468C83162F589A0C
SHA-512:	4A51E23B3BC07D7A7F8354C5E5B1760D354DD87879D4AABAF7AC3FE1346F7DEFBFF5BDE4A36F2C09684AA65CE1B92CF6ECFD05340D9015946F537282CC0F85C1
Malicious:	false
Preview:	.PNG.....IHDR.....(.....c.....IDATx^.\.tT....sg&.3....j.....y.A__....?.5..R.(h).".....w.I.J..j..Zi....Ikk}.=...Q....%d.7..s.[{..5.$.."...s.g.....5l.#....J55r7l)..D.}..%.$..L.SW.P...(..7Z..(.....Y.....L.B.....v.B.X.^../4~...0.3..g..3.@....].t.9.....w.....f.$..-%.....k.@Rbw.G.d..Z...#%..?7x.!....s.p.-.`..G..1.-p..3'M.H7).W..,.....~..mKKJ.AH.j..U..z9h.e.....-0....l...h.a..... ..-0....l...h.a.....z.9.UUU...4..8.T..y.3.....l2..;w..]QQQ....oYY..r...w.g.....6^VVVy.q.e.>...r....S...q..t...y..~R..,.<.....s]...q....t....k..UZZ.$....~~.B.MD..r.....J!DZ)5..aC.!\..&.qf.!. ..VJ}....1...W}....i.@...o..-;....B|.m,.d....y.&...y..^.x...B.KB..`.k..6.N..?...nmm.....B.....%.d.....jjj.1..3..7!b..WJ..Z.....w.....X,.\Jy..yy.b.....H);..l...a.N&.*.....G.....d.'..#..X.b..ywK)..6.S. .zc:.....,X.`Dii.R..C....i.q...K...DDO(.>.6...}.Fcc.....9..Z.DJ.)c....v2.T..e..Z.+....1'..K.l..u..yC...e...Dt..8.9.Ay.G.J..Z.M.....jjj"....)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\F860BCA1.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	PNG image data, 96 x 96, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1604
Entropy (8bit):	7.6935953601521865
Encrypted:	false
SSDEEP:	48:7qI05bLpn+kAcm6uWavE8xrzbFolf+Ud2R8DZ+qC7:7q3JIcWWsHA8aZ07
MD5:	CC88C60FD2660CFF828977A4990A9D96
SHA1:	68100B92B26040D5A243C585964BB03536C21860
SHA-256:	AA694497406EC6F5C284C34504C660E4C129F0DD5AA9A6A7B1358A7E332D7DDA
SHA-512:	3765218D791E1E23E2E84B13DFE7DB05ADA17B7082AD9648DBAB522DAE60664AA3954797CD5CC63FFEF395702FD656F8F6A84CD640B53C72791DE201B4DF004
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\F860BCA1.png	
Preview:	.PNG.....IHDR...`...`.....w8....IDATx^.]l.U....4..5!.>(.....UyP.)..D.P...P.....).V.[.4P.K4..P#."..[L.....4+Xs6..t...3..l..~.{...s.vg..+P..@k.....X.....hijj.i....T..a.]...]...R.<.i...u.Wf..Y-.M..K....A;..."].P(..>YWU]...a..o\.@.K..Xy../g.....G.8.....q./...@}.]..... v...._..@...../...._.....? 0...tC`...tB`...tA`...t@`....!0...(!0.... 0...(0....B`....@`.D..B`...O7?.L.5...\.....MN{.. .N..#...}M}..;...$TM.R.....'~.sllT.....({.....d.g...i+..H.....V.3)..u0ml...K.....5...FX.t...'....^.M.W2.Xk.B.....b..V.....u.#..3...k+.p.....E'Z..^.....N.....p.....j.-...y..I.BU..7dW..P.b'....SPF..#-..Mw.....V.7t.V.....~.,...QSA...ddB..x...K....)..]v?l...<.Q|. s..,....R.2..6.B..]...}....)..eW..Ww.(..5.e[..=k....JE...vc<....L?.....rvg#;s?W.{]....W....D.R0..W'....+.%.+....(d7..{t..sdO...]5~....>^H.....$.K4 c.....T/.....p.....i.|!.LQ..T/.`..(.....MWe.....C....Vs.9?.P..v....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{FABF639E-4792-4112-BF52-2B5E333F7251}.tmp	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	7680
Entropy (8bit):	3.962771299760653
Encrypted:	false
SSDEEP:	96:7cOjeQZj9TUzn5AqArr9PBOAu9ewuoV9vM28s2Jbs9NPabBW:7rjeQZj1U5/QVchuo3M2gBS2BW
MD5:	8D6A63569220358BAC45BF7676C005D3
SHA1:	26BBA0AEF5F43A34A104DCFDD48E73A6CF7D4A09
SHA-256:	F971319A2227E126403375322C0454F3B0A08716B42DFEC2AB21F4C451D0D432
SHA-512:	D204372A5402F19C72D9BB6BED240D8168F0C200FCC11B7EB6C890FBAEF283F769089794459FB761046B4147F12A1B998FB076288655726CD94790F961FB61B8
Malicious:	false
Preview:	..... .!.".#.$.%.&.'.(.).*.+.,.-.../.0.1.2.3.4.5.6.7.8.9.:.;.<.=.>...../..... .M.a.r.k. .G.o.w.l.a.n.d. .s.h.a.r.e.d. .a. .f.i.l.e. .w.i.t.h. .y.o.u...../. .T.h.i.s. .l.i.n.k. .w.i.l.l. .w.o.r.k. .f.o.r. .e.v.e.r.y.o.n.e...../...-. .P.a.y.m.e.n.t. .R.u.n..... . . . . .T.h.i.s. .l.i.n.k. .e.x.p.i.r.e.s. .i.n. .2.4. .h.o.u.r.s.....v.....`.....$..d.....a$.gdH.L.l..... .....i...$..$.lf.....!v..h.#v..y.:V....].t....6`.....k.....0.....y..6.....5.....y.2.....2.....3.....4.....B.....`.....p.....yt.k.....$..d.....a$.gdH.L.l..... ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{FE51252F-4CD4-4977-A57E-E1D5999F0844}.tmp	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28BA4
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\ZJH_2F3Xi0SopxxCuN7EKeDY[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, baseline, precision 8, 1920x1080, frames 3
Category:	downloaded
Size (bytes):	17453
Entropy (8bit):	3.890509953257612
Encrypted:	false
SSDEEP:	192:P7FRTHQpmA3ZkXOL25cYty7l6UWUjMJBSab/vR+yzP:P/cpmgkF5+JWUjMp40P
MD5:	7916A894EBDE7D29C2CC29B267F1299F
SHA1:	78345CA08F9E2C3C2CC9B318950791B349211296
SHA-256:	D8F5AB3E00202FD3B45BE1ACD95D677B137064001E171BC79B06826D98F1E1D3
SHA-512:	2180ABE47FBF76E2E0608AB3A4659C1B7AB027004298D81960DC575CC2E912ECCA8C131C6413EBBF46D2AAA90E392EB00E37AED7A79CDC0AC71BA78D828A8C7
Malicious:	false
IE Cache URL:	http://https://s3.amazonaws.com/simbla-static-2/2020/11/5faba665321d68001d4fc0e4/5faba6db73aef50019af7085/ZJH_2F3Xi0SopxxCuN7EKeDY.jpg
Preview:	.....Phttp://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c142 79.160924, 2017/07/13-01:06:39 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about=""/> </rdf:RDF> </x:xmpmeta>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\css[1].css

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\css[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	748
Entropy (8bit):	5.145901704840272
Encrypted:	false
SSDEEP:	12:jFMO6ZN6p4aJqFMO6ZRoT6pIFqFMO6ZN76pYnJqFMO6Zd66pxJY:5MOYNFMOYsiMOYN7qMOYd6b
MD5:	8D16141128F29CBCE3B14C993B5B8328
SHA1:	439E68D66D1083B292B0B34CF2D6E76C91D390E2
SHA-256:	D1D6EB851B081A55059BA87236DFB146CCA801EDA1E2D7DCD60F6FCE111A450E
SHA-512:	A431B863FEE4084EAB5AF14B184685A9E93072DAF01E2E4766914BA1148F4F4E6F0E9E1BF2E0112F087239332F235CA741F80D77944E3A00AC94CB70EE5C42C1
Malicious:	false
Preview:	@font-face {. font-family: 'Open Sans';. font-style: normal;. font-weight: 300;. src: url(https://fonts.gstatic.com/s/opensans/v18/mem5YaGs126MiZpBA-UN_r8OU uhv.woff) format('woff');.}.@font-face {. font-family: 'Open Sans';. font-style: normal;. font-weight: 400;. src: url(https://fonts.gstatic.com/s/opensans/v18/mem8YaG s126MiZpBA-UFVZ0d.woff) format('woff');.}.@font-face {. font-family: 'Open Sans';. font-style: normal;. font-weight: 700;. src: url(https://fonts.gstatic.com/s/opensa ns/v18/mem5YaGs126MiZpBA-UN7rgOUuhv.woff) format('woff');.}.@font-face {. font-family: 'Open Sans';. font-style: normal;. font-weight: 800;. src: url(https://fonts.gs tatic.com/s/opensans/v18/mem5YaGs126MiZpBA-UN8rsOUuhv.woff) format('woff');.}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\css[2].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:	9EA12CC277C9858524083FEBBE1A3E61FDECE5268F63B14C9FFAFE29396C7CCDB3B07BE10E829936BCCD8F3B9E39DCFA6BC4316F189E4CEA914F1D06916DB 66B
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/tss 0ApVBdCYD5Q7hcxTE1ArZ0bbwiXo.woff) format('woff');.}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\dfce06801e1a85d6d06f1fdd4475dacd[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	11724
Entropy (8bit):	5.142570243800562
Encrypted:	false
SSDEEP:	192:fCVFt3uv8AIW93kXLHkwBcAfSdIYjf0yChCTfbOtfC9QdHn:KXW42I9QTfbO49U
MD5:	50A0037A600BA8C10F993DB1F075AF0C
SHA1:	6CF8EC58F39CC2D77BC7CE84FED0C669E84D9E21
SHA-256:	3660F800D33EA3E7A1835B48188AA5F50ADBE40E1E833246159699673AEBAAAD
SHA-512:	5559E835A704742995271877247EB5AADD20E33C13A1332C7F68245E5C2D2B1B7712A1F1F0EFF2F70B4C63ECC3EB588C3CD4DD9A264D2B688FBBB19D43D6EA F
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_10, Description: Yara detected HtmlPhish_10, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\dfce06801e1a85d6d06f1fdd4475dacd[1].htm, Author: Joe Security
IE Cache URL:	http://https://jamif-cdn3d.us-east-1.linodeobjects.com/dfce06801e1a85d6d06f1fdd4475dacd.html
Preview:	..<!doctype html>..<html lang="en">..<head>.. <script src="https://ajax.googleapis.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>.. <script src="https://code.jquer y.com/jquery-3.1.1.min.js"></script>.. <script src="https://code.jquery.com/jquery-3.3.1.js" integrity="sha256-2Kok7MbOyxpgUVvAk/HJ2jigOSYS2auK4Pfzbm7uH60=" cr ossorigin="anonymous"></script>.. Required meta tags -->.. <meta charset="utf-8">.. <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fi t=no">.... Bootstrap CSS -->.. <link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/css/bootstrap.min.css" integrity="sha384-Gn5384 xqQ1aoWXA+058RXPxPg6fy4IWvTNh0E263XmFcJlSAwiGgFAW/dAiS6JXm" crossorigin="anonymous">.. <link href="https://fonts.googleapis.com/css?family= Archivo+Narrow&display=swap" rel="stylesheet">.. <script src="https://kit.fontawesome.com/585b051251.js" crossorigin="anonymous"></script>.. <title>Log-In</title>.. <link href="css/hover.c

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\document_view.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with NEL line terminators
Category:	downloaded
Size (bytes):	2273519

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\document_view.min[1].js	
Entropy (8bit):	5.559905400521439
Encrypted:	false
SSDEEP:	49152:SNx768bLt7j4KWF38OHZ4tkGSNiiul1EII:StA6iBI
MD5:	4178D793497614CBF5B74C0C8979754F
SHA1:	700184FFA5B57AF2316B37DF357E02BA2346352B
SHA-256:	AA3D1A96BF8F4EED52C33D311D1CEDE1A735C7595E567BF81E9397480B7E4D48
SHA-512:	C18F6431A04794ACC19209530CDF60AF5E6CE77115D5BC9A65C83B243F1FA5530D06431CDC8652DF4D7A1EC27D7F76DF4E0B6F6139E01EA75ED746B6655653D
Malicious:	false
IE Cache URL:	http://https://workflowy.com/media/js/document_view.min.js?v=610982d
Preview:	!function(e){var t={};function n(r){if(t[r])return t[r].exports;var o=t[r]={i:r,l:!1,exports:{}};return e[r].call(o.exports,o,o.exports,n),o.l=!0,o.exports}n.m=e,n.c=t,n.d=function(e,t,r){n.o(e,t)||Object.defineProperty(e,t,{enumerable:!0,get:r})},n.r=function(e){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(e,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(e,"__esModule",{value:!0})},n.t=function(e,t){if(1&t&&(e=n(e)),8&t)return e;if(4&t&&"object"==typeof e&&e&&e.__esModule)return e;var r=Object.create(null);if(n.r(r),Object.defineProperty(r,"default",{enumerable:!0,value:e}),2&t&&"string"!=typeof e)for(var o in e)n.d(r,o,function(t){return e[t]}.bind(null,o));return r},n.n=function(e){var t=e&&e.__esModule?function(){return e.default}:function(){return e};return n.d(t,"a",t),t},n.o=function(e,t){return Object.prototype.hasOwnProperty.call(e,t)},n.p="/media/js/",n(n.s=885)}([function(e,t,n){"use strict";e.exports=n(438)},function(e,t,n){"use strict";

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\ga[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	46274
Entropy (8bit):	5.48786904450865
Encrypted:	false
SSDEEP:	768:aqNVrKn0VGhn+K7U1r2p/Y60fyy3/g3OMZht1z1prkfw1+9NZ5VA:RHrLVGhnpIwp/Y7cnz1RkLL5m
MD5:	E9372F0EBBCF71F851E3D321EF2A8E5A
SHA1:	2C7D19D1AF7D97085C977D1B69DCB8B84483D87C
SHA-256:	1259EA99BD76596239BFD3102C679EB0A5052578DC526B0452F4D42F8BCDD45F
SHA-512:	C3A1C74AC968FC2FA366D9C25442162773DB9AF1289ADFB165FC71E7750A7E62BD22F424F241730F3C2427AFFF8A540C214B3B97219A360A231D4875E6DDEE6
Malicious:	false
IE Cache URL:	http://https://ssl.google-analytics.com/ga.js
Preview:	(function(){var E;var g=window,n=document,p=function(a){var b=g._gaUserPrefs;if(b&&b.ioo&&b.ioo()||a&&!0===g["ga-disable-"+a])return!0;try{var c=g.external;if(c&&c._gaUserPrefs&&"oo"==c._gaUserPrefs)return!0}catch(f){}a=[];b=n.cookie.split(";");c=/^\s*AMP_TOKEN=\s*(.*?)\s*$/;for(var d=0;d<b.length;d++){var e=b[d].match(c);e&&a.push(e[1])}for(b=0;b<a.length;b++)if("$OPT_OUT"==decodeURIComponent(a[b]))return!0;return!1};var q=function(a){return encodeURIComponent?encodeURIComponent(a).replace(/\(/g,"%28").replace(/\)/g,"%29"):a},r=/^(www\.)?google(\.com?)?(\.[a-z]{2})?$/,u=/(^\|\.)doubleclick\.net$/i;function Aa(a,b){switch(b){case 0:return""+a;case 1:return 1*a;case 2:return!!a;case 3:return 1E3*a}return a}function Ba(a){return"function"==typeof a}function Ca(a){return void 0!=a&&-1<(a.constructor+"").indexOf("String")}function F(a,b){return void 0==a||"-"==a&&!b||""==a}function Da(a){if(!a||""==a)return"";for(;a&&-1<" \n\r\t".indexOf(a.charAt(0));)a=a.substring(1);for(;a&&-1<" \n\r\t".i

