ID: 321374
Sample Name: Fennec Pharma
.docx
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 02:05:59
Date: 21/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

Table of Contents 2
Analysis Report Fennec Pharma .docx 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Yara Overview 4
Sigma Overview 4
Signature Overview 4
AV Detection: 5
Mitre Att&ck Matrix 5
Behavior Graph 5
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 7
URLs 7
Domains and IPs 8
Contacted Domains 8
Contacted URLs 8
URLs from Memory and Binaries 8
Contacted IPs 9
Public 9
General Information 9
Simulations 10
Behavior and APIs 10
Joe Sandbox View / Context 10
IPs 11
Domains 11
ASN 12
JA3 Fingerprints 13
Dropped Files 13
Created / dropped Files 14
Static File Info 35
General 35
File Icon 35
Network Behavior 35
Network Port Distribution 35
TCP Packets 36
UDP Packets 37
DNS Queries 38
DNS Answers 38
HTTPS Packets 39
Code Manipulations 40
Statistics 41
Behavior 41
System Behavior 41
Analysis Process: WINWORD.EXE PID: 2004 Parent PID: 584 41
General 41

File Activities 41
File Created 41
File Deleted 41
File Read 42
Registry Activities 42
Key Created 42
Key Value Created 42
Key Value Modified 44
Analysis Process: iexplore.exe PID: 2568 Parent PID: 584 46
General 46
File Activities 46
Registry Activities 46
Analysis Process: iexplore.exe PID: 2560 Parent PID: 2568 46
General 46
File Activities 47
Registry Activities 47
Disassembly 47

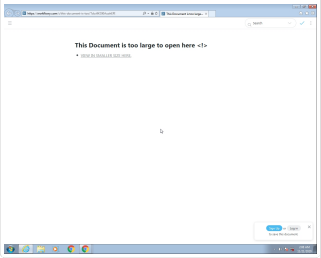
Analysis Report Fennec Pharma .docx

Overview

General Information

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

Most interesting Screenshot:



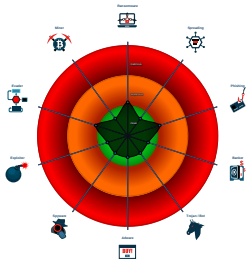
Detection

Score:	48
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- IP address seen in connection with o…
- JA3 SSL client fingerprint seen in co…

Classification



Startup

- **System is w7x64**
- WINWORD.EXE (PID: 2004 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
- iexplore.exe (PID: 2568 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 4EB098135821348270F27157F7A84E65)
  - iexplore.exe (PID: 2560 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2568 CREDAT:275457 /prefetch:2 MD5: 8A590F790A98F3D77399BE457E01386A)
- **cleanup**

Malware Configuration

No configs have been found

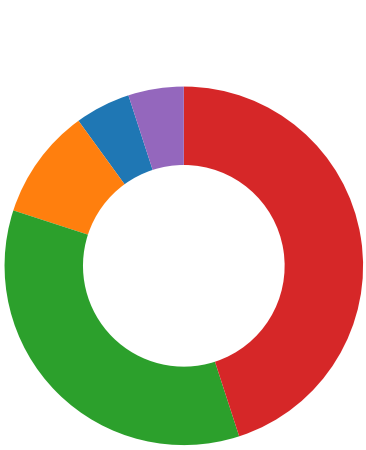
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