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\login[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	169
Entropy (8bit):	4.534640683711167
Encrypted:	false
SSDEEP:	3:qVoB3tUROGclXqyvXboAcMBXqWSZUXqXIlVLLPbCXqwcWWGu:q43tISl6kXiMIWSU6XII5LPJpfGu
MD5:	7B4F513528A3D65397F0E7F6DEF7AD4A
SHA1:	5DA8E55D7F30D9530BDEFB6FD670C273FF9DDD66
SHA-256:	5075788CBBDF48D111B4882949D3E50856C81CA87630A85D7C8DD1E600CDC691
SHA-512:	1EAAE52797DDC5ECC686D6351BFB152DB1276C644E33DAFE9ACA9B81EE9AA75D29FA04A12A64B3B281E0163C318E9832861D9553C67A984D3958E90EF57FE5C
Malicious:	false
Preview:	<html>..<head><title>301 Moved Permanently</title></head>..<body>.. 301 Moved Permanently ..<hr> nginx/1.19.4 ..</body>..</html>..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\mem5YaGs126MiZpBA-UN_r8OUuhv[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 18668, version 1.1
Category:	downloaded
Size (bytes):	18668
Entropy (8bit):	7.969106009002288
Encrypted:	false
SSDEEP:	384:Wv4QHZChiRh3lwLOf8cWN78NXpcr6gBUA9CD/q4cOPZmPO:WvwhNOkvvxC7qnc
MD5:	A7622F60C56DDD5301549A786B54E6E6
SHA1:	D55574524345932DB3968C675E1AEA08C68A456F
SHA-256:	6E8A28A0638C920E5B76177E5F03BA94FCDEDD3E3ECD347C333D82876B51C9C0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\mem5YaGs126MiZpBA-UN_r8OUuhv[1].woff	
SHA-512:	1A842E5EDFFFFBAE353AD16545D9886E3E176755F22B86ECCC9B8B010FC79DB7194B7C5518CC190BF5B78B332C7D542B70A6A53B3BAF23366708DF348C2C2D9
Malicious:	false
IE Cache URL:	http://https://fonts.gstatic.com/s/opensans/v18/mem5YaGs126MiZpBA-UN_r8OUuhv.woff
Preview:	wOFF.....H.....n0.....GDEF.....GPOS.....GSUB.....X...t...OS/2.....^...`}...cmap...`.....X..cvt .....]....fpgm...t.....~a..gasp.....#glyf... ..8...WP..M.head..@....6...6..F.hhea..A.....$...chmtx..A8....._{loca..CL.....K.4&maxp..E.... ... .name..E0....."c?Jpost..F.....x.U..prep..G.....:..].... .....x...5.A.....m."gW..`.L..&N".?.....IF....a.^...b1.....Uh."4...>..=x.c`fig.a`e``..j...(.../2.1..`b.ffcfeabbi``Pg``..b.. 0t.vfp`P...M...C.G/S....|...=.6 .....m/....x.\.!..q.....#aff... #1Q@.'U..@5.".llt.Aa#.f\|c.W.....'..X..!..C...ITPE.;..V.j.....0. .L0E...Yd.mN....:.....F....GG.g.s,x.>0....v..I;o..<.$G9.\f2...e{}.IS2..uc]p.....M.x.c.a.g.c..$K..$..`.g.e..... ..... R.g.....?.....x.)d.....$...."....0.#.A@X..0.....x.uTGw.F.....)..)7.W.$`*.....G.Kz.)e....t.|.1.7...s.g...3.7mgf..~{1...s.3.S...co..o.~.Zy.u...kW.\.t...N

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\mem8YaGs126MiZpBA-UFVZ0d[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 18100, version 1.1
Category:	downloaded
Size (bytes):	18100
Entropy (8bit):	7.962027637722169
Encrypted:	false
SSDEEP:	384:aHQHZuiZQFFlimUy1oml4hN2Vmw1Qa57YC74ObDDj08X0UJQiXc:1ZQT0UySml4bEmAP5EC7PbDH4U1M
MD5:	DE0869E324680C99EFA1250515B4B41C
SHA1:	8033A128504F11145EA791E481E3CF79DCD290E2
SHA-256:	81F0EC27796225EA29F9F1C7B74F083EDCD7BC97A09D5FC4E8D03C0134E62445
SHA-512:	CD616DB99B91C6CBF427969F715197D54287BAFA60C3B58B93FF7837C21A6AAC1A984451AEEB9E07FD5B1B0EC465FE020ACBE1BFF8320E1628E970DDF37B0F0E
Malicious:	false
IE Cache URL:	http://https://fonts.gstatic.com/s/opensans/v18/mem8YaGs126MiZpBA-UFVZ0d.woff
Preview:	wOFF.....F.....i.....GDEF.....GPOS.....GSUB.....X...t...OS/2.....^...`~]..cmap...`.....X..cvt .....Y.....M..fpgm...p.....~a..gasp.....#glyf... ...6...S...]head..>....6...6..cphhea..>.....$....hmtx..?.....[$loca..A4.....f..maxp..B.... ... .name..C.....&:A.post..D.....x.U..prep..E.....C..... ..x...5.A.....m."gW..`.L..&N".?.....IF....a.^...b1.....Uh."4...>..=x.c`f..8.....u..1...<.f.....A.....5....1...A._6..".-..L.....Ar,.....3..(....x.\.!..q.....#aff...#1Q@.'U..@5." .llt.Aa#.f|c.W.....'..X..!..C...ITPE.;..V.j.....0. .L0E...Yd.mN....:.....F....GG.g.s,x.>0....v..I;o..<.$G9.\f2...e{}.IS2..uc]p.....M.x.c.a.g.c..$KY...e@.,.."..... .....?....%.g....Z..... ("o..Y..Bu342.e.....0.....M=.....x.uTGw.F.....)..)7.W.$`*.....G.Kz.)e....t.|.1.7...s.g...3.7mgf..~{1...s.3.S...co..o.~.Zy.u...kW.\.t...N.KG.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\rC56cpX1uS2qJKOxJ-5Sb8u-[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://s3.amazonaws.com/simbla-static-2/2020/11/5faba665321d68001d4fc0e4/5faba6db73aef50019af7085/rC56cpX1uS2qJKOxJ-5Sb8u-.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="108" height="24" viewBox="0 0 108 24"><title>assets</title><path d="M44.836,4.6V18.4h-2.4V7.583H42.4L38 .119,18.4H36.531L32.142,7.583h-.029V18.4H29.9V4.6h3.436L37.3,14.83h.058L41.545,4.6Zm2,1.049a1.268,1.268,0,0,1,.419-.967,1.413,1.413,0,0,1,1-.39,1.392, 1.392,0,0,1,1.02.4,1.3,1.3,0,0,1,.4.958,1.248,1.248,0,0,1-.414.953,1.428,1.428,0,0,1-1.01.385A1.4,1.4,0,0,1,47.25,6.6a1.261,1.261,0,0,1-.409-.948M49.41,18.4H47. 081V8.507H49.41Zm7.064-1.694a3.213,3.213,0,0,0,1.145-.241,4.811,4.811,0,0,0,1.155-.635V18a4.665,4.665,0,0,1-1.266.481,6.886,6.886,0,0,1-1.554.164,4.707,4.707,0, 0,1-4.918-4.908,5.641,5.641,0,0,1,1.4-3.932,5.055,5.055,0,0,1,3.955-1.545,5.414,5.414,0,0,1,1.324.168,4.431,4.431,0,0,1,1.063.39v2.233a4.763,4.763,0,0,0-1.1-.61 1,3.184,3.184,0,0,0-1.15-.217,2.919,2.919,0,0,0-2.223.9,3.37,3.37,0,0,0-.847,2.416,3.216,3.216,0,0,0,.813,2.338,2.936,2.936,0,0,0,2.209.837M65.4,8.343a2.952,2.9 52,0,0,1,.5.039,2.1,2.1,0,0,1,.375.1v2.358a2.04,2.04,0,0,0-.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\585b051251[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	9972
Entropy (8bit):	5.162816885495512
Encrypted:	false
SSDEEP:	192:VEH6KnRK9ZoshohwIQEEKIMTmlD0yZTwUEhA0jxRjhO3YXyl80YT1rxMn:rxDohl1OrfohwYXyl80YZm
MD5:	BA42298E76E6F714456BF30A3C080955
SHA1:	C4DA8F08824D48D16936871078DCDCEFF875137F
SHA-256:	704E83D712675EF5372B082BC11DCE00C8E498836B383C4514099BA5E0B9F833
SHA-512:	8B4664DCCA234CF61D3D72655252B73FF100E1EE96D2902B3F4E09099AAEC9DDF1AE538642366CC957FDAE5C489AFDECF756BF75A5F89A3D424ED65C139F81C
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\585b051251[1].js	
IE Cache URL:	http://https://kit.fontawesome.com/585b051251.js
Preview:	window.FontAwesomeKitConfig = {"asyncLoading":{"enabled":true},"autoA11y":{"enabled":true},"baseUrl":"https://ka-f.fontawesome.com","detectConflictsUntil":null,"iconUploads":{},"license":"free","method":"css","minify":{"enabled":true},"token":"585b051251","v4FontFaceShim":{"enabled":false},"v4shim":{"enabled":true},"version":"5.15.1"};.!function(t){"function"==typeof define&&define.amd?define(t):t()}((function(){"use strict";function t(e){return(t="function"==typeof Symbol&&"symbol"==typeof Symbol.iterator?function(t){return typeof t}:function(t){return t&&"function"==typeof Symbol&&t.constructor===Symbol&&t!==Symbol.prototype?"symbol":typeof t})(e)}function e(t,e,n){return e in t?Object.defineProperty(t,e,{value:n,enumerable:!0,configurable:!0,writable:!0}):t[e]=n,t}function n(t,e){var n=Object.keys(t);if(Object.getOwnPropertySymbols){var o=Object.getOwnPropertySymbols(t);e&&(o=o.filter((function(e){return Object.getOwnPropertyDescriptor(t,e).enumerable}))),n.push.apply(n,o)}return n}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\6f0b670eddaac85c5e4a[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	48788
Entropy (8bit):	5.359595203167086
Encrypted:	false
SSDEEP:	384:NA+C8e79Ye4hXZFCaWhz4EYrquM5FX4PV2YER6tTDf4z+l2PtmAucSOrxFqw66MG:74B4hWaOGrMhaTza/k6BG+7r
MD5:	8AFD3E7AEF0EF52C3EC7F4647F443AE4
SHA1:	21B6CC97A07DE5C5E62A5A0BEE624DE2B8033A23
SHA-256:	FA8372A7BFB9536773A97EF134BD77AAA88295B10382F5885C70C639C51EB5B3
SHA-512:	07131B6D036AD0475B406DD79747589A461AAA9C16477C3209E20E0333270A320F23E0EF6BF18D4899F2854569F95966C8F2FC9AD5CB57B08DE27B7AD2FBEBE2
Malicious:	false
IE Cache URL:	http://https://workflowy.com/media/js/6f0b670eddaac85c5e4a.js
Preview:	(window.webpackJsonp=window.webpackJsonp||[]).push([[0],{10:function(e,r,t){"use strict";t.d(r,"c",function(){return g}),t.d(r,"d",function(){return h}),t.d(r,"e",function(){return y}),t.d(r,"b",function(){return v}),t.d(r,"a",function(){return x}),t.d(r,"f",function(){return w});var n,o=t(0),a=t(9),i=t(2),u=function(){return(u=Object.assign||function(e){for(var r,t=1,n=arguments.length;t<n;t++)for(var o in r=arguments[t])Object.prototype.hasOwnProperty.call(r,o)&&(e[o]=r[o]);return e}).apply(this,arguments)},c={gray1:a.g,gray2:a.f,gray3:a.n,gray4:a.k,gray5:a.l,gray6:a.m,gray7:a.b,gray8:a.s,sharing:a.r,accent:a.a,overlay:a.s},l={gray1:"#ffffff",gray2:"#d9dbdb",gray3:"#9ea1a2",gray4:"#7c7f81",gray5:"#5c6062",gray6:"#42484b",gray7:"#353c3f",gray8:"#2a3135",sharing:"#367",accent:"#367",overlay:"#2a3135"},s=function(e){return void 0===e&&(e=c),u(u({},e),{arrowColor:e.gray2,background:e.gray8,backgroundImage:null,backgroundImageSet:null,bulletColor:e.gray2,bulletHalo:e.gray5,bulletHaloHover

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\Tdcv9KOl0AuohEPl[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	15359
Entropy (8bit):	5.427573051037356
Encrypted:	false
SSDEEP:	384:doPdCvSS/yNrbLXTkc4SRzKeO0bT9GVYlTrc4Un0u0aOuPgl5YGm3TF9:doPNwcDPDbT/tQ4UnUaOPmGm3Tv
MD5:	13EAD2B2FF7EEAE1321F5E821823F973
SHA1:	91A8D0CA2926F32FA0669934DFC0F59A3ADD6707
SHA-256:	E97FEBFB1C13A0B5BDB683F4481749FE31B17F91D2A9CEFEE4917F9194BA2A2E
SHA-512:	DE46BB4984676D9307734ECEE4F8702644B33345E6F62A58B8EB2223C029B8967202FA5644106177456267 20C3E2A8E1F204EAA6DED8A04A4CB95D2CEDAD00D
Malicious:	false
Preview:	<!DOCTYPE html>...<html>. <head>. <meta charset="utf-8">. <meta http-equiv="X-UA-Compatible" content="chrome=1"><script type="text/javascript">(window.NREUM||(NREUM={})).loader_config={licenseKey:"eaeea54ab7",applicationID:"61695248"};window.NREUM||(NREUM={}),__nr_require=function(e,t,n){function r(n){if(!t[n]){var i=t[n]={exports:{}};e[n][0].call(i.exports,function(t){var i=e[n][1][t];return r(i||t)},i,i.exports)}return t[n].exports}if("function"==typeof __nr_require)return __nr_require;for(var i=0;i<n.length;i++)r(n[i]);return r}({1:[function(e,t,n){function r(){}function i(e,t,n){return function(){return o(e,[u.now()].concat(c(arguments)),t?null:this,n),t?void 0:this}}var o=e("handle"),a=e(6),c=e(7),f=e("ee").get("tracer"),u=e("loader"),s=NREUM;"undefined"==typeof window.newrelic&&(newrelic=s);var d=["setPageViewName","setCustomAttribute","setErrorHandler","finished","addToTrace","inlineHit","addRelease"],p="api-",l=p+"ixn-";a(d,function(e,t){s[t]=i(p+t,!0,"api")}),s.addPageA

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\adf9fc155506e2fa3fbf[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	6865
Entropy (8bit):	5.310715814564055
Encrypted:	false
SSDEEP:	192:276Udb4Zz7Gf3XmkhlmClBRQ/IaAeLKKd5ceK:M60SGfrhplBRQ/IheLKKQ
MD5:	B0CCC823DF717416D5EAA426AAC6BA86
SHA1:	6984D4F8B021EC07E4EEB338F9F6F8431C6C18EB
SHA-256:	53BDF5DAE2A46EE74470051D7AF9FB93BEAF8659D193322D4916EB758FE87294
SHA-512:	49298181F084D342B04993DB1D59A443933D153C6B2D378E2AF4B95769785CC13053E2213473800EF8F0AD0E240E98DBE93DAB1805272BEEAC8E0A1D90AD93B
Malicious:	false
IE Cache URL:	http://https://workflowy.com/media/js/adf9fc155506e2fa3fbf.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\adf9fc155506e2fa3fbf[1].js	
Preview:	(window.webpackJsonp=window.webpackJsonp||[]).push([[11],{921:function(e,t,n){"use strict";var a=n(0),r=n(3),i=function(){return(i=Object.assign||function(e){for(var t,n=1,a=arguments.length;n<a;n++)for(var r in t=arguments[n])Object.prototype.hasOwnProperty.call(t,r)&&(e[r]=t[r]);return e}).apply(this,arguments)};function o(e){return JSON.stringify(e).replace(/\u2028/g,"\\u2028").replace(/\u2029/g,"\\u2029").replace(/<\//g,"<\\/")}var l=a.memo(function(e){var t=e.title,n=e.description,l=e.style,c=e.children,s=e.context;return a.useEffect(function(){document.title=t},[t]),Object(r.g)("html",{margin:0,padding:0,height:"100%"}),Object(r.g)("body",i({margin:0,padding:0,height:"100%"},l)),Object(r.g)("#page",{height:"100%"}),s.pageOnly?c:a.createElement("html",null,a.createElement("head",null,a.createElement("title",null,t),n&&a.createElement("meta",{name:"description",content:n}),a.createElement("meta",{httpEquiv:"X-UA-Compatible",content:"chrome=1"}),a.createElement("link",{href:"https:/

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\bootstrap.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	144877
Entropy (8bit):	5.049937202697915
Encrypted:	false
SSDEEP:	1536:GcoqwrUPyDHU7c7TcDEBi82NcuSELL4d/+oENM6HN26Q:VoPgPard2oENM6HN26Q
MD5:	450FC463B8B1A349DF717056FBB3E078
SHA1:	895125A4522A3B10EE7ADA06EE6503587CBF95C5
SHA-256:	2C0F3DCFE93D7E380C290FE4AB838ED8CADFF1596D62697F5444BE460D1F876D
SHA-512:	93BF1ED5F6D8B34F53413A86EFD4A925D578C97ABC757EA871F3F46F340745E4126C48219D2E8040713605B64A9ECF7AD986AA8102F5EA5ECF9228801D962F5D
Malicious:	false
IE Cache URL:	http://https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/css/bootstrap.min.css
Preview:	/*!. * Bootstrap v4.0.0 (https://getbootstrap.com). * Copyright 2011-2018 The Bootstrap Authors. * Copyright 2011-2018 Twitter, Inc.. * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE). */:root{--blue:#007bff;--indigo:#6610f2;--purple:#6f42c1;--pink:#e83e8c;--red:#dc3545;--orange:#fd7e14;--yellow:#ffc107;--green:#28a745;--teal:#20c997;--cyan:#17a2b8;--white:#fff;--gray:#6c757d;--gray-dark:#343a40;--primary:#007bff;--secondary:#6c757d;--success:#28a745;--info:#17a2b8;--warning:#ffc107;--danger:#dc3545;--light:#f8f9fa;--dark:#343a40;--breakpoint-xs:0;--breakpoint-sm:576px;--breakpoint-md:768px;--breakpoint-lg:992px;--breakpoint-xl:1200px;--font-family-sans-serif:-apple-system,BlinkMacSystemFont,"Segoe UI",Roboto,"Helvetica Neue",Arial,sans-serif,"Apple Color Emoji","Segoe UI Emoji","Segoe UI Symbol";--font-family-monospace:SFMono-Regular,Menlo,Monaco,Consolas,"Liberation Mono","Courier New",monospace}*,::after,::before{box-sizing:border-box}html{font-family:sans