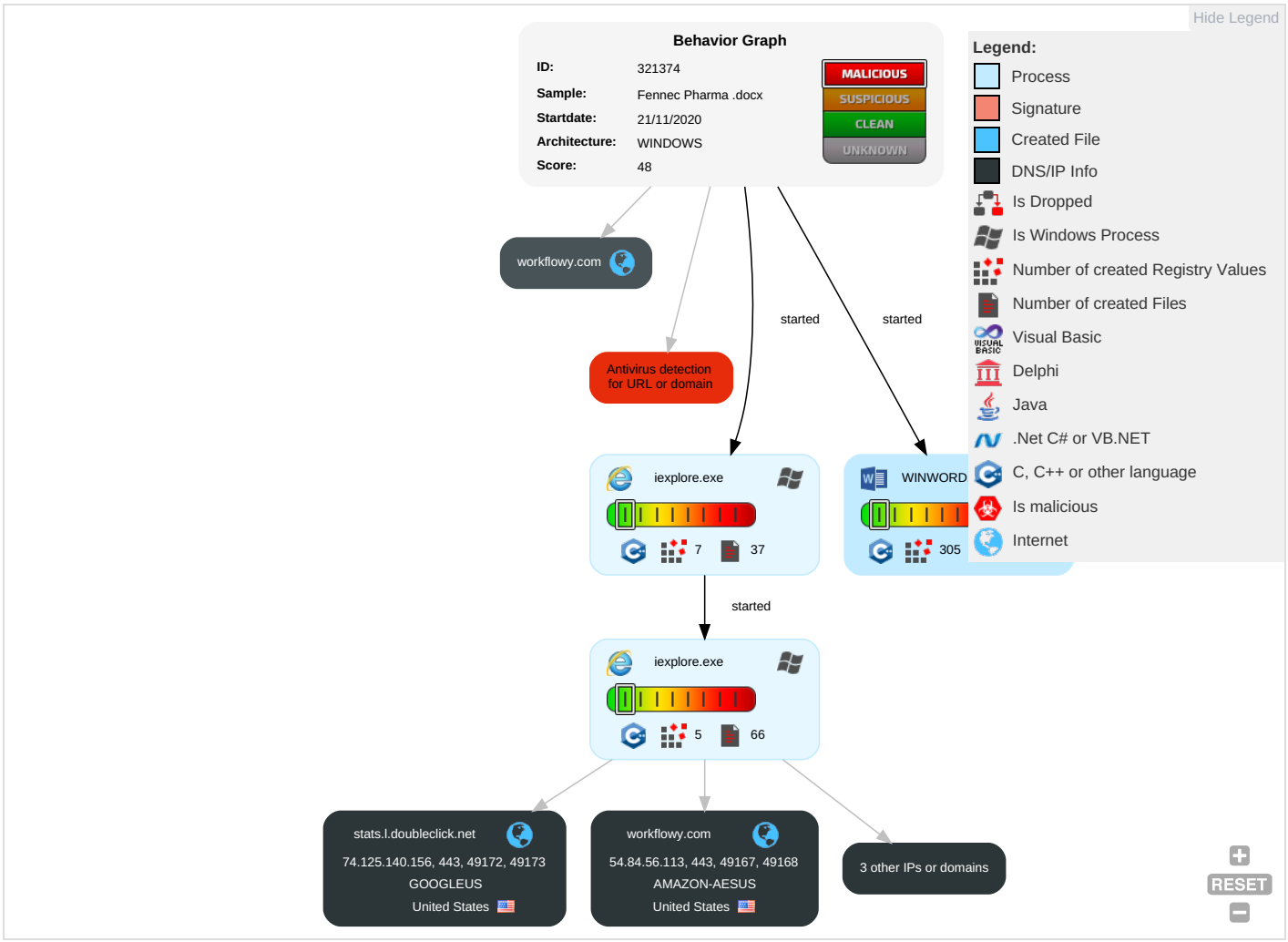
AV Detection:

Antivirus detection for URL or domain

Mitre Att&ck Matrix

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

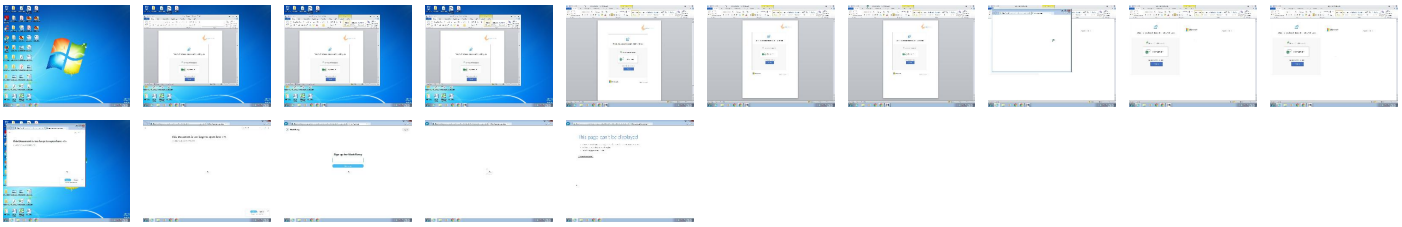
Behavior Graph

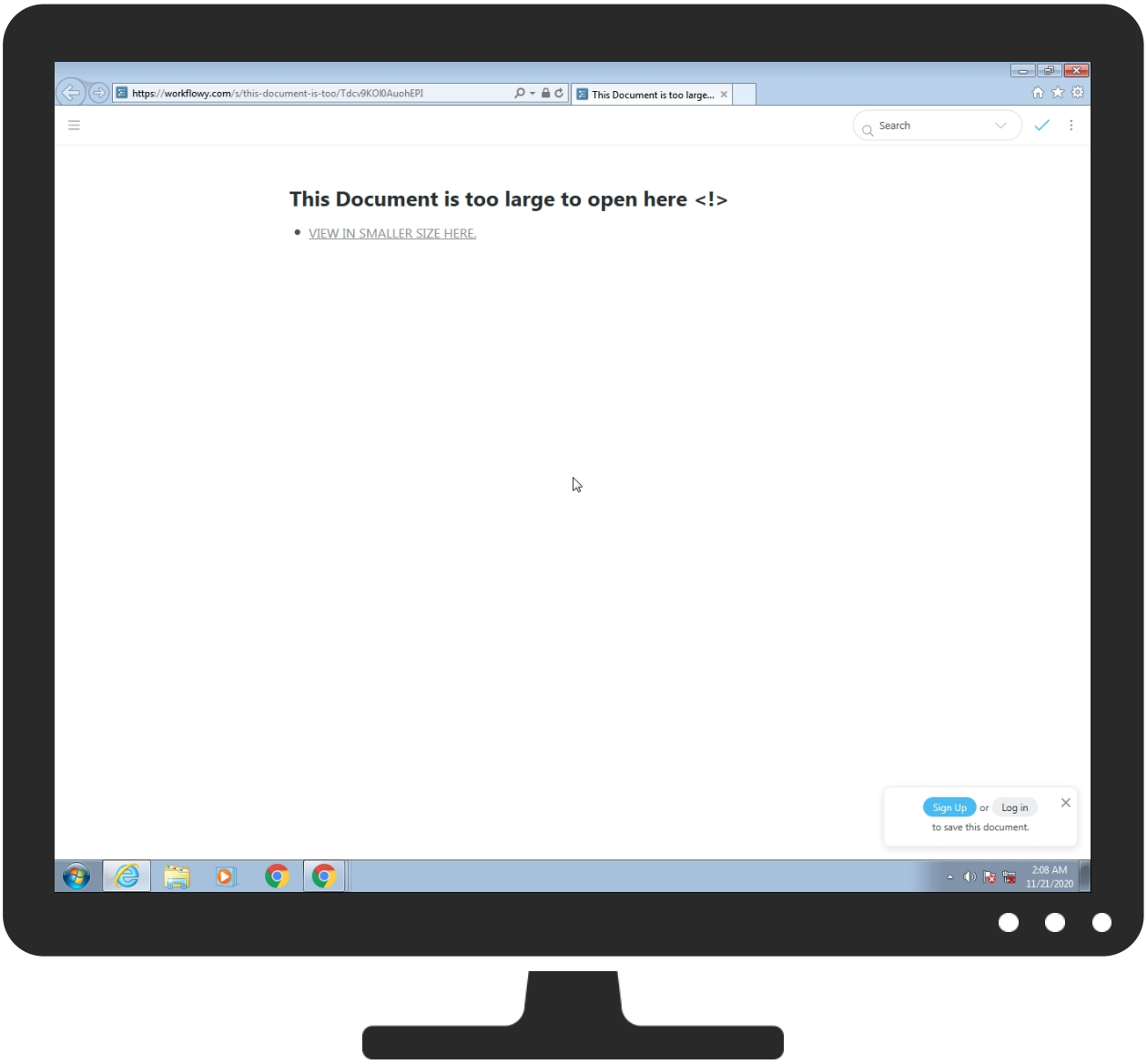


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

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

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
bam-cell.nr-data.net	0%	Virustotal		Browse