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\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"),require("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.prototype.hasOwnProperty.call(n,i)&&(t[i]=n[i])}return t}).apply(this,arguments)}e=e&&e.hasOwnProperty("default")?e.default:e,n=n&&n.hasOwnProp

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\eaeea54ab7[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	57
Entropy (8bit):	4.31817604175005
Encrypted:	false
SSDEEP:	3:U3KTDWuvMiqVkMWVrfUh:HnNukMWVr8h
MD5:	79F2D634CE67570918939DF10A075576
SHA1:	BA47B7DACB11250F9B1B3974B34954B188E3ECAD
SHA-256:	D10C94B6CDB747904BAEE9070F003BB45849DA46F8100B1320F286C21CBCAAA1
SHA-512:	155FAB1EC68F300DDCB948D024995539C721A2AB0FD89C220F0EFFA68C3863507CBEF806F087F5C84EAB38D4C53DA94BC893894E8FC9DED388DACFE3244E18E
Malicious:	false
Preview:	NREUM.setToken({'stn':1,'err':1,'ins':1,'cap':0,'spa':1})

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\logo-bullet-lines-blue[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	589
Entropy (8bit):	4.972593672152842
Encrypted:	false
SSDEEP:	12:trZ9/MKuCoYUddWAbkLbcJfC4PbHTZL+xKC4nPHvoLrMltEulatEmZCtE+:tV9/MKuNT4sCGbHTZbC0oXw5WhAP
MD5:	7C6542F8D09ED039CEAD9A46BA912E53
SHA1:	45BECA1B83D4B72F79D1A10C6210ACDFF355C23B
SHA-256:	1255B7A53BEFBB4A3C4031F9582FE1936B8D124DE5B8B693B03358CB3E492071
SHA-512:	3900389574C26E5EAE008CC91F369C5346FC5C0501D9B773AFFF4FAFEC9F690A257B795742AB80980F025E645B5DC581AC1B26E42ECA6E51400C84EEBDC018F
Malicious:	false
IE Cache URL:	http://https://workflowy.com/media/i/logo-bullet-lines-blue.svg
Preview:	<svg width="579" height="580" viewBox="0 0 579 580" fill="none" xmlns="http://www.w3.org/2000/svg">.<path d="M116 35H531C557.51 35 579 56.4903 579 83V83C579 109.51 557.51 131 531 131H116V35Z" fill="#B2CADB"/>.<path d="M218 242H531C557.51 242 579 263.49 579 290V290C579 316.51 557.51 338 531 338H218V242Z" fill="#B2CADB"/>.<path d="M116 449H531C557.51 449 579 470.49 579 497V497C579 523.51 557.51 545 531 545H116V449Z" fill="#B2CADB"/>.<circle cx="83" cy="83" r="83" fill="#47525B"/>.<circle cx="235" cy="290" r="83" fill="#47525B"/>.<circle cx="83" cy="497" r="83" fill="#47525B"/>.</svg>.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\reset[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	928
Entropy (8bit):	4.754464678335133
Encrypted:	false
SSDEEP:	24:LFc0a1DMd2Uhsq1wJjtqQqvAQbCFD+FW9N3/s:xLzhsJVtf/F3X0
MD5:	11B989919D8B8857A3700B00F4E8F184
SHA1:	0D909DA6DE2B0157D07D0FCB721221F5D49688C0
SHA-256:	20B1C4B5D2BE0EED0ABB524023534E08D98D34D82C01D60CEB40D9B387EB8AC5
SHA-512:	BA320F903E0EDEF9E65861F931F4711E8556723560EAD36D46935BB126BAF4CEFDC08A14A1F5AA9F517AD5EF79CE67213391B0BA1ABC46A9F34F841A3BADC2A7
Malicious:	false
IE Cache URL:	http://https://workflowy.com/media/css/reset.css
Preview:	html, body, div, span, applet, object, iframe,.h1, h2, h3, h4, h5, h6, p, blockquote, pre,.a, abbr, acronym, address, big, cite, code,.del, dfn, em, font, img, ins, kbd, q, s, samp,.small, strike, strong, sub, sup, tt, var,.b, u, i, center,.dl, dt, dd, ol, ul, li,.fieldset, form, label, legend,.table, caption, tbody, tfoot, thead, tr, th, td {.margin: 0;.padding: 0;.border: 0;.outline: 0;.font-size: 100%;.vertical-align: baseline;.background: transparent;.}.body {.line-height: 1;.}.ol, ul {.list-style: none;.}.blockquote, q {.quotes: none;.}.blockquote:before, blockquote:after,.q:before, q:after {.content: '';.content: none;.}../* remember to define focus styles! */.:focus {.outline: 0;.}../* remember to highlight inserts somehow! */.ins {.text-decoration: none;.}.del {.text-decoration: line-through;.}../* tables still need 'cellspacing="0"' in the markup */.table {.border-collapse: collapse;.border-spacing: 0;.}..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\signup[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	169
Entropy (8bit):	4.534640683711167
Encrypted:	false
SSDEEP:	3:qVoB3tUROGclXqyvXboAcMBXqWSZUXqXIlVLLPbCXqwcWWGu:q43tISl6kXiMIWSU6XII5LPJpfGu
MD5:	7B4F513528A3D65397F0E7F6DEF7AD4A
SHA1:	5DA8E55D7F30D9530BDEFB6FD670C273FF9DDD66
SHA-256:	5075788CBBDF48D111B4882949D3E50856C81CA87630A85D7C8DD1E600CDC691
SHA-512:	1EAAE52797DDC5ECC686D6351BFB152DB1276C644E33DAFE9ACA9B81EE9AA75D29FA04A12A64B3B281E0163C318E9832861D9553C67A984D3958E90EF57FE5C
Malicious:	false
Preview:	<html>..<head><title>301 Moved Permanently</title></head>..<body>.. 301 Moved Permanently ..<hr> nginx/1.19.4 ..</body>..</html>..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\site.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with LF, NEL line terminators
Category:	downloaded
Size (bytes):	344855
Entropy (8bit):	5.299148755710273
Encrypted:	false
SSDEEP:	6144:AxSzp/o/iitbtNUaeRjLSuE4kIOFAweV0AAF:Ak1ottxNUNjLStrfeV07

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\site.min[1].js	
MD5:	D06B9C7BBDB584E891AF7470C540373F
SHA1:	9E09177E303D5EC1876E1183842BFE60D4BCBC17
SHA-256:	1D96DED3CBB2E05D247CA03185BA021F790DBE8AABDD03DF56BBC27AB84BD7D6
SHA-512:	C53D4C04BA93098544DC3C9EDA61CA61D72153F3B871E36786F5961CBB6E6BB8FB567D215D8B04B487825535E4313A313DDB4F0D38CCFB6E7EFB45DE5900C9E
Malicious:	false
IE Cache URL:	http://https://workflowy.com/media/js/site.min.js
Preview:	!function(e){function t(t){for(var n,o,i=t[0],a=t[1],u=0,c=[];u<i.length;u++)o=i[u],r[o]&&c.push(r[o][0]),r[o]=0;for(n in a)Object.prototype.hasOwnProperty.call(a,n)&&(e[n]=a[n]);for(l&&l(t);c.length;)c.shift()()}var n={},r={17:0};function o(t){if(n[t])return n[t].exports;var r=n[t]={i:t,l:!1,exports:{}};return e[t].call(r.exports,r,r.exports,o),r.l=!0,r.exports}o.e=function(e){var t=[],n=r[e];if(0!==n)if(n)t.push(n[2]);else{var i=new Promise(function(t,o){n=r[e]=[t,o]});t.push(n[2]=i);var a,u=document.createElement("script");u.charset="utf-8",u.timeout=120,o.nc&&u.setAttribute("nonce",o.nc),u.src=function(e){return o.p+""+{0:"6f0b670eddaac85c5e4a",1:"8503ebe23bbb553931eb",2:"691a58eec3574cfa110c",3:"b27f856295365a42f064",4:"8c28c7d27117534a86a4",5:"1524dae43e7dbf404f3f",6:"65247b01f18ac82607ac",7:"9ca9fbac43f0e272661a",8:"e42577a28f6c3e306a7f",9:"5ba570c48ff05a4b5218",10:"7fb5d00134d0d26577a6",11:"adf9fc155506e2fa3fbf",12:"f216138f9312c91eee7d",13:"018fa7a115dcad40b512"}[e]+".js"}(e);

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\eaeea54ab7[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped
Size (bytes):	24
Entropy (8bit):	2.459147917027245
Encrypted:	false
SSDEEP:	3:CUXJ/lH:Dl
MD5:	BC32ED98D624ACB4008F986349A20D26
SHA1:	2D3DF8C11D2168CE2C27E0937421D11D85016361
SHA-256:	0C9CF152A0AD00D4F102C93C613C104914BE5517AC8F8E0831727F8BFBE8B300
SHA-512:	71ACC6DA78D5D5BF0EEA30E2EE0AC5C992B00EFEC959077DFE0AB769F1DBBD9AF12D5C5C155046283D5416BEB606A9EF323FB410E903768B1569B69F37075B4E
Malicious:	false
Preview:	GIF89a.......,..........

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\favicon[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 6 icons, 256x256, 32 bits/pixel, 128x128, 32 bits/pixel
Category:	downloaded
Size (bytes):	370070
Entropy (8bit):	4.80845072778125
Encrypted:	false
SSDEEP:	1536:ZD48rp0/IBXhIyuy/7rbkQblJ0AA/NPwITv:28e/IBXjxA1IITv
MD5:	F411E7E8A5B13EB1DE3974675C0D8CFC
SHA1:	86E1C2A83787FF51333BA6CF512A7C125DE16429
SHA-256:	D183C18DB92DD74B44320182C14B12A627B9F0A836776A7E0C263BE8D2792995
SHA-512:	2B5371D4A7539CD1F142B62BCA89CC806A6A7CE98851BC8AAA103BFD2CF2862F1680A513E0AB65783B88DCA84525B251DFC026172D553F76796D7F4A16C7426
Malicious:	false
IE Cache URL:	http://https://workflowy.com/media/i/favicon.ico
Preview:	....(..f......... .(.... ..@@.... .(B...(..00.... ..%...j.. .... .h.......(............. ....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\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:	53A2B560B20551672FBB0E6E72632D4FD1C7E2DD2ECF7337EBAAAB179CB8BE7C87E9D803CE7765706BC7FCBCF993C34587CD1237DE5A279AEA19911D69067B65
Malicious:	false
IE Cache URL:	http://https://code.jquery.com/jquery-3.1.1.min.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\jquery-3.1.1.min[1].js	
Preview:	/*! jQuery v3.1.1 | (c) jQuery Foundation | jquery.org/license */!function(a,b){"use strict";"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a document");return b(a)}:b(a)}("undefined"!=typeof window?window:this,function(a,b){"use strict";var c=[],d=a.document,e=Object.getPrototypeOf,f=c.slice,g=c.concat,h=c.push,i=c.indexOf,j={},k=j.toString,l=j.hasOwnProperty,m=l.toString,n=m.call(Object),o={};function p(a,b){b=b||d;var c=b.createElement("script");c.text=a,b.head.appendChild(c).parentNode.removeChild(c)}var q="3.1.1",r=function(a,b){return new r.fn.init(a,b)},s=/^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g,t=/^-ms-/,u=/-([a-z])/g,v=function(a,b){return b.toUpperCase()};r.fn=r.prototype={jquery:q,constructor:r,length:0,toArray:function(){return f.call(this)},get:function(a){return null==a?f.call(this):a<0?this[a+this.length]:this[a]},pushStack:function(a){var b=r.merge(this.con

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\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:	CAB8C4AFA1D8E3A8B7856EE29AE92566D44CEEAD70C8D533F2C98A976D77D0E1D314719B5C6A473789D8C6B21EBB4B89A6B0EC2E1C9C618FB1437EBC77D3A269
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).parentNode.removeChild(c)}var q="3.2.1 -ajax,-ajax/jsonp,-ajax/load,-ajax/parseXML,-ajax/script,-ajax/var/location,-ajax/var/nonce,-ajax/var/rquery,-ajax/xhr,-manipulation/_e

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\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/umH4N0IPfKu5AA11vrIY:9pZcYmDcHwFygmY1PfjAA1Br3
MD5:	6A07DA9FAE934BAF3F749E876BBFDD96
SHA1:	46A436EBA01C79ACDB225757ED80BF54BAD6416B
SHA-256:	D8AA24ECC6CECB1A60515BC093F1C9DA38A0392612D9AB8AE0F7F36E6EEE1FAD
SHA-512:	E525248B09A6FB4022244682892E67BBF64A3E875EB889DB43B0A24AB4A75077B5D5D26943CA382750D4FEBC3883193F3BE581A4660065B6FC7B5EC20C4A044B
Malicious:	false
IE Cache URL:	http://https://code.jquery.com/jquery-3.3.1.js
Preview:	/*!. * jQuery JavaScript Library v3.3.1. * https://jquery.com/. *. * Includes Sizzle.js. * https://sizzlejs.com/. *. * Copyright JS Foundation and other contributors. * Released 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\INetCache\IE\PSUEOSZZ\jquery.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	85578
Entropy (8bit):	5.366055229017455
Encrypted:	false
SSDEEP:	1536:EYE1JVoiB9JqZdXXe2pD3PgoIiulrUndZ6a4tfOR7WpfWBZ2BJda4w9W3qG9a986:v4J+OlfOhWppCW6G9a98Hr2
MD5:	2F6B11A7E914718E0290410E85366FE9
SHA1:	69BB69E25CA7D5EF0935317584E6153F3FD9A88C
SHA-256:	05B85D96F41FFF14D8F608DAD03AB71E2C1017C2DA0914D7C59291BAD7A54F8E
SHA-512:	0D40BCCAA59FEDECF7243D63B33C42592541D0330FEFC78EC81A4C6B9689922D5B211011CA4BE23AE22621CCE4C658F52A1552C92D7AC3615241EB640F8514B
Malicious:	false
IE Cache URL:	http://https://ajax.googleapis.com/ajax/libs/jquery/2.2.4/jquery.min.js

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\js[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	236106
Entropy (8bit):	5.533561304172417
Encrypted:	false
SSDEEP:	3072:gkcJX1bt8LWk0R6BjrHZvl/A38cJxcI8X1bt8iWk0R6BjrHgvl/Ata1hQz:1uXYFzxKbgXPFzQ1a
MD5:	996189BBAA2186177F20B284BB5FB131
SHA1:	B78B0264EB3939FDE6E072A4514994F63D06A0A1
SHA-256:	658E7FF38BED42EA22BBC96E0A763B7081C925A33493582356540328CD008CAD
SHA-512:	9CBA04D2F9FA38120E995A9966A6F24971A27166A2B2F429DD42B75DFAEE30A1B2C1BE53A719D90C0B103AABDDDDF48269A0B46F6E657821A2294162BD77CA8
Malicious:	false
IE Cache URL:	http://https://www.googletagmanager.com/gtag/js?id=G-58EY0922SL&l=dataLayer&cx=c
Preview:	.// Copyright 2012 Google Inc. All rights reserved..(function(){..var data = {."resource": {. "version":"1",. . "macros":[{. "function":"__e". },{. "function":"__c",. "vtp_value":"undefined". }],. "tags":[{. "function":"__rep",. "vtp_containerId":"UA-11472180-1",. "vtp_remoteConfig":["map"],. "tag_id":1. },{. "function":"__zone",. "vtp_childContainers":["list",["map","publicId","G-58EY0922SL"]],. "tag_id":3. }],. "predicates":[{. "function":"_eq",. "arg0":["macro",0],. "arg1":"gtm.js". }],. "rules":[. [["if",0],["add",0,1]]].},."runtime":[].....};./*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var aa,ba=function(a){var b=0;return function(){return b<a.length?{done:!1,value:a[b++]}:{done:!0}}},ca="function"==typeof Object.create?Object.create:function(a){var b=function(){};b.prototype=a;return new b},da;if("function"==typeof Object.setPrototypeOf)da=Object.setPro

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\login[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):	7301
Entropy (8bit):	5.357066025426497
Encrypted:	false
SSDEEP:	96:Awj4cNN8Afppuu5EVJSWhGUUkIkKyOd0JbAWAbEbaxx33GNNqkUka6WqyZ4bEm9d:ADu5S5YUudwkNL33GXbgqNt
MD5:	5462057035E108135972ABB914FB85A8
SHA1:	580BDFA18401421EC757AA11F6138BE4DE233D6B
SHA-256:	357F8DC902E87B5F314CBCC917B670FE608B3284BE46ED5AD083A64D9126FF99
SHA-512:	E8429B1EA465EAE47132E08149EA7976176A63CF1A72E55918DC8A6C107B3EC270B838902492DF8E78640DC96BF434CC943AEDE9D5E78CE88DA28D440066173
Malicious:	false
IE Cache URL:	http://https://workflowy.com/login/?next=/s/this-document-is-too/Tdcv9KOl0AuohEPI
Preview:	<!doctype html><html><head><title>Log in to WorkFlowy</title><meta http-equiv="X-UA-Compatible" content="chrome=1"/><link href="https://fonts.googleapis.com/css?family=Open+Sans:300,400,700,800" rel="stylesheet" type="text/css"/><meta name="ahrefs-site-verification" content="1e02598fc87129fdd8624212a90901b5a29fe287c590c9740af3c21f34784f42"/><link rel="shortcut icon" type="image/x-icon" href="/media/i/favicon.ico"/><link rel="apple-touch-icon" href="/media/i/icon-57x57.png"/><link rel="apple-touch-icon" sizes="72x72" href="/media/i/icon-72x72.png"/><link rel="apple-touch-icon" sizes="114x114" href="/media/i/icon-114x114.png"/><link rel="apple-touch-startup-image" sizes="768x1004" href="/media/i/workflowy-startup-image-ipad.png"/><link rel="apple-touch-startup-image" href="/media/i/workflowy-startup-image.png"/><meta name="apple-mobile-web-app-status-bar-style" content="black"/><meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=0"/><met