URLs

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	

Source	Detection	Scanner	Label	Link
http://https://jamif-cdn3d.us-east-1.linodeobjects.com/dfce06801e1a85d6d06f1fdd4475dacd.html	100%	UrlScan	phishing brand: generic microsoft	Browse
http://https://workflowy-east-1.linodeobjects.com/dfce06801e1a85d6d06f1fdd4475dacd.htmlRoot	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://www.google.%/ads/ga-audiences?	0%	URL Reputation	safe	
http://https://jamif-cdn3d.us	0%	Avira URL Cloud	safe	
http://getfirefox.com	0%	Avira URL Cloud	safe	
http://https://jamif-cdn3d.us-east-1.linodeobjects.com/dfce06801e1a85d6d06f1fdd4475dacd.html8This	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
stats.l.doubleclick.net	74.125.140.156	true	false		high
js-agent.newrelic.com	unknown	unknown	false		high
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://workflowy.com/s/this-document-is-too/Tdcv9KOl0AuohEPI	false		high
http://https://workflowy.com/s/this-document-is-too/Tdcv9KOl0AuohEPI#/7686a5f8c6e6	false		high
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/login/?next=/s/this-document-is-too/Tdcv9KOl0AuohEPI	false		high
http://https://workflowy.com/signup/?next=/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.3.dr	false		high
http://https://workflowy.com/s/this-document-is-too/Tdcv9KOl0AuohEPI#/7686a5f8c6e6	~DF2A13DD1A919A2BA2.TMP.2.dr	false		high
http://https://workflowy.com/s/this-document-is-too/Tdcv9KOl0AuohEPIRoot	{4D8EA032-2BE1-11EB-ADCF-ECF4BBB5915B}.dat.2.dr	false		high
http://https://workflowy.com/media/i/favicon.ico	imagestore.dat.3.dr	false		high
http://https://jamif-cdn3d.us-east-1.linodeobjects.com/dfce06801e1a85d6d06f1fdd4475dacd.html	~DF2A13DD1A919A2BA2.TMP.2.dr	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	~DF2A13DD1A919A2BA2.TMP.2.dr	false		high
http://https://workflowy.com/s/this-document-is-too/Tdcv9KOl0AuohEPInThis	~DF2A13DD1A919A2BA2.TMP.2.dr	false		high
http://https://workflowy.com/login/?next=/s/this-document-is-too/Tdcv9KOl0AuohEPI	~DF2A13DD1A919A2BA2.TMP.2.dr	false		high
http://https://workflowy-east-1.linodeobjects.com/dfce06801e1a85d6d06f1fdd4475dacd.htmlRoot	{4D8EA032-2BE1-11EB-ADCF-ECF4BBB5915B}.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://workflowy.com/s/this-doRoot	{4D8EA032-2BE1-11EB-ADCF-ECF4BBB5915B}.dat.2.dr	false		high
http://https://workflowy.com/	{4D8EA032-2BE1-11EB-ADCF-ECF4BBB5915B}.dat.2.dr	false		high
http://https://workflowy.com/s/this-document-is-too/Tdcv9KOl0AuohEPI	~DF2A13DD1A919A2BA2.TMP.2.dr, ~WRS{0863C5D3-5908-4917-8FD7-8909E0160183}.tmp.0.dr	false		high
http://https://www.google.%/ads/ga-audiences?	ga[1].js.3.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://https://stats.g.doubleclick.net/j/collect?	ga[1].js.3.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://workflowy.com/login/?next=/s/this-document-is-too/Tdcv9KOl0AuohEPI&Log	~DF2A13DD1A919A2BA2.TMP.2.dr	false		high
http://https://workflowy.com/media/i/favicon.ico~	imagestore.dat.3.dr	false		high
http://https://jamif-cdn3d.us	{4D8EA032-2BE1-11EB-ADCF-ECF4BBB5915B}.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://workflowy.com/s/this-document-is-too/Tdcv9KOl0AuohEPI#/7686a5f8c6e6workflowy.com/media/i/fav	~DF2A13DD1A919A2BA2.TMP.2.dr	false		high
http://getfirefox.com	document_view.min[1].js.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://workflowy.com/accounts/password_reset/	signup[1].htm0.3.dr, login[1].htm0.3.dr	false		high
http://https://jamif-cdn3d.us-east-1.linodeobjects.com/dfce06801e1a85d6d06f1fdd4475dacd.html8This	~DF2A13DD1A919A2BA2.TMP.2.dr	true	• Avira URL Cloud: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
74.125.140.156	unknown	United States		15169	GOOGLEUS	false
54.84.56.113	unknown	United States		14618	AMAZON-AESUS	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	321374
Start date:	21.11.2020
Start time:	02:05:59
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 17s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Fennec Pharma .docx
Cookbook file name:	defaultwindowsofficecookbook.jbs

Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	6
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal48.winDOCX@4/71@5/2
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): dllhost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 88.221.62.148, 216.58.212.136, 13.107.5.80, 204.79.197.200, 13.107.21.200, 151.101.2.110, 151.101.66.110, 151.101.130.110, 151.101.194.110, 162.247.243.146, 162.247.243.147, 152.199.19.161 • Excluded domains from analysis (whitelisted): www.bing.com, dual-a-0001.a-msedge.net, tls12.newrelic.com.cdn.cloudflare.net, ie9comview.vo.msecnd.net, api.bing.com, f4.shared.global.fastly.net, r20swj13mr.microsoft.com, e11290.dspg.akamaiedge.net, ssl.google-analytics.com, iecvlist.microsoft.com, e-0001.e-msedge.net, go.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, go.microsoft.com.edgekey.net, www-bing-com.dual-a-0001.a-msedge.net, ssl-google-analytics.l.google.com, api-bing-com.e-0001.e-msedge.net, cs9.wpc.v0cdn.net • Report size getting too big, too many NtDeviceIoControlFile calls found. • Report size getting too big, too many NtQueryAttributesFile calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
74.125.140.156	http://secure.aypf.org	Get hash	malicious	Browse	
	http://pizzaeaters.top	Get hash	malicious	Browse	
	http://https://outlookonedriveupd.wixsite.com/office	Get hash	malicious	Browse	
	http://sjmm.2.vu/vv	Get hash	malicious	Browse	
	http://https://ws.onehub.com/files/mz8ok6gf	Get hash	malicious	Browse	
	http://https://www.paperturn-view.com/?pid=MTE116034	Get hash	malicious	Browse	
	http://mediaonetv.in	Get hash	malicious	Browse	
	http://https://urldefense.com/v3/__https://www.swapcard.com/fr/support/?entity=Attendee__;!!ORetoJg!cvFBCSJtUQP4SxbgyWoSvc6xFbn2Yxso1-ZyBfSCejSXmPOASW6xeeoHHlcA0bUqeo8I$	Get hash	malicious	Browse	
	http://https://joom.ag/ZLwC	Get hash	malicious	Browse	
	http://https://www.flipsnack.com/securedocument/secure-document/full-view.html	Get hash	malicious	Browse	
	http://https://pcparch.bubbleapps.io/version-test?debug_mode=true	Get hash	malicious	Browse	
	http://https://redbooth.com/n/a9e9c571c584d07e/defabco-inc	Get hash	malicious	Browse	
	http://https://metalloidcorp.bubbleapps.io/version-test?debug_mode=true	Get hash	malicious	Browse	
	http://wholesale.everlyclothing.com	Get hash	malicious	Browse	
	http://creativegigs.net	Get hash	malicious	Browse	
	http://https://deref-mail.com/mail/client/QUue7ijDGeE/dereferrer/?redirectUrl=https%3A%2F%2Fadmin.microsoft.com%2Fadminportal%2Fhome%3Fref%3DMessageCenter%3FshowPref%3D1	Get hash	malicious	Browse	
	http://https://joom.ag/kjjC	Get hash	malicious	Browse	
	http://www.martialtalk.com/threads/a-day-with-ron-chapel.27329/	Get hash	malicious	Browse	
	http://https://irzizagmouzen2020s.com/.login/	Get hash	malicious	Browse	
	http://https://event.on24.com/wcc/r/2462461/BB0A869CCD07459AE0E4C73F0AD810E3/1209023?partnerref=connect	Get hash	malicious	Browse	
54.84.56.113	Fennec Pharma.xlsx	Get hash	malicious	Browse	
	Fennec Pharma.xlsx	Get hash	malicious	Browse	

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
stats.l.doubleclick.net	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
	http://https://tgcdevgroup-my.sharepoint.com/:b:/g/personal/jmoore_tgcgroup_net/EcgJdwLEdb9OriDBRaw9slAB4_8AMjn68ZCbL_ahHtwjIA?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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
	http://https://soprapaludo.it/	Get hash	malicious	Browse	• 108.177.15.157

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AMAZON-AESUS	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
	