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\mem5YaGs126MiZpBA-UN7rgOUuhv[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 18900, version 1.1
Category:	downloaded
Size (bytes):	18900
Entropy (8bit):	7.96514104643824
Encrypted:	false
SSDEEP:	384:nejx4dDcsFhu/3v79dEAUdH6XSw1fz9fKQm9LQNG/X1epB:ejadDrhYTf3Udaieza98Nbz
MD5:	1F85E92D8FF443980BC0F83AD7B23B60
SHA1:	EE8642C4FAE325BB460EC29C0C2C9AD8A4C7817D
SHA-256:	EA20E5DB3BA915C503173FAE268445FC2745FC9A5DCE2F58D47F5A355E1CDB18
SHA-512:	F34099C30F35F782C8BB2B92D7F44549013D90E9EEDE13816D4C7380147D5B2C8373CC4D858CDF3248AAA8A73948350340EE57DAE9734038FC80615848C7133E
Malicious:	false
IE Cache URL:	http://https://fonts.gstatic.com/s/opensans/v18/mem5YaGs126MiZpBA-UN7rgOUuhv.woff

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\mem5YaGs126MiZpBA-UN7rgOUuhv[1].woff	
Preview:	wOFF.....l.....p.....GDEF.....GPOS.....GSUB.....X...t...OS/2.....^...`....cmap...`.....X..cvt .....]....-..fpgm...t.....s.ugasp.....glyf...$ ..9...Y..(.head..A....6...6.%I.hhea..B,.....$.)..hmtx..BL.....O,loca..D`.....9yfmaxp..F$... ... .q..name..FD.....#.>.post..G4.....x.U..prep..H.....k..... .....x...5.A.....m."gW..`.L..&N".?.....IF....a.^...b1.....Uh."4...>..=x.c`f.g.....:....Q.B3_dHc.....@`...../..?....^..... 9.8.m@J....w..!..x.\.!..q.....#aff...#1Q@ .'U..@5.".llt.Aa#.f|c.W.....'..X..!..C...ITPE.;..V.j.....0. .L0E...Yd.mN....:....F....GG.g.s,x.>0....v..I;o..<.$G9.\f2...e{}.IS2..uc]p.....M.x.c.a.g``..$KY...e@.,q@.j...o@<..O.H.t..... .....c .p@.....3lbd.....-.}.M...!...!....x.TGw.F.....)..)7.W..`*.j.-...=*'_..sI...2...O>....[tt....TK]..|...G.....^.m..=..x.q...+./].p...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\mem5YaGs126MiZpBA-UN8rsOUuhv[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 19072, version 1.1
Category:	downloaded
Size (bytes):	19072
Entropy (8bit):	7.966673384993769
Encrypted:	false
SSDEEP:	384:UCwUC2nJxPRk+P/Qvm6DBM1W71wcdDmyBE+2fweE9m0aGuTeopiH:PJC2nJxP++P/36QWpwNyb2tqgk
MD5:	05EBDBE10796850F045FCD484F35788D
SHA1:	07744CFE76B8C37096443A6BCC3FBD04F93AD05B
SHA-256:	35EB714D45479FE35586513C7D372CED0AE3E26EB05883950BEA2669C6E802AA
SHA-512:	D4F293115640C05E3134D635AA077BC91BF35E80463C93C14646D97784CD9FC8D4CD4E10EEAA7BE621DBD9FA0DE5BE943328014ED505C217E61769F76BFA7F4
Malicious:	false
IE Cache URL:	http://https://fonts.gstatic.com/s/opensans/v18/mem5YaGs126MiZpBA-UN8rsOUuhv.woff
Preview:	wOFF.....J.....p.....GDEF.....GPOS.....GSUB.....X...t...OS/2.....^...`...vcmap...`.....X..cvt .....g.....o.[fpgm...|.....s.ugasp... .....#glyf...0 ..:"..Yr....head..BT...6...6....hhea..B.....$....hmtx..B....*....#.C.loca..D.....n..maxp..F.... ... .name..F.....%.@cpost..G.....x.U..prep..lp.....1..S..... x...5.A.....m."gW..`.L..&N".?.....IF....a.^...b1.....Uh."4...>..=x.c`f.cV``e``..j...(.../2.11s01qs.1s.01.400.300x.....:.;380(...&.O.....)B..q>H.%.u..R``.....x.\.!..q..... .#aff...#1Q@.'U..@5.".llt.Aa#.f\|c.W.....'..X..!..C...ITPE.;..V.j.....0. .L0E...Yd.mN....:.....F....GG.g.s,x.>0....v..I;o..<.$G9.\f2...e{}.IS2..uc]p.....M.x.c.a.g``..$K..(..`.e.a.a`....C ..L..@t.....A..L..&.....1\gta.e....320.0...2.g.j...=...x.TGw.F.....)..)7.W..`*.j.-...=*'_..sI...2...O>....[tt....TK]..|...G.....^.m..=..x.q...+.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\nr-1184.min[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):	27995
Entropy (8bit):	5.315806784478887
Encrypted:	false
SSDEEP:	384:yZevj5JLnX8Rfz4cNc4esZt2mwUyAH77jx+zaTgEgi2bikgHIvxYocboatVFKFJb:yZUrW13Zt2A7pFFIpYo8ltqWE5
MD5:	3D7F312BE60D08A2568E311E4762F3AF
SHA1:	EDC028ACC27FB8DC6E2106A071A03AE7F93DC3B4
SHA-256:	780861F2AB29C0144055244696561FB0306C8CB3CB7F548F9105C763B0E91F77
SHA-512:	01507CB531465D496E475994A901D2E54E654810BDADE13BEB0480E9CA75FC92B0E4A5689646CC17FC2B10F93F00C1B000CD5B7C9B024F4A7A60F97905C1658I
Malicious:	false
IE Cache URL:	http://https://js-agent.newrelic.com/nr-1184.min.js
Preview:	!function(n,e,t){function r(t,i){if(!e[t]){if(!n[t]){var a="function"==typeof __nr_require&&__nr_require;if(!i&&a)return a(t,!0);if(o)return o(t,!0);throw new Error("Cannot find mo dule '"+t+"'")}var u=e[t]={exports:{}};n[t][0].call(u.exports,function(e){var o=n[t][1][e];return r(o||e)},u,u.exports)}return e[t].exports}for(var o="function"==typeof __nr_requir e&&__nr_require,i=0;i<t.length;i++)r(t[i]);return r}({1:[function(n,e,t){e.exports=function(n,e){return"addEventListener"in window?window.addEventListener(n,e,!1):"attach Event"in window?window.attachEvent("on"+n,e):void 0}},{}],2:[function(n,e,t){function r(n,e,t,r,i){l[n]||(l[n]={});var a=l[n][e];return a||(a=l[n][e]={params:t||{}},i&&(a.custom=i)),a.metrics=o(r,a.metrics),a}function o(n,e){return e||(e={count:0}),e.count+=1,f(n,function(n,t){e[n]=i(t,e[n])}),e}function i(n,e){return e?(e&&!e.c&&(e={t:e.t,min:e.t, max:e.t,sos:e.t*e.t,c:1}),e.c+=1,e.t+=n,e.sos+=n*n,n>e.max&&(e.max=n),n<e.min&&(e.min=n),e):{t:n}}function a(n,e){return

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\Tdcv9KOl0AuohEPI[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	15359
Entropy (8bit):	5.427707213531538
Encrypted:	false
SSDEEP:	384:doPdCvSS/yNrbLXTkc4SRzKeO0bT9GVYlTrcRUn0c0aOuPgl5YGm3TF9:doPNwcDPDbT/tQRUnuaOPmGm3Tv
MD5:	62323B1FEF7F6342B6EC09142301C386
SHA1:	07839ECAC668EEEBBC7E1F8F09E08F419A2AF99B
SHA-256:	E18D9AD2C80E45EEF2E95957985F20A4325822CBC181D24476739F0B003A208E
SHA-512:	F8477A33D15C4E4BECE1DF24DB755401E23F7F87A2FBCC4BC40C1190EE3485AE030C01728B050181E95E3B6DAC9065997FACB70E8EEC5914BE70D16178D5E9 C
Malicious:	false
Preview:	<!DOCTYPE html>...<html>. <head>. <meta charset="utf-8">. <meta http-equiv="X-UA-Compatible" content="chrome=1"><script type="text/javascript">(window.NR EUM||(NREUM={})).loader_config={licenseKey:"eaeea54ab7",applicationID:"61695248"};window.NREUM||(NREUM={}),__nr_require=function(e,t,n){function r(n){if(!t[n]){ var i=t[n]={exports:{}};e[n][0].call(i.exports,function(t){var i=e[n][1][t];return r(i||t)},i,i.exports)}return t[n].exports}if("function"==typeof __nr_require)return __nr_require;for(var i=0;i<n.length;i++)r(n[i]);return r}({1:[function(e,t,n){function r(){}function i(e,t,n){return function(){return o(e,[u.now()].concat(c(arguments)),t?null:this,n),t?void 0:this}}var o=e("handle"),a=e(6),c=e(7),f=e("ee").get("tracer"),u=e("loader"),s=NREUM;"undefined"==typeof window.newrelic&&(newrelic=s);var d=["setPageViewName","setCustom Attribute","setErrorHandler","finished","addToTrace","inlineHit","addRelease"],p="api-",l=p+"ixn-";a(d,function(e,t){s[t]=i(p+t,!0,"api")}),s.addPageA

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\analytics[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	47051
Entropy (8bit):	5.516264124030958
Encrypted:	false
SSDEEP:	768:ryOveCSBZfsnt5XqY/yPndFTkoWY3SoavqVy2rlebYUDTJC6g0stZm:ryJNDfs5hYdFTwY3SorSg0su
MD5:	53EE95B384D866E8692BB1AEF923B763
SHA1:	A82812B87B667D32A8E51514C578A5175EDD94B4
SHA-256:	E441C3E2771625BA05630AB464275136A82C99650EE2145CA5AA9853BEDEB01B
SHA-512:	C1F98A09A102BB1E87BFDF825A725B0E2CC1DBEDB613D1BD9E8FD9D8FD8B145104D5F4CACA44D96DB14AC20F2F51B4C653278BFC87556E7F00E48A5FA6231AD
Malicious:	false
IE Cache URL:	http://https://www.google-analytics.com/analytics.js
Preview:	(function(){/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var l=this||self,m=function(a,b){a=a.split(".");var c=l;a[0]in c||"undefined"==typeof c.execScript||c.execScript("var "+a[0]);for(var d;a.length&&(d=a.shift());)a.length||void 0===b?c=c[d]&&c[d]!==Object.prototype[d]?c[d]:c[d]={}:c[d]=b};var q=function(a,b){for(var c in b)b.hasOwnProperty(c)&&(a[c]=b[c])},r=function(a){for(var b in a)if(a.hasOwnProperty(b))return!0;return!1};var t=/^(?:(?:https?|mailto|ftp):|[^:/?#]*(?:[/?#]|$))/i;var u=window,v=document,w=function(a,b){v.addEventListener?v.addEventListener(a,b,!1):v.attachEvent&&v.attachEvent("on"+a,b)};var x={},y=function(){x.TAGGING=x.TAGGING\|\|[];x.TAGGING[1]=!0};var z=/:[0-9]+$/,A=function(a,b,c){a=a.split("&");for(var d=0;d<a.length;d++){var e=a[d].split("=");if(decodeURIComponent(e[0]).replace(/\+/g," ")===b)return b=e.slice(1).join("="),c?b:decodeURIComponent(b).replace(/\+/g," ")}},D=function(a,b){b&&(b=String(b).toLowerCase());if("p

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\e42577a28f6c3e306a7f[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	6932
Entropy (8bit):	5.314316385992555
Encrypted:	false
SSDEEP:	192:q76Udb4Zz7Gf3XmkhlmClBRQ/IaAjL5d5P1n1:g60SGfrhplBRQ/IhjL5T
MD5:	AD5D37EB59C3360ECE2973696A3520D4
SHA1:	74E94926731088E2CCD62DD065CDB1B7316FF1AA
SHA-256:	1463EEA0C3698C8760F805F7720FC1A8195AF56227DF0D22CCEB1955C2858646
SHA-512:	BAE6B49423CA1AB5EB8120E63B1ACE31DB57CE5C830749A3F86FF219733B8B90F2E2C1D54D616B4FB9B8DA6699499FFBFBD978F0EE13EA20E94A017B39CC9856
Malicious:	false
IE Cache URL:	http://https://workflowy.com/media/js/e42577a28f6c3e306a7f.js
Preview:	(window.webpackJsonp=window.webpackJsonp||[]).push([[8],{921:function(e,t,n){"use strict";var a=n(0),r=n(3),i=function(){return(i=Object.assign||function(e){for(var t,n=1,a=arguments.length;n<a;n++)for(var r in t=arguments[n])Object.prototype.hasOwnProperty.call(t,r)&&(e[r]=t[r]);return e}).apply(this,arguments)};function o(e){return JSON.stringify(e).replace(/\u2028/g,"\\u2028").replace(/\u2029/g,"\\u2029").replace(/<\//g,"<\\/")}var l=a.memo(function(e){var t=e.title,n=e.description,l=e.style,c=e.children,s=e.context;return a.useEffect(function(){document.title=t},[t]),Object(r.g)("html",{margin:0,padding:0,height:"100%"}),Object(r.g)("body",i({margin:0,padding:0,height:"100%"},l)),Object(r.g)("#page",{height:"100%"}),s.pageOnly?c:a.createElement("html",null,a.createElement("head",null,a.createElement("title",null,t),n&&a.createElement("meta",{name:"description",content:n}),a.createElement("meta",{httpEquiv:"X-UA-Compatible",content:"chrome=1"}),a.createElement("link",{href:"https://

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\eaeea54ab7[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped
Size (bytes):	24
Entropy (8bit):	2.459147917027245
Encrypted:	false
SSDEEP:	3:CUXJ/lH:Dl
MD5:	BC32ED98D624ACB4008F986349A20D26
SHA1:	2D3DF8C11D2168CE2C27E0937421D11D85016361
SHA-256:	0C9CF152A0AD00D4F102C93C613C104914BE5517AC8F8E0831727F8BFBE8B300
SHA-512:	71ACC6DA78D5D5BF0EEA30E2EE0AC5C992B00EFEC959077DFE0AB769F1DBBD9AF12D5C5C155046283D5416BEB606A9EF323FB410E903768B1569B69F37075B4E
Malicious:	false
Preview:	GIF89a.....,.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\eaeea54ab7[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	57
Entropy (8bit):	4.31817604175005
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\eaeea54ab7[1].js	
SSDEEP:	3:U3KTDWuvMiqVkMWVrfUh:HnNukMWVr8h
MD5:	79F2D634CE67570918939DF10A075576
SHA1:	BA47B7DACB11250F9B1B3974B34954B188E3ECAD
SHA-256:	D10C94B6CDB747904BAEE9070F003BB45849DA46F8100B1320F286C21CBCAAA1
SHA-512:	155FAB1EC68F300DDCB948D024995539C721A2AB0FD89C220F0EFFA68C3863507CBEF806F087F5C84EAB38D4C53DA94BC893894E8FC9DED388DACFE3244E18E
Malicious:	false
Preview:	NREUM.setToken({'stn':1,'err':1,'ins':1,'cap':0,'spa':1})

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\free-fa-regular-400[1].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), Font Awesome 5 Free Regular family
Category:	downloaded
Size (bytes):	34350
Entropy (8bit):	6.320570887190345
Encrypted:	false
SSDEEP:	384:HbFILSQt3owpXUazLuDULbNVTH/oOkKQB3I+89AyI6WcRwkRcQUta:HbeLSe3yy6DOP/oDB29uc5RcQUA
MD5:	991B587DBEE2E132C9542FB1280F1372
SHA1:	660DA8C03735C9DFFB26205AAD19EA6B1916268A
SHA-256:	44F6500D0D5D7F3F8422B9790EAA47DF4E1D812C90239602E53429376B96D1DF
SHA-512:	A9AF4B58640B47D1EF7B6E2126BA6908AF9A4027D3961E3889732E433B9CED8E49F0BB17E54FEA602FFC46E93206DBA088EFC9CC41940477C3DCC3687D0C9BD
Malicious:	false
IE Cache URL:	http://https://ka-f.fontawesome.com/releases/v5.15.1/webfonts/free-fa-regular-400.eot?
Preview:	.....LP.....6.F.o.n.t. .A.w.e.s.o.m.e. .5. .F.r.e.e. .R.e.g.u.l.a.r.....R.e.g.u.l.a.r...L.3.3.1...5.2.1. .(.F.o.n.t. .A.w.e.s.o.m.e. .v.e.r.s .i.o.n.:. .5...1.5...1.)...6.F.o.n.t. .A.w.e.s.o.m.e. .5. .F.r.e.e. .R.e.g.u.l.a.r.....PFFTM.,.....GDEF.*.....OS/2A.S....X...`cmap.....gasp.....glyf|.7.... ..n.head.. .....6hhea.5.....$hmtx...t.....Tloca.e.....6maxp.....8... name8.8"..w....[post.iA...}.....K.`.._.<.....w.....z.....@. .....L.f...G.L.f.....PfEd.....T.....:.... .....@.....@.....@.....@.....@...@.....@...@..... ..`.....@.....@.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\free-fa-solid-900[1].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), Font Awesome 5 Free Solid family
Category:	downloaded
Size (bytes):	204814
Entropy (8bit):	6.34341654497633
Encrypted:	false
SSDEEP:	6144:5t+zd6McnODzpN2BDXTIRSwRKSK3NC5xMG:GELnODze58Rjg+55
MD5:	D3B45D588F61AB38CB31CBA544B4373C
SHA1:	627D2C71A5FFC7E5F17DA0897EE1B73CD30D255F
SHA-256:	366C63E48A15576AA55ED76DB0EBCCA8BCE15F6EFC881BD0AC75982FF1233699
SHA-512:	6D178A6671E6C1E4148770A4FD6351FD237628A48748047006B350E3FBD2BDFD0257BD908BAA26606D3326FE2F7D1E80B505E533716D9EFE8490A6EEC99D83BC
Malicious:	false
IE Cache URL:	http://https://ka-f.fontawesome.com/releases/v5.15.1/webfonts/free-fa-solid-900.eot?
Preview:	. .....LP.....O..O.....2.F.o.n.t. .A.w.e.s.o.m.e. .5. .F.r.e.e. .S.o.l.i.d.....S.o.l.i.d...L.3.3.1...5.2.1. .(.F.o.n.t. .A.w.e.s.o.m.e. .v.e.r.s.i.o.n.:. .5...1.5...1.)...2.F.o.n.t. .A.w.e.s.o.m.e. .5. .F.r.e.e. .S.o.l.i.d.....PFFTM.,.....GDEF.*.....OS/23.V`...X...`cmap.j.4...h....gasp.....glyfh.....-....dhead.,.....6 hhea.C.-.....$hmtx.Q.....loca.....8....maxp.N.`...8... name!.-....P...+post..Fa...|..1.....K.`O..O_.<.....x.....z.....]. .....@..... .....L.f...G.L.f.....PfEd.....T.....:.... .....@.....@. .....@.....@..... .....@.....`.....@.....@.....@.....@....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\free-v4-shims.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	26701
Entropy (8bit):	4.829785000026929
Encrypted:	false
SSDEEP:	192:bP6hT1bIl4w0QUmQ10PwKLaAu5CwWavpHo4O6wgLPbJVR8XD7mycP:Ohal4w0QK+PwK05eavpmgPPeXD7mycP
MD5:	2E4C3DA4EAE1C876A281D6CA5A7A5B4C
SHA1:	92AD084AAB53B7AA8C761CD66BDFB1F79B9CAED7
SHA-256:	CFFF9EA502195A7B96FE38DECA9188A59B758DEEECC2CD4E78AEA7D911E638C6
SHA-512:	F324F308649F47E3C25BF021C1776A4326750D04D9392B7F200331E806514B69E7579FB23D7B2107A3B30CB96926554C0DE13F45FD1397BDAE89938DD52A7EBF
Malicious:	false
IE Cache URL:	http://https://ka-f.fontawesome.com/releases/v5.15.1/css/free-v4-shims.min.css

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\free-v4-shims.min[1].css	
Preview:	/*!. * Font Awesome Free 5.15.1 by @fontawesome - https://fontawesome.com. * License - https://fontawesome.com/license/free (Icons: CC BY 4.0, Fonts: SIL OFL 1.1, Code: MIT License). */.fa.fa-glass:before{content:"\f000"}.fa.fa-meetup{font-family:"Font Awesome 5 Brands";font-weight:400}.fa.fa-star-o{font-family:"Font Awesome 5 Free";font-weight:400}.fa.fa-star-o:before{content:"\f005"}.fa.fa-close:before,.fa.fa-remove:before{content:"\f00d"}.fa.fa-gear:before{content:"\f013"}.fa.fa-trash-o{font-family:"Font Awesome 5 Free";font-weight:400}.fa.fa-trash-o:before{content:"\f2ed"}.fa.fa-file-o{font-family:"Font Awesome 5 Free";font-weight:400}.fa.fa-file-o:before{content:"\f15b"}.fa.fa-clock-o{font-family:"Font Awesome 5 Free";font-weight:400}.fa.fa-clock-o:before{content:"\f017"}.fa.fa-arrow-circle-o-down{font-family:"Font Awesome 5 Free";font-weight:400}.fa.fa-arrow-circle-o-down:before{content:"\f358"}.fa.fa-arrow-circle-o-up{font-family:"Font Awesome 5 Free";font-weight:400}.fa.fa-arro

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\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-variant:normal;text-rendering:auto;line-height:1}.fa-lg{font-size:1.33333em;line-height:.75em;vertical-align:-.0667em}.fa-xs{font-size:.75em}.fa-sm{font-size:.875em}.fa-1x{font-size:1em}.fa-2x{font-size:2em}.fa-3x{font-size:3em}.fa-4x{font-size:4em}.fa-5x{font-size:5em}.fa-6x{font-size:6em}.fa-7x{font-size:7em}.fa-8x{font-size:8em}.fa-9x{font-size:9em}.fa-10x{font-size:10em}.fa-fw{text-align:center;width:1.25em}.fa-ul{list-style-type:none;margin-left:2.5em;padding-left:0}.fa-ul>li{position:relative}.fa-li{left:-2em;position:absolute;text-align:center;width:2em;line-height:inherit}.fa-border{border:.08em solid #eee;border-radius:.1em;padding:.2em .25em .15em}.fa-pul

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\js[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	135362
Entropy (8bit):	5.543879784402906
Encrypted:	false
SSDEEP:	1536:LSJxcILAX1bKwn8qZWk0mA6wRV2RnjrY6/A+6NK8vTvJxx/JKj1P9GvKPGrlG+H8:eJxcI8X1bt8iWk0R6BjrHgvl/Ata1hQz
MD5:	A55FD4E3804FDBFE4866EFA2EC81DA48
SHA1:	84D7E3B561CAA718E4FDCBE757C9F51437FB8B61
SHA-256:	A30CA49C9DE677205368B37F4821C93261D085606824306B1F8B057DDFD622A5
SHA-512:	5684E4CB0839FA1E9FDEFA935610676012D454B84790140CDFBA5C655C86BC887CA4B42C68FDD7C16AD9294799E30B682C09362CE38184BBB551BC0342F3DAC A
Malicious:	false
Preview:	.// Copyright 2012 Google Inc. All rights reserved..(function(){..var data = {."resource": {. "version":"1",. . "macros":[{. "function":"__e". },{. "vtp_signal":0,. "function":"__c",. "vtp_value":0. },{. "function":"__c",. "vtp_value":"google.co.uk". },{. "function":"__c",. "vtp_value":false. },{. "function":"__aev",. "vtp_varType":"URL",. "vtp_component":"IS_OUTBOUND",. "vtp_affiliatedDomains":["list"]. },{. "function":"__v",. "vtp_name":"gtm.triggers",. "vtp_dataLayerVersion":2,. "vtp_setDefaultValue":true,. "vtp_defaultValue":"". },{. "function":"__v",. "vtp_name":"gtm.elementId",. "vtp_dataLayerVersion":1. },{. "function":"__v",. "vtp_name":"gtm.elementClasses",. "vtp_dataLayerVersion":1. },{. "function":"__aev",. "vtp_varType":"URL",. "vtp_component":"URL_NO_FRAGMENT". },{. "function":"__aev",. "vtp_varType":"URL"

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\js[2].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	100744
Entropy (8bit):	5.516236625985929
Encrypted:	false
SSDEEP:	1536:gkcJX1bKwn8LWk0mA6wRV2RnjrY6/3+6NK8vTvJxx/JKj1P9GSKPNAGFX6Z6X2xk:gkcJX1bt8LWk0R6BjrHZvl/A38h
MD5:	9471B1B754EEA7C7E93DF2BACC1A66BD
SHA1:	7D01ECDE61567BBB2037DC6729C7A9251420AC1F
SHA-256:	CC80E836B4E1336FD5B775C1019BF1F58F5281CC96AB0EC66A1B5D126D89257E
SHA-512:	235CF91B6BAFAAF468648A9CBA97ECD14AC102E5076F90F4964A86C57E72073CF8AEAB5943E2F1B5544AC88D92D6114A7C893B105A5A7F904D859589AF25BF6 C
Malicious:	false
IE Cache URL:	http://https://www.googletagmanager.com/gtag/js?id=UA-11472180-1

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\js[2].js	
Preview:	.// Copyright 2012 Google Inc. All rights reserved..(function(){..var data = {."resource": {. "version":"1",. . "macros":[{. "function":"__e". },{. "function":"__c",. "vtp_value":"undefined". }],. "tags":[{. "function":"__rep",. "vtp_containerId":"UA-11472180-1",. "vtp_remoteConfig":["map"],. "tag_id":1. },{. "function":"__zone",. "vtp_childContainers":["list",["map","publicId","G-58EY0922SL"]],. "tag_id":3. }],. "predicates":[{. "function":"_eq",. "arg0":["macro",0],. "arg1":"gtm.js". }],. "rules":[. [["if",0],["add",0,1]]].},."runtime":[].....};./*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var aa,ba=function(a){var b=0;return function(){return b<a.length?{done:!1,value:a[b++]}:{done:!0}}},ca="function"==typeof Object.create?Object.create:function(a){var b=function(){};b.prototype=a;return new b},da;if("function"==typeof Object.setPrototypeOf)da=Object.setPro

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\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\INetCache\IE\WJ8I2OL4\print[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	1316
Entropy (8bit):	4.5361774193775695
Encrypted:	false
SSDEEP:	24:Ev7iax0Ra6+G0EBxLCKrqwjtRiRRl/H+VEgTKwubs:Ev7ia6sG0E/CIJI56qo
MD5:	7471DC37D85CB2B6BAAC70B6A9312DB4
SHA1:	D4775C3D288899890AA0874D3F9AC33843680119
SHA-256:	858EBBB77D7504548FED0FB9088D90B774945E88B0464D42A44C4829A84B972D
SHA-512:	062806344E9E5904BF3A0DBAB95E4272C0D84DD654DD29BDCC95BC5FDBED6436B4D8C079425C94282FCDE57801D3B5B16820EA010A829624191A2CC4D771FC8
Malicious:	false
IE Cache URL:	http://https://workflowy.com/media/css/print.css
Preview:	.leftBar {. display: none;.}..body {. padding-left: 0 !important;.}...page {. border: none !important;.. /* Add space at top of page so there is some margin. */. margin-top: 0 !important;. margin-bottom: 0 !important;.. min-height: 10px !important;. box-shadow: none !important;.. /* Style the page width and margins so that they adjust dynamically. depending on width used for printing (and turn off the. transform that is normally used for this). We need to use pure. CSS for positioning the page when printing (rather than the JS. that adjusts things on 'resize' events normally) because we. don't know what the print width will be. */. width: auto !important;. max-width: 700px !important;. margin-left: auto !important;. margin-right: auto !important;. left: 0 !important;.. transform: none !important;. -webkit-transform: none !important;. -moz-transform: none !important;. -ms-transform: none !important;.}...mainTreeRoot {. min-height: 0px !im

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\signup[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):	7312
Entropy (8bit):	5.357545787870613
Encrypted:	false
SSDEEP:	96:jwj4cNN8AfppuL5EVJSWhGUUklkKyOd0JbAWAbEbaxx33GNNqkUka6WqyZXOREmi:jDL5S5YUudwkNL33GXbgevDPO
MD5:	8A0730731A4463EAF1E9C6057B1CE100
SHA1:	C654D4BC0F4FE542744603F4478A6EDAE4A4ED3E
SHA-256:	38DFDE1431EE46C01C9F41C1DF70DBEE7415BBE0C0C83787F2736330DEB59F48
SHA-512:	1E4B55AD170093209A66BC73A53BAC3A780761C02D35BA42E9A31B8FE3F97F7E201B07DB92C944E46A7181C06A4EC96CE2946FD8828A7A15D719F389AF18A88
Malicious:	false
IE Cache URL:	http://https://workflowy.com/signup/?next=/s/this-document-is-too/Tdcv9KOl0AuohEPI

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\signup[1].htm	
Preview:	<!doctype html><html><head><title>Sign up for WorkFlowy</title><meta http-equiv="X-UA-Compatible" content="chrome=1"/><link href="https://fonts.googleapis.com/css?family=Open+Sans:300,400,700,800" rel="stylesheet" type="text/css"/><meta name="ahrefs-site-verification" content="1e02598fc87129fdd8624212a90901b5a29fe287c590c9740af3c21f34784f42"/><link rel="shortcut icon" type="image/x-icon" href="/media/i/favicon.ico"/><link rel="apple-touch-icon" href="/media/i/icon-57x57.png"/><link rel="apple-touch-icon" sizes="72x72" href="/media/i/icon-72x72.png"/><link rel="apple-touch-icon" sizes="114x114" href="/media/i/icon-114x114.png"/><link rel="apple-touch-startup-image" sizes="768x1004" href="/media/i/workflowy-startup-image-ipad.png"/><link rel="apple-touch-startup-image" href="/media/i/workflowy-startup-image.png"/><meta name="apple-mobile-web-app-status-bar-style" content="black"/><meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=0"/><m

C:\Users\user\AppData\Local\Temp\mso7346.tmp	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	GIF image data, version 89a, 15 x 15
Category:	dropped
Size (bytes):	663
Entropy (8bit):	5.949125862393289
Encrypted:	false
SSDEEP:	12:PlrojAxh4bxdtT/CS3wkxWHMGBJg8E8gKVYQezuYEecp:trPsTTaWKbBCgVqSF
MD5:	ED3C1C40B68BA4F40DB15529D5443DEC
SHA1:	831AF99BB64A04617E0A42EA898756F9E0E0BCCA
SHA-256:	039FE79B74E6D3D561E32D4AF570E6CA70DB6BB3718395BE2BF278B9E601279A
SHA-512:	C7B765B9AFBB9810B6674DBC5C5064ED96A2682E78D5DFFAB384D81EDBC77D01E0004F230D4207F2B7D89CEE9008D79D5FBADC5CB486DA4BC43293B7AA87841
Malicious:	false
Preview:	GIF89a....w..!..MSOFFICE9.0.....sRGB.....!..MSOFFICE9.0.....msOPMSOFFICE9.0Dn&P3.!..MSOFFICE9.0.....cmPPJCmp0712.....!.....,.....'..;..b...RQ.xx.....,+.....yy..;..b.....qp.bb.....uv.ZZ.LL.....xw.jj.NN.A@....zz.mm.^_.....yw.....yx.xw.RR.,*.++,.....8...>.....4567...=.../0123.....<9:.()*+,-.B.@...."#$%&'..... !.....C.?....A;<...HT(..;

C:\Users\user\AppData\Local\Temp\~DF058B1B9EB731C27D.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.2882731879707672
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laA9:kBqoxxJhHWSVSEab9
MD5:	BE0715C655605A41D0FA9D032CF5EB0E
SHA1:	6FF18CC59646BD46EB0A2E2E337AE80D26E3FF4A
SHA-256:	95AAE1C424618EEFB9E49349B5AA69A7E5A635C77C63B29566AD8F735022BD7D
SHA-512:	195020E5FD193A5F6F51370C71BCC91708D15B1C3A2F7EEF6DA719DC345F0DF22B940E43A8F51ECEEA1B3DF79101F7844BF97116771DDFADB9B95C147374E9F
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF36F3C25722F1499C.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	75283
Entropy (8bit):	0.8969986130176656
Encrypted:	false
SSDEEP:	384:kBqoxKAuqR+PxzaB6/H4nH4+UkkApv6ybJCDZ7eZX6LI:XCoy
MD5:	D438260809F95DB7879BE7797E72E5F2
SHA1:	30DBCEEE4110A495CA8E9E60D09F8E716CC151D5
SHA-256:	E4E2B963F01ACD463F2021759B7F7D0FAC485CE15C6DC0432764B6FC2E34BC6C
SHA-512:	0AFF5920DA897EA2BD1E82DB3D90965D89CC24268D03C480A4C6B5D8EEDDB8AA83756B58DFC8D56864D3D3C70EE5160547E898A97C6E8E628F8591788D43EC
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF6E9E146EF88F1592.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe

C:\Users\user\AppData\Local\Temp\~DF6E9E146EF88F1592.TMP	
File Type:	data
Category:	dropped
Size (bytes):	13077
Entropy (8bit):	0.5139209429437767
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9logWtF9logWn9lWgWeEkSI7EkonPkoZkoZ6j:kBqoIdId2deEkSI7EkonPkoZkoZ6j
MD5:	5F01858715955C3A6560D118A5C26334
SHA1:	9BD6BB0A3FE76D81529A890D9E9DDDFB30CF6774
SHA-256:	EA4705CB6DB49598D1BAAA017BA21735A37D16A84F1FA9D158ABECE7530795BD
SHA-512:	A801126ECDEF3A908AC772A70C3E1DAABA230F1B3BFA240FEDEAF19984BBB584DB6A0E37E9DC1F8AAEFECFBD2EC055DDF3344CAB8996CFB31A67E8F4B2CF7C6C
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Fennec Pharma .docx.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Sep 30 14:03:41 2020, mtime=Sat Nov 21 09:13:47 2020, atime=Sat Nov 21 09:13:44 2020, length=49414, window=hide
Category:	dropped
Size (bytes):	2160
Entropy (8bit):	4.70618682599084
Encrypted:	false
SSDEEP:	24:8SfarlCAsgU6aDrU7aB6mySfarlCAsgU6aDrU7aB6m:8SfcsgexB6pSfcsgexB6
MD5:	0FEDED0CF14150972A8721826E80098B
SHA1:	507979AF9647CB30FE7B04E83428E315CDDFEEC4
SHA-256:	60A5B4C0746567E7D7FE04F9AAC8893CCB3DB22C7473B26F27DE6C714461EC48
SHA-512:	FCE8A044ECA196A74D3F58F0C7141017DBDF3D5D185B78556DC35B7C673B4EEED306EB5140D65EB709FAC56415BB041B7E8B4E47078F55646FCA17F0E5E6AEB4
Malicious:	false
Preview:	L.....F.... ...Whh.:.....;....N.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L..uQ.Q.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....P.1.....>Qvx..user.<.....Ny.uQ.Q.....S.....?.i.h.a.r.d.z.....~.1.....>Qwx..Desktop.h.....Ny.uQ.Q.....Y.....>.....f.D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....t.2.....uQ.Q .FENNEC~1.DOC..X.....>QuxuQ.Q....h.....F.e.n.n.e.c. .P.h.a.r.m.a. ...d.o.c.x.....Y.....-.....X.....>.S.....C:\Users\user\Desktop\Fennec Pharma .docx..*.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.F.e.n.n.e.c. .P.h.a.r.m.a. ...d.o.c.x.....:.,.LB.)...As...`.....X.....445817.....!a..%.H.VZAj...j..-.....-..!a..%.H.VZAj...j..-.....-.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.-.1

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	97
Entropy (8bit):	4.523248445579843
Encrypted:	false
SSDEEP:	3:HoAL/FX6BS7oFX6BSmxWoAL/FX6BSv:Hdx6BSe6Bax6Bc
MD5:	E92F8E71C858C8E1A08B13AE6EE6A4CB
SHA1:	E6C001C7436FF58889E9BEDF6464FA8CE7B4A62A
SHA-256:	F094AB6BEC7C65D56286E3423D5E903EBB6CDC3628B09C89AEA3EFCC94B3A13F
SHA-512:	3BD0839EACACF3C2D0CC43104408B84E74C620CCA75E2EA7C8C6072297C4CF4D8051B6ED61D375DD4955869C89E3ADE9535BAF27B67C6555A447C3E8BDB788A
Malicious:	false
Preview:	[misc]..Fennec Pharma .docx.LNK=0..Fennec Pharma .docx.LNK=0..[misc]..Fennec Pharma .docx.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.298238083977649
Encrypted:	false
SSDEEP:	3:Rl/ZdOP/7lqKjnbYl///9kwxJ:RtZ54bY1
MD5:	E157987597244361306D8870B9A09806
SHA1:	CB312F1B186434993C95567C33141F18A4818BF7
SHA-256:	A86FE6856CD666F79D1C5D56E369F5237732BD1FAAE13DBE546B9AFC00F1FBD3

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
SHA-512:	A8146E4B96A3314463E3AFA63EC62BEB770FCFCE4A427F0DF480C3B5D90760A55002C021797D3BA40C43A6E94C97390D717BC3E69DFD2C6E32153CCCF9EA275
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....|.$.....H.....6C.....|.%.....|-&.....T...

C:\Users\user\Desktop\~$nnec Pharma .docx	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.298238083977649
Encrypted:	false
SSDEEP:	3:Rl/ZdOP/7lqKjnbYl///9kwxJ:RtZ54bY1
MD5:	E1579875972443613O6D8870B9A09806
SHA1:	CB312F1B186434993C95567C33141F18A4818BF7
SHA-256:	A86FE6856CD666F79D1C5D56E369F5237732BD1FAAE13DBE546B9AFC00F1FBD3
SHA-512:	A8146E4B96A3314463E3AFA63EC62BEB770FCFCE4A427F0DF480C3B5D90760A55002C021797D3BA40C43A6E94C97390D717BC3E69DFD2C6E32153CCCF9EA275
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....|.$.....H.....6C.....|.%.....|-&.....T...

Static File Info

General

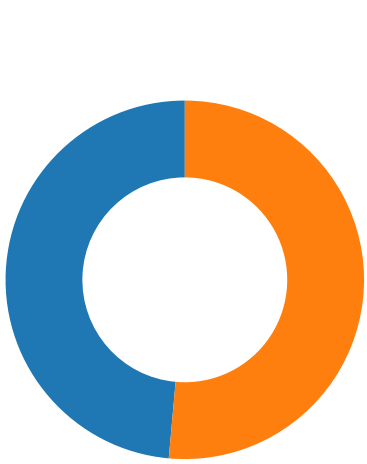
File type:	Microsoft Word 2007+
Entropy (8bit):	7.777800311829734
TrID:	• Word Microsoft Office Open XML Format document (49504/1) 49.01% • Word Microsoft Office Open XML Format document (43504/1) 43.07% • ZIP compressed archive (8000/1) 7.92%
File name:	Fennec Pharma .docx
File size:	49414
MD5:	e935876bc1daf073b5730cfef5ee1b6f
SHA1:	2f0444a05ac3eca81313712825fec001efceb3ac
SHA256:	494148b0b3b41783ae059b3344248b7ea1d5ce4a99f00c55f7631f9493d44483
SHA512:	7fe31a1910da1a1ad328224950f9cca2ca1934c4665699c4b9d4998ca031d8f23a8fd2115f73df2261fc06916257bc3d7e4837d351691e96f96a1dbe1dc81f25
SSDEEP:	768:AY8dpA6x2DTvT8XSm/CE0O2WtEHnlu62x5MHzcWwJ1PuA84Xon71y10lxllNicuO:+di6x8DT8Cm3+IA5UnwiRn41gBlZilqX
File Content Preview:	PK.....!...wj...._.....[Content_Types].xml ...(..... ....

File Icon

Icon Hash:	74fcd0d2d6d6d0cc

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 21, 2020 02:14:18.067675114 CET	49729	443	192.168.2.3	54.84.56.113
Nov 21, 2020 02:14:18.067912102 CET	49730	443	192.168.2.3	54.84.56.113
Nov 21, 2020 02:14:18.171215057 CET	443	49729	54.84.56.113	192.168.2.3
Nov 21, 2020 02:14:18.171264887 CET	443	49730	54.84.56.113	192.168.2.3
Nov 21, 2020 02:14:18.171458006 CET	49729	443	192.168.2.3	54.84.56.113
Nov 21, 2020 02:14:18.171495914 CET	49730	443	192.168.2.3	54.84.56.113
Nov 21, 2020 02:14:18.196891069 CET	49729	443	192.168.2.3	54.84.56.113
Nov 21, 2020 02:14:18.196964979 CET	49730	443	192.168.2.3	54.84.56.113
Nov 21, 2020 02:14:18.299741983 CET	443	49730	54.84.56.113	192.168.2.3
Nov 21, 2020 02:14:18.299787998 CET	443	49729	54.84.56.113	192.168.2.3
Nov 21, 2020 02:14:18.301151037 CET	443	49729	54.84.56.113	192.168.2.3
Nov 21, 2020 02:14:18.301202059 CET	443	49729	54.84.56.113	192.168.2.3
Nov 21, 2020 02:14:18.301230907 CET	443	49729	54.84.56.113	192.168.2.3
Nov 21, 2020 02:14:18.301261902 CET	443	49729	54.84.56.113	192.168.2.3
Nov 21, 2020 02:14:18.301291943 CET	443	49730	54.84.56.113	192.168.2.3
Nov 21, 2020 02:14:18.301331043 CET	443	49730	54.84.56.113	192.168.2.3
Nov 21, 2020 02:14:18.301368952 CET	443	49730	54.84.56.113	192.168.2.3
Nov 21, 2020 02:14:18.301409960 CET	49729	443	192.168.2.3	54.84.56.113
Nov 21, 2020 02:14:18.301440001 CET	49729	443	192.168.2.3	54.84.56.113
Nov 21, 2020 02:14:18.301450014 CET	443	49730	54.84.56.113	192.168.2.3
Nov 21, 2020 02:14:18.301466942 CET	49730	443	192.168.2.3	54.84.56.113
Nov 21, 2020 02:14:18.301501036 CET	49730	443	192.168.2.3	54.84.56.113
Nov 21, 2020 02:14:18.301506996 CET	49730	443	192.168.2.3	54.84.56.113
Nov 21, 2020 02:14:18.301512003 CET	49730	443	192.168.2.3	54.84.56.113
Nov 21, 2020 02:14:18.353482008 CET	49730	443	192.168.2.3	54.84.56.113
Nov 21, 2020 02:14:18.359318018 CET	49730	443	192.168.2.3	54.84.56.113
Nov 21, 2020 02:14:18.359571934 CET	49730	443	192.168.2.3	54.84.56.113
Nov 21, 2020 02:14:18.359751940 CET	49729	443	192.168.2.3	54.84.56.113
Nov 21, 2020 02:14:18.363516092 CET	49729	443	192.168.2.3	54.84.56.113
Nov 21, 2020 02:14:18.456724882 CET	443	49730	54.84.56.113	192.168.2.3
Nov 21, 2020 02:14:18.456774950 CET	443	49730	54.84.56.113	192.168.2.3
Nov 21, 2020 02:14:18.456876040 CET	49730	443	192.168.2.3	54.84.56.113
Nov 21, 2020 02:14:18.456927061 CET	49730	443	192.168.2.3	54.84.56.113
Nov 21, 2020 02:14:18.457638025 CET	49730	443	192.168.2.3	54.84.56.113
Nov 21, 2020 02:14:18.462097883 CET	443	49730	54.84.56.113	192.168.2.3
Nov 21, 2020 02:14:18.462183952 CET	443	49730	54.84.56.113	192.168.2.3
Nov 21, 2020 02:14:18.462379932 CET	49730	443	192.168.2.3	54.84.56.113
Nov 21, 2020 02:14:18.462588072 CET	443	49729	54.84.56.113	192.168.2.3
Nov 21, 2020 02:14:18.462704897 CET	443	49729	54.84.56.113	192.168.2.3
Nov 21, 2020 02:14:18.462759972 CET	49729	443	192.168.2.3	54.84.56.113
Nov 21, 2020 02:14:18.462805033 CET	49729	443	192.168.2.3	54.84.56.113
Nov 21, 2020 02:14:18.463216066 CET	49729	443	192.168.2.3	54.84.56.113
Nov 21, 2020 02:14:18.466161966 CET	443	49729	54.84.56.113	192.168.2.3
Nov 21, 2020 02:14:18.466389894 CET	49729	443	192.168.2.3	54.84.56.113

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 21, 2020 02:14:18.502927065 CET	443	49730	54.84.56.113	192.168.2.3
Nov 21, 2020 02:14:18.502993107 CET	443	49730	54.84.56.113	192.168.2.3
Nov 21, 2020 02:14:18.503031969 CET	443	49730	54.84.56.113	192.168.2.3
Nov 21, 2020 02:14:18.503079891 CET	443	49730	54.84.56.113	192.168.2.3
Nov 21, 2020 02:14:18.503098965 CET	49730	443	192.168.2.3	54.84.56.113
Nov 21, 2020 02:14:18.503123045 CET	443	49730	54.84.56.113	192.168.2.3
Nov 21, 2020 02:14:18.503133059 CET	49730	443	192.168.2.3	54.84.56.113
Nov 21, 2020 02:14:18.503138065 CET	49730	443	192.168.2.3	54.84.56.113
Nov 21, 2020 02:14:18.503143072 CET	49730	443	192.168.2.3	54.84.56.113
Nov 21, 2020 02:14:18.503161907 CET	443	49730	54.84.56.113	192.168.2.3
Nov 21, 2020 02:14:18.503175974 CET	49730	443	192.168.2.3	54.84.56.113
Nov 21, 2020 02:14:18.503204107 CET	443	49730	54.84.56.113	192.168.2.3
Nov 21, 2020 02:14:18.503231049 CET	49730	443	192.168.2.3	54.84.56.113
Nov 21, 2020 02:14:18.503276110 CET	49730	443	192.168.2.3	54.84.56.113
Nov 21, 2020 02:14:18.559777021 CET	443	49730	54.84.56.113	192.168.2.3
Nov 21, 2020 02:14:18.559842110 CET	443	49730	54.84.56.113	192.168.2.3
Nov 21, 2020 02:14:18.559885025 CET	443	49730	54.84.56.113	192.168.2.3
Nov 21, 2020 02:14:18.559925079 CET	443	49730	54.84.56.113	192.168.2.3
Nov 21, 2020 02:14:18.559927940 CET	49730	443	192.168.2.3	54.84.56.113
Nov 21, 2020 02:14:18.559977055 CET	49730	443	192.168.2.3	54.84.56.113
Nov 21, 2020 02:14:18.559983969 CET	49730	443	192.168.2.3	54.84.56.113
Nov 21, 2020 02:14:18.559990883 CET	49730	443	192.168.2.3	54.84.56.113
Nov 21, 2020 02:14:18.565128088 CET	443	49730	54.84.56.113	192.168.2.3
Nov 21, 2020 02:14:18.568528891 CET	49730	443	192.168.2.3	54.84.56.113
Nov 21, 2020 02:14:18.606184959 CET	443	49729	54.84.56.113	192.168.2.3
Nov 21, 2020 02:14:18.620362997 CET	49730	443	192.168.2.3	54.84.56.113
Nov 21, 2020 02:14:18.620764017 CET	49730	443	192.168.2.3	54.84.56.113
Nov 21, 2020 02:14:18.621016979 CET	49730	443	192.168.2.3	54.84.56.113
Nov 21, 2020 02:14:18.723537922 CET	443	49730	54.84.56.113	192.168.2.3
Nov 21, 2020 02:14:18.724215031 CET	443	49730	54.84.56.113	192.168.2.3
Nov 21, 2020 02:14:18.724252939 CET	443	49730	54.84.56.113	192.168.2.3
Nov 21, 2020 02:14:18.724281073 CET	443	49730	54.84.56.113	192.168.2.3
Nov 21, 2020 02:14:18.724437952 CET	443	49730	54.84.56.113	192.168.2.3
Nov 21, 2020 02:14:18.724447966 CET	49730	443	192.168.2.3	54.84.56.113
Nov 21, 2020 02:14:18.724494934 CET	49730	443	192.168.2.3	54.84.56.113
Nov 21, 2020 02:14:18.724519968 CET	443	49730	54.84.56.113	192.168.2.3
Nov 21, 2020 02:14:18.724582911 CET	49730	443	192.168.2.3	54.84.56.113
Nov 21, 2020 02:14:18.725512981 CET	443	49730	54.84.56.113	192.168.2.3
Nov 21, 2020 02:14:18.725553036 CET	443	49730	54.84.56.113	192.168.2.3
Nov 21, 2020 02:14:18.725583076 CET	49730	443	192.168.2.3	54.84.56.113
Nov 21, 2020 02:14:18.725591898 CET	443	49730	54.84.56.113	192.168.2.3
Nov 21, 2020 02:14:18.725606918 CET	49730	443	192.168.2.3	54.84.56.113
Nov 21, 2020 02:14:18.725632906 CET	443	49730	54.84.56.113	192.168.2.3
Nov 21, 2020 02:14:18.725646973 CET	49730	443	192.168.2.3	54.84.56.113
Nov 21, 2020 02:14:18.725671053 CET	443	49730	54.84.56.113	192.168.2.3
Nov 21, 2020 02:14:18.725688934 CET	49730	443	192.168.2.3	54.84.56.113
Nov 21, 2020 02:14:18.725712061 CET	443	49730	54.84.56.113	192.168.2.3
Nov 21, 2020 02:14:18.725737095 CET	49730	443	192.168.2.3	54.84.56.113
Nov 21, 2020 02:14:18.725750923 CET	443	49730	54.84.56.113	192.168.2.3
Nov 21, 2020 02:14:18.725768089 CET	49730	443	192.168.2.3	54.84.56.113
Nov 21, 2020 02:14:18.725799084 CET	443	49730	54.84.56.113	192.168.2.3
Nov 21, 2020 02:14:18.725805998 CET	49730	443	192.168.2.3	54.84.56.113
Nov 21, 2020 02:14:18.725841999 CET	443	49730	54.84.56.113	192.168.2.3
Nov 21, 2020 02:14:18.725857973 CET	49730	443	192.168.2.3	54.84.56.113
Nov 21, 2020 02:14:18.725883007 CET	443	49730	54.84.56.113	192.168.2.3
Nov 21, 2020 02:14:18.725923061 CET	443	49730	54.84.56.113	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 21, 2020 02:13:40.863727093 CET	63492	53	192.168.2.3	8.8.8.8
Nov 21, 2020 02:13:40.891136885 CET	53	63492	8.8.8.8	192.168.2.3
Nov 21, 2020 02:13:41.791352987 CET	60831	53	192.168.2.3	8.8.8.8
Nov 21, 2020 02:13:41.827271938 CET	53	60831	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 21, 2020 02:13:45.885591030 CET	60100	53	192.168.2.3	8.8.8.8
Nov 21, 2020 02:13:45.921506882 CET	53	60100	8.8.8.8	192.168.2.3
Nov 21, 2020 02:13:47.075037003 CET	53195	53	192.168.2.3	8.8.8.8
Nov 21, 2020 02:13:47.102164984 CET	53	53195	8.8.8.8	192.168.2.3
Nov 21, 2020 02:13:47.143141985 CET	50141	53	192.168.2.3	8.8.8.8
Nov 21, 2020 02:13:47.180702925 CET	53	50141	8.8.8.8	192.168.2.3
Nov 21, 2020 02:13:47.618674994 CET	53023	53	192.168.2.3	8.8.8.8
Nov 21, 2020 02:13:47.662453890 CET	53	53023	8.8.8.8	192.168.2.3
Nov 21, 2020 02:13:48.637340069 CET	53023	53	192.168.2.3	8.8.8.8
Nov 21, 2020 02:13:48.674746990 CET	53	53023	8.8.8.8	192.168.2.3
Nov 21, 2020 02:13:48.906933069 CET	49563	53	192.168.2.3	8.8.8.8
Nov 21, 2020 02:13:48.943015099 CET	53	49563	8.8.8.8	192.168.2.3
Nov 21, 2020 02:13:49.638348103 CET	53023	53	192.168.2.3	8.8.8.8
Nov 21, 2020 02:13:49.674359083 CET	53	53023	8.8.8.8	192.168.2.3
Nov 21, 2020 02:13:49.712146997 CET	51352	53	192.168.2.3	8.8.8.8
Nov 21, 2020 02:13:49.739533901 CET	53	51352	8.8.8.8	192.168.2.3
Nov 21, 2020 02:13:50.525584936 CET	59349	53	192.168.2.3	8.8.8.8
Nov 21, 2020 02:13:50.561530113 CET	53	59349	8.8.8.8	192.168.2.3
Nov 21, 2020 02:13:51.356724977 CET	57084	53	192.168.2.3	8.8.8.8
Nov 21, 2020 02:13:51.392381907 CET	53	57084	8.8.8.8	192.168.2.3
Nov 21, 2020 02:13:51.657723904 CET	53023	53	192.168.2.3	8.8.8.8
Nov 21, 2020 02:13:51.695800066 CET	53	53023	8.8.8.8	192.168.2.3
Nov 21, 2020 02:13:52.197968006 CET	58823	53	192.168.2.3	8.8.8.8
Nov 21, 2020 02:13:52.225301027 CET	53	58823	8.8.8.8	192.168.2.3
Nov 21, 2020 02:13:53.030800104 CET	57568	53	192.168.2.3	8.8.8.8
Nov 21, 2020 02:13:53.058087111 CET	53	57568	8.8.8.8	192.168.2.3
Nov 21, 2020 02:13:55.399708033 CET	50540	53	192.168.2.3	8.8.8.8
Nov 21, 2020 02:13:55.435461998 CET	53	50540	8.8.8.8	192.168.2.3
Nov 21, 2020 02:13:55.669420958 CET	53023	53	192.168.2.3	8.8.8.8
Nov 21, 2020 02:13:55.705116034 CET	53	53023	8.8.8.8	192.168.2.3
Nov 21, 2020 02:13:56.503451109 CET	54366	53	192.168.2.3	8.8.8.8
Nov 21, 2020 02:13:56.530641079 CET	53	54366	8.8.8.8	192.168.2.3
Nov 21, 2020 02:14:07.432063103 CET	53034	53	192.168.2.3	8.8.8.8
Nov 21, 2020 02:14:07.459306955 CET	53	53034	8.8.8.8	192.168.2.3
Nov 21, 2020 02:14:15.416830063 CET	57762	53	192.168.2.3	8.8.8.8
Nov 21, 2020 02:14:15.457030058 CET	53	57762	8.8.8.8	192.168.2.3
Nov 21, 2020 02:14:16.945832968 CET	55435	53	192.168.2.3	8.8.8.8
Nov 21, 2020 02:14:16.983011007 CET	53	55435	8.8.8.8	192.168.2.3
Nov 21, 2020 02:14:18.017821074 CET	50713	53	192.168.2.3	8.8.8.8
Nov 21, 2020 02:14:18.057737112 CET	53	50713	8.8.8.8	192.168.2.3
Nov 21, 2020 02:14:18.983889103 CET	56132	53	192.168.2.3	8.8.8.8
Nov 21, 2020 02:14:19.019846916 CET	53	56132	8.8.8.8	192.168.2.3
Nov 21, 2020 02:14:19.754179001 CET	58987	53	192.168.2.3	8.8.8.8
Nov 21, 2020 02:14:19.798026085 CET	53	58987	8.8.8.8	192.168.2.3
Nov 21, 2020 02:14:21.270925045 CET	56579	53	192.168.2.3	8.8.8.8
Nov 21, 2020 02:14:21.308199883 CET	53	56579	8.8.8.8	192.168.2.3
Nov 21, 2020 02:14:21.405998945 CET	60633	53	192.168.2.3	8.8.8.8
Nov 21, 2020 02:14:21.433263063 CET	53	60633	8.8.8.8	192.168.2.3
Nov 21, 2020 02:14:25.727269888 CET	61292	53	192.168.2.3	8.8.8.8
Nov 21, 2020 02:14:25.754611969 CET	53	61292	8.8.8.8	192.168.2.3
Nov 21, 2020 02:14:41.500925064 CET	63619	53	192.168.2.3	8.8.8.8
Nov 21, 2020 02:14:41.528223991 CET	53	63619	8.8.8.8	192.168.2.3
Nov 21, 2020 02:14:46.069849968 CET	64938	53	192.168.2.3	8.8.8.8
Nov 21, 2020 02:14:46.106991053 CET	53	64938	8.8.8.8	192.168.2.3
Nov 21, 2020 02:14:46.922219038 CET	61946	53	192.168.2.3	8.8.8.8
Nov 21, 2020 02:14:46.958028078 CET	53	61946	8.8.8.8	192.168.2.3
Nov 21, 2020 02:14:47.643959999 CET	64910	53	192.168.2.3	8.8.8.8
Nov 21, 2020 02:14:47.679975033 CET	53	64910	8.8.8.8	192.168.2.3
Nov 21, 2020 02:14:47.921466112 CET	61946	53	192.168.2.3	8.8.8.8
Nov 21, 2020 02:14:47.948889017 CET	53	61946	8.8.8.8	192.168.2.3
Nov 21, 2020 02:14:48.653568983 CET	64910	53	192.168.2.3	8.8.8.8
Nov 21, 2020 02:14:48.680869102 CET	53	64910	8.8.8.8	192.168.2.3
Nov 21, 2020 02:14:48.934495926 CET	61946	53	192.168.2.3	8.8.8.8
Nov 21, 2020 02:14:48.972407103 CET	53	61946	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 21, 2020 02:14:49.671011925 CET	64910	53	192.168.2.3	8.8.8.8
Nov 21, 2020 02:14:49.698406935 CET	53	64910	8.8.8.8	192.168.2.3
Nov 21, 2020 02:14:50.950193882 CET	61946	53	192.168.2.3	8.8.8.8
Nov 21, 2020 02:14:50.986027002 CET	53	61946	8.8.8.8	192.168.2.3
Nov 21, 2020 02:14:51.684539080 CET	64910	53	192.168.2.3	8.8.8.8
Nov 21, 2020 02:14:51.720325947 CET	53	64910	8.8.8.8	192.168.2.3
Nov 21, 2020 02:14:54.954463005 CET	61946	53	192.168.2.3	8.8.8.8
Nov 21, 2020 02:14:54.990370989 CET	53	61946	8.8.8.8	192.168.2.3
Nov 21, 2020 02:14:55.686819077 CET	64910	53	192.168.2.3	8.8.8.8
Nov 21, 2020 02:14:55.714175940 CET	53	64910	8.8.8.8	192.168.2.3
Nov 21, 2020 02:15:16.030801058 CET	52123	53	192.168.2.3	8.8.8.8
Nov 21, 2020 02:15:16.058160067 CET	53	52123	8.8.8.8	192.168.2.3
Nov 21, 2020 02:15:17.661761045 CET	56130	53	192.168.2.3	8.8.8.8
Nov 21, 2020 02:15:17.689182043 CET	53	56130	8.8.8.8	192.168.2.3
Nov 21, 2020 02:15:29.033541918 CET	56338	53	192.168.2.3	8.8.8.8
Nov 21, 2020 02:15:29.069438934 CET	53	56338	8.8.8.8	192.168.2.3
Nov 21, 2020 02:15:31.442131996 CET	59420	53	192.168.2.3	8.8.8.8
Nov 21, 2020 02:15:31.443289042 CET	58784	53	192.168.2.3	8.8.8.8
Nov 21, 2020 02:15:31.486918926 CET	53	58784	8.8.8.8	192.168.2.3
Nov 21, 2020 02:15:31.487720966 CET	53	59420	8.8.8.8	192.168.2.3
Nov 21, 2020 02:15:31.597182989 CET	63978	53	192.168.2.3	8.8.8.8
Nov 21, 2020 02:15:31.641057014 CET	53	63978	8.8.8.8	192.168.2.3
Nov 21, 2020 02:15:31.807648897 CET	62938	53	192.168.2.3	8.8.8.8
Nov 21, 2020 02:15:31.852011919 CET	53	62938	8.8.8.8	192.168.2.3
Nov 21, 2020 02:15:35.877655983 CET	55708	53	192.168.2.3	8.8.8.8
Nov 21, 2020 02:15:35.929924965 CET	53	55708	8.8.8.8	192.168.2.3
Nov 21, 2020 02:15:36.400579929 CET	56803	53	192.168.2.3	8.8.8.8
Nov 21, 2020 02:15:36.405499935 CET	57145	53	192.168.2.3	8.8.8.8
Nov 21, 2020 02:15:36.408896923 CET	55359	53	192.168.2.3	8.8.8.8
Nov 21, 2020 02:15:36.432404041 CET	53	57145	8.8.8.8	192.168.2.3
Nov 21, 2020 02:15:36.435828924 CET	53	55359	8.8.8.8	192.168.2.3
Nov 21, 2020 02:15:36.443717003 CET	53	56803	8.8.8.8	192.168.2.3
Nov 21, 2020 02:15:36.455532074 CET	58306	53	192.168.2.3	8.8.8.8
Nov 21, 2020 02:15:36.458267927 CET	64124	53	192.168.2.3	8.8.8.8
Nov 21, 2020 02:15:36.482462883 CET	53	58306	8.8.8.8	192.168.2.3
Nov 21, 2020 02:15:36.487581968 CET	49361	53	192.168.2.3	8.8.8.8
Nov 21, 2020 02:15:36.493678093 CET	53	64124	8.8.8.8	192.168.2.3
Nov 21, 2020 02:15:36.514436960 CET	53	49361	8.8.8.8	192.168.2.3
Nov 21, 2020 02:15:36.792023897 CET	63150	53	192.168.2.3	8.8.8.8
Nov 21, 2020 02:15:36.827775955 CET	53	63150	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 21, 2020 02:14:18.017821074 CET	192.168.2.3	8.8.8.8	0x9d7c	Standard query (0)	workflowy.com	A (IP address)	IN (0x0001)
Nov 21, 2020 02:14:19.754179001 CET	192.168.2.3	8.8.8.8	0x85cb	Standard query (0)	stats.g.doubleclick.net	A (IP address)	IN (0x0001)
Nov 21, 2020 02:14:21.270925045 CET	192.168.2.3	8.8.8.8	0xb38	Standard query (0)	js-agent.newrelic.com	A (IP address)	IN (0x0001)
Nov 21, 2020 02:14:21.405998945 CET	192.168.2.3	8.8.8.8	0xc4f	Standard query (0)	bam-cell.nr-data.net	A (IP address)	IN (0x0001)
Nov 21, 2020 02:15:29.033541918 CET	192.168.2.3	8.8.8.8	0x8c75	Standard query (0)	workflowy.com	A (IP address)	IN (0x0001)
Nov 21, 2020 02:15:35.877655983 CET	192.168.2.3	8.8.8.8	0x6ce9	Standard query (0)	jamif-cdn3d.us-east-1.linodeobjects.com	A (IP address)	IN (0x0001)
Nov 21, 2020 02:15:36.405499935 CET	192.168.2.3	8.8.8.8	0x3c7a	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)
Nov 21, 2020 02:15:36.408896923 CET	192.168.2.3	8.8.8.8	0xce65	Standard query (0)	maxcdn.bootstrapcdn.com	A (IP address)	IN (0x0001)
Nov 21, 2020 02:15:36.455532074 CET	192.168.2.3	8.8.8.8	0xb29f	Standard query (0)	kit.fontawesome.com	A (IP address)	IN (0x0001)
Nov 21, 2020 02:15:36.458267927 CET	192.168.2.3	8.8.8.8	0x8d8e	Standard query (0)	s3.amazonaws.com	A (IP address)	IN (0x0001)
Nov 21, 2020 02:15:36.487581968 CET	192.168.2.3	8.8.8.8	0x8cb1	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 21, 2020 02:15:36.792023897 CET	192.168.2.3	8.8.8.8	0x361d	Standard query (0)	ka-f.fontawesome.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 21, 2020 02:14:18.057737112 CET	8.8.8.8	192.168.2.3	0x9d7c	No error (0)	workflowy.com		54.84.56.113	A (IP address)	IN (0x0001)
Nov 21, 2020 02:14:18.057737112 CET	8.8.8.8	192.168.2.3	0x9d7c	No error (0)	workflowy.com		107.23.99.91	A (IP address)	IN (0x0001)
Nov 21, 2020 02:14:18.057737112 CET	8.8.8.8	192.168.2.3	0x9d7c	No error (0)	workflowy.com		54.164.228.73	A (IP address)	IN (0x0001)
Nov 21, 2020 02:14:19.798026085 CET	8.8.8.8	192.168.2.3	0x85cb	No error (0)	stats.g.doubleclick.net	stats.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 02:14:19.798026085 CET	8.8.8.8	192.168.2.3	0x85cb	No error (0)	stats.l.doubleclick.net		74.125.140.157	A (IP address)	IN (0x0001)
Nov 21, 2020 02:14:19.798026085 CET	8.8.8.8	192.168.2.3	0x85cb	No error (0)	stats.l.doubleclick.net		74.125.140.156	A (IP address)	IN (0x0001)
Nov 21, 2020 02:14:19.798026085 CET	8.8.8.8	192.168.2.3	0x85cb	No error (0)	stats.l.doubleclick.net		74.125.140.154	A (IP address)	IN (0x0001)
Nov 21, 2020 02:14:19.798026085 CET	8.8.8.8	192.168.2.3	0x85cb	No error (0)	stats.l.doubleclick.net		74.125.140.155	A (IP address)	IN (0x0001)
Nov 21, 2020 02:14:21.308199883 CET	8.8.8.8	192.168.2.3	0xb38	No error (0)	js-agent.newrelic.com	f4.shared.global.fastly.net		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 02:14:21.433263063 CET	8.8.8.8	192.168.2.3	0xc4f	No error (0)	bam-cell.nr-data.net	tls12.newrelic.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 02:15:29.069438934 CET	8.8.8.8	192.168.2.3	0x8c75	No error (0)	workflowy.com		107.23.99.91	A (IP address)	IN (0x0001)
Nov 21, 2020 02:15:29.069438934 CET	8.8.8.8	192.168.2.3	0x8c75	No error (0)	workflowy.com		54.164.228.73	A (IP address)	IN (0x0001)
Nov 21, 2020 02:15:29.069438934 CET	8.8.8.8	192.168.2.3	0x8c75	No error (0)	workflowy.com		54.84.56.113	A (IP address)	IN (0x0001)
Nov 21, 2020 02:15:35.929924965 CET	8.8.8.8	192.168.2.3	0x6ce9	No error (0)	jamif-cdn3d.us-east-1.linodeobjects.com	us-east-1.linodeobjects.com		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 02:15:35.929924965 CET	8.8.8.8	192.168.2.3	0x6ce9	No error (0)	us-east-1.linodeobjects.com		97.107.137.245	A (IP address)	IN (0x0001)
Nov 21, 2020 02:15:35.929924965 CET	8.8.8.8	192.168.2.3	0x6ce9	No error (0)	us-east-1.linodeobjects.com		45.56.104.115	A (IP address)	IN (0x0001)
Nov 21, 2020 02:15:35.929924965 CET	8.8.8.8	192.168.2.3	0x6ce9	No error (0)	us-east-1.linodeobjects.com		45.79.157.59	A (IP address)	IN (0x0001)
Nov 21, 2020 02:15:35.929924965 CET	8.8.8.8	192.168.2.3	0x6ce9	No error (0)	us-east-1.linodeobjects.com		173.255.231.96	A (IP address)	IN (0x0001)
Nov 21, 2020 02:15:35.929924965 CET	8.8.8.8	192.168.2.3	0x6ce9	No error (0)	us-east-1.linodeobjects.com		96.126.106.143	A (IP address)	IN (0x0001)
Nov 21, 2020 02:15:35.929924965 CET	8.8.8.8	192.168.2.3	0x6ce9	No error (0)	us-east-1.linodeobjects.com		45.79.137.127	A (IP address)	IN (0x0001)
Nov 21, 2020 02:15:36.432404041 CET	8.8.8.8	192.168.2.3	0x3c7a	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 02:15:36.435828924 CET	8.8.8.8	192.168.2.3	0xce65	No error (0)	maxcdn.bootstrapcdn.com	cds.j3z9t3p6.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 02:15:36.482462883 CET	8.8.8.8	192.168.2.3	0xb29f	No error (0)	kit.fontawesome.com	kit.fontawesome.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 02:15:36.493678093 CET	8.8.8.8	192.168.2.3	0x8d8e	No error (0)	s3.amazonaws.com		52.217.4.102	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 21, 2020 02:15:36.514436960 CET	8.8.8.8	192.168.2.3	0x8cb1	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Nov 21, 2020 02:15:36.514436960 CET	8.8.8.8	192.168.2.3	0x8cb1	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Nov 21, 2020 02:15:36.827775955 CET	8.8.8.8	192.168.2.3	0x361d	No error (0)	ka-f.fontawesome.com	ka-f.fontawesome.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Nov 21, 2020 02:14:18.301261902 CET	54.84.56.113	443	192.168.2.3	49729	CN=*.workflowy.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	Sun Oct 25 02:00:00 CEST 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 Nov 25 00:59:59 CET 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Nov 21, 2020 02:14:18.301450014 CET	54.84.56.113	443	192.168.2.3	49730	CN=*.workflowy.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	Sun Oct 25 02:00:00 CEST 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 Nov 25 00:59:59 CET 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		

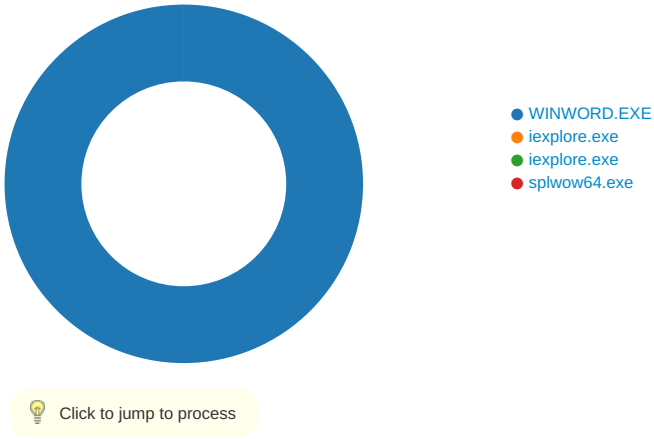
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Nov 21, 2020 02:14:19.857593060 CET	74.125.140.157	443	192.168.2.3	49733	CN=*.g.doubleclick.net, 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 08:33:42 CET 2020 Thu Jun 15 02:00:42 CEST 2017	Tue Jan 26 08:33:42 CET 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Nov 21, 2020 02:14:19.858072042 CET	74.125.140.157	443	192.168.2.3	49734	CN=*.g.doubleclick.net, 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 08:33:42 CET 2020 Thu Jun 15 02:00:42 CEST 2017	Tue Jan 26 08:33:42 CET 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Nov 21, 2020 02:15:36.256736040 CET	97.107.137.245	443	192.168.2.3	49765	CN=linodeobjects.com 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.	Mon Sep 28 14:53:21 CEST 2020 Thu Mar 17 17:40:46 CET 2016	Sun Dec 27 13:53:21 CET 2020 Wed Mar 17 17:40:46 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 17 17:40:46 CET 2016	Wed Mar 17 17:40:46 CET 2021		
Nov 21, 2020 02:15:36.264358997 CET	97.107.137.245	443	192.168.2.3	49766	CN=linodeobjects.com 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.	Mon Sep 28 14:53:21 CEST 2020 Thu Mar 17 17:40:46 CET 2016	Sun Dec 27 13:53:21 CET 2020 Wed Mar 17 17:40:46 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 17 17:40:46 CET 2016	Wed Mar 17 17:40:46 CET 2021		
Nov 21, 2020 02:15:36.564673901 CET	104.16.19.94	443	192.168.2.3	49779	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Oct 21 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Thu Oct 21 01:59:59 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Nov 21, 2020 02:15:36.564790964 CET	104.16.19.94	443	192.168.2.3	49778	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Oct 21 02:00:00 CEST 2020	Thu Oct 21 01:59:59 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Nov 21, 2020 02:15:36.722412109 CET	52.217.4.102	443	192.168.2.3	49777	CN=s3.amazonaws.com, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Aug 04 02:00:00 CEST 2020	Mon Aug 09 14:00:00 CEST 2021	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	3faf2df7ab96c36419c31725cb1fa7d6
					CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Dec 08 13:05:07 CET 2015	Sat May 10 14:00:00 CEST 2025		
Nov 21, 2020 02:15:36.722641945 CET	52.217.4.102	443	192.168.2.3	49776	CN=s3.amazonaws.com, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Aug 04 02:00:00 CEST 2020	Mon Aug 09 14:00:00 CEST 2021	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	3faf2df7ab96c36419c31725cb1fa7d6
					CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Dec 08 13:05:07 CET 2015	Sat May 10 14:00:00 CEST 2025		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: WINWORD.EXE PID: 488 Parent PID: 792

General

Start time:	02:13:45
Start date:	21/11/2020
Path:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE' /Automation -Embedding
Imagebase:	0x970000
File size:	1937688 bytes
MD5 hash:	0B9AB9B9C4DE429473D6450D4297A123
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\VBE	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	66B8977C	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\2D18C2DB.png	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | delete on close | open no recall	success or wait	1	66AB5805	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\2F482720.png	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | delete on close | open no recall	success or wait	1	66AB5805	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\F860BCA1.png	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | delete on close | open no recall	success or wait	1	66AB5805	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\93CABA2E.png	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | delete on close | open no recall	success or wait	1	66AB5805	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\75F7C857.png	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | delete on close | open no recall	success or wait	1	66AB5805	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$nnec Pharma .docx	success or wait	1	66AB5805	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\2D18C2DB.png	0	2528	89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 60 00 00 00 60 08 06 00 00 00 e2 98 77 38 00 00 09 a7 49 44 41 54 78 5e ed 9d 7f 8c 1c 65 19 c7 3f cf ee 9e 77 17 91 50 84 6a f8 59 2d d7 dd 2d 2a a0 54 51 23 09 e2 1f 28 89 89 9a 52 24 44 30 51 0a 2d 2d 14 50 77 b7 77 b0 70 d7 9d 6d 29 b4 fc 94 1f 26 d2 08 69 44 42 34 a0 4d 48 a0 98 f0 07 fa 07 20 0a 3b db 2b 42 31 62 50 81 06 45 38 ee 76 1e 33 db de 41 6f 67 67 66 f7 e6 c7 1e 9d 49 2e 97 76 9e f7 79 df f9 7e de e7 9d 77 de 5f 27 24 57 ac 0a 48 ac b9 27 99 93 00 88 b9 12 24 00 12 00 31 29 50 30 47 30 b2 63 88 68 4c 25 68 66 7b f0 46 40 a1 b6 07 e4 11 8c ec 45 71 42 38 c8 01 70 1c c2 dd 54 72 2b e3 82 90 00 d8 d7 0e c4 06 21 01 f0 de 0b e0 2e 8c dc c5 51 47 42 02 e0 fd 6f 60 91 3b a9 64 2f 89 12 42	.PNG........IHDR...`...`..... .w8....IDATx^.....e..?...w..P. j.Y-..-*.TQ#...(...R$D0Q.-- .Pw .w.p..m)....&..iDB4.MH..... . ;.+B1bP..E8.v.3..Aoggf.....I ..v..y..~...w._'$W..H..'.....$. ..1)P0G0.c.hL%hf{.F@..... .EqB 8..p...Tr+.....!.....Q GB...o`.;.d/..B	success or wait	1	66AB5805	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\2F482720.png	0	2058	89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 30 00 00 00 30 08 06 00 00 00 57 02 f9 87 00 00 07 d1 49 44 41 54 68 43 cd 5a 4d 4c 54 57 14 3e 8f 66 48 65 14 07 77 45 30 5a bb d0 40 53 4d ab 06 12 53 4d 04 59 55 8d 06 5c 32 44 13 c5 45 51 5c 69 e4 af b1 2b 81 e9 42 68 84 80 dd 15 a2 51 ba 11 74 21 d5 04 02 36 91 05 24 2e 6a 6b c0 b2 94 01 1d 24 e2 cc 6d be cb 9c d7 3b 6f de 7d f7 0d 62 d2 93 10 60 de 7d f7 9e ef fc 9f 73 c7 a2 35 a0 50 5d 28 b4 fc 6e f9 28 59 f4 95 10 62 ab 45 d6 2e 22 0a 25 7f f8 84 17 64 d1 0b 22 9a a0 04 4d c4 45 fc f7 a5 9f 97 f0 ff 07 91 b5 da b7 c1 f4 fb 77 ef eb 84 25 be 25 41 07 56 b5 8f 25 c1 44 3e 04 4c c6 00 6c c6 49 7c cf 12 ce 5d 97 4b a5 db 4b a9 64 7b 09 15 e6 15 52 f1 e6 62 c2 67 b9 9f e6 4a 5c 0b 4b 0b 34 f3 6a	.PNG........IHDR...0...0..... W ....IDAThC.ZMLTW.>.fHe ..wE0 Z..@SM...SM.YU..\2D..EQ \i...+. .Bh.....Q..t!...6..$.jk.....$. .m....;o.}..b...`.}.....s..5.P] (..n.(Y...b.E..".%....d.."... M.E.............w...%.%A.V.. %.D>.L..l.l|...].K..K.d{....R. .b.g...J\.K.4.j	success or wait	1	66AB5805	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\F860BCA1.png	0	1604	89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 60 00 00 00 60 08 06 00 00 00 e2 98 77 38 00 00 06 0b 49 44 41 54 78 5e ed 9d 5d 6c 14 55 14 c7 cf a0 d9 34 c5 d2 35 21 a9 3e 28 c4 a2 86 a8 84 87 d6 8f 12 0d 55 79 50 a2 29 0f d6 44 b6 50 13 b3 98 50 ab f8 1d a1 c6 d8 d8 f8 09 0d 29 1a 56 89 5b ba 34 50 13 4b 34 85 07 50 23 84 22 d8 07 5b 4c fc 02 b4 f6 c1 d4 b4 a9 0b d2 34 2b 58 73 36 bb eb 74 f6 ce ec bd 33 e7 ce 6c cb 99 a7 7e 9c 7b ee 9d ff ef 9e 73 bf 76 67 0c e0 2b 50 05 8c 40 6b e7 ca 81 01 04 dc 09 18 00 03 08 58 81 80 ab e7 08 98 eb 00 a2 d1 68 69 6a 6a f2 99 69 80 a5 01 df ab 54 f5 86 61 8c 5d f1 cf a5 f6 5d dd dd c3 52 05 3c 1a 69 8f 80 c6 75 91 57 66 8b f8 59 2d e7 4d c3 e4 bc 4b ff b6 f9 01 41 3b 80 f5 eb 22 5d a1 50 28 14 8d 3e 59 57	.PNG.....IHDR...`...`..... .w8....IDATx^..]l.U.....4..5!. >(.....UyP.)..D.P...P.... .....).V.[.4P.K4..P#."..[L... .....4+Xs6..t....3..l...~.{. ....s.vg..+P..@k.....X.. .....hijj..i.....T..a.]....]...R. <.i...u.Wf..Y-.M...K.... A;...'].P(..>YW	success or wait	1	66AB5805	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\93CABA2E.png	0	5572	89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 ac 00 00 00 28 08 06 00 00 00 63 10 11 16 00 00 15 8b 49 44 41 54 78 5e ed 5c 0d 74 54 d5 b5 de fb 9c 73 67 26 09 33 09 81 00 d6 6a e4 a7 f6 bd a7 fd 79 16 41 5f 5f ad f5 07 c5 3f b0 35 e8 b3 c5 52 a5 28 68 20 29 7f 22 a2 e3 b2 82 99 b9 77 12 49 b5 4a ad b5 6a a9 95 5a 69 ad d6 da 16 6c 6b 6b 7d f5 3d b5 8a fd 51 a8 e0 d2 87 fc 25 64 f2 37 f7 de 73 f6 5b 7b b8 97 35 c4 84 24 d3 ae e5 22 e6 ae 95 c5 9a 99 73 ce bd 67 9f ef ee b3 f7 b7 bf 03 c2 f0 35 6c 81 23 c8 02 c8 cf 4a 35 35 72 37 6c 29 89 02 44 8a 7d f6 84 25 09 24 ba b7 4c fc 53 57 d9 a9 50 d2 11 87 28 b4 15 37 5a b4 0c 28 d7 0a b9 e4 85 d0 59 dc 08 c3 bd 86 aa 05 f2 80 cd d6 4c aa 42 9f a6 0b a2 a9 1e 01 0d 76 b2 42 00 58 08 5e ce 17 2f 34 7e	.PNG.....IHDR.....(.....c .....IDATx^.\.tT.....sg&.3.. ..j.....y.A__....?.5...R.(h) ."......w.I.J..j..Zi....Ikk}.= ...Q.....%d.7..s.[{..5..$...". .....s..g.....5l.#....J55 r7l)..D.}..%.$..L.SW..P... (..7Z..(.....Y.....L.B..... ...v.B.X.^../4~	success or wait	1	66AB5805	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\75F7C857.png	0	11108	89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 01 fe 00 00 01 18 08 06 00 00 00 bd 72 94 ba 00 00 00 19 74 45 58 74 53 6f 66 74 77 61 72 65 00 41 64 6f 62 65 20 49 6d 61 67 65 52 65 61 64 79 71 c9 65 3c 00 00 03 28 69 54 58 74 58 4d 4c 3a 63 6f 6d 2e 61 64 6f 62 65 2e 78 6d 70 00 00 00 00 00 3c 3f 78 70 61 63 6b 65 74 20 62 65 67 69 6e 3d 22 ef bb bf 22 20 69 64 3d 22 57 35 4d 30 4d 70 43 65 68 69 48 7a 72 65 53 7a 4e 54 63 7a 6b 63 39 64 22 3f 3e 20 3c 78 3a 78 6d 70 6d 65 74 61 20 78 6d 6c 6e 73 3a 78 3d 22 61 64 6f 62 65 3a 6e 73 3a 6d 65 74 61 2f 22 20 78 3a 78 6d 70 74 6b 3d 22 41 64 6f 62 65 20 58 4d 50 20 43 6f 72 65 20 35 2e 36 2d 63 31 33 38 20 37 39 2e 31 35 39 38 32 34 2c 20 32 30 31 36 2f 30 39 2f 31 34 2d 30 31 3a 30 39 3a 30 31 20 20	.PNG.....IHDR.....r.....tEXtSoftware.Adobe ImageReadyq.e<...(iTXtXML:com.adobe.xmp.....<?xpacket begin="..." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c138 79.159824, 2016/09/14-01:09:01	success or wait	1	66AB5805	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\Fennec Pharma .docx	14683	2528	success or wait	5	66AB5805	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	66AC8A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1	success or wait	1	66AC8A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common	success or wait	1	66AC8A84	RegCreateKeyExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	success or wait	1	66AB5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery	success or wait	1	66AB5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery\20381	success or wait	1	66AB5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations	success or wait	1	66AB5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	success or wait	1	66AB5805	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Name	unicode	Recover Text from Any File	success or wait	1	66AB5805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Path	unicode	C:\Program Files (x86)\Common Files\Microsoft Shared\TextConv\RECOVR32.CNV	success or wait	1	66AB5805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Extensions	unicode	*	success or wait	1	66AB5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Cambria Math	binary	02 04 05 03 05 04 06 03 02 04	success or wait	1	66AB5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Segoe UI	binary	02 0B 05 02 04 02 04 02 02 03	success or wait	1	66AB5805	unknown
HKEY_CURRENT_USER\Software\Mic	20381	binary		success or wait	1	66AB5805	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
rosoft\Office\16.0\Word\Resiliency\DocumentRecovery\20381			04 00 00 00 E8 01 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 68 00 61 00 72 00 64 00 7A 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 08 00 00 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 00 00 00 00 01 00 00 00 00 00 00 00 9C 92 04 16 EF BF D6 01 81 03 02 00 81 03 02 00 00 00 00 00 DB 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00				

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00				
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	File Path	unicode	C:\Users\user\AppData\Local\Temp\imgs.htm	success or wait	1	66AB5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	Datetime	unicode	2020-11-21T02:14	success or wait	1	66AB5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	Position	unicode	1395772239 0	success or wait	1	66AB5805	unknown

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109110000000000000000F01FEC\Usage	ProductFiles	dword	1366622224	1366622225	success or wait	1	66AB5805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109110000000000000000F01FEC\Usage	ProductFiles	dword	1366622225	1366622226	success or wait	1	66AB5805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Name	unicode	Recover Text from Any File	WordPerfect 5.x	success or wait	1	66AB5805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Path	unicode	C:\Program Files (x86)\Common Files\Microsoft Shared\TextConv\RECOVR32.CNV	C:\Program Files (x86)\Common Files\Microsoft Shared\TextConv\WPFT532.CNV	success or wait	1	66AB5805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Extensions	unicode	*	doc	success or wait	1	66AB5805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Name	unicode	WordPerfect 5.x	WordPerfect 6.x - 7.0	success or wait	1	66AB5805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Path	unicode	C:\Program Files (x86)\Common Files\Microsoft Shared\TextConv\WPFT532.CNV	C:\Program Files (x86)\Common Files\Microsoft Shared\TextConv\WPFT632.CNV	success or wait	1	66AB5805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Extensions	unicode	doc	wpd doc	success or wait	1	66AB5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery\20381	20381	binary	04 00 00 00 E8 01 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 68 00 61 00 72 00 64 00 7A 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 08 00 00 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 00 00 00 00 01 00 00 00 00 00 00 00 9C 92 04 16 EF BF D6 01 81 03 02 00 81 03 02 00 00 00 00 00 DB 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	04 00 00 00 E8 01 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 68 00 61 00 72 00 64 00 7A 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 08 00 00 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 81 03 02 00 81 03 02 00 00 00 00 00 DB 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 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	66AB5805	unknown

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00				

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00				

Analysis Process: iexplore.exe PID: 6300 Parent PID: 792

General

Start time:	02:14:16
Start date:	21/11/2020
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff6c2e20000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: iexplore.exe PID: 6344 Parent PID: 6300

General

Start time:	02:14:16
Start date:	21/11/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6300 CREDAT:17410 /prefetch:2
Imagebase:	0xb20000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	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: splwow64.exe PID: 6640 Parent PID: 488

General

Start time:	02:14:20
Start date:	21/11/2020
Path:	C:\Windows\splwow64.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\splwow64.exe 12288
Imagebase:	0x7ff718e80000
File size:	130560 bytes
MD5 hash:	8D59B31FF375059E3C32B17BF31A76D5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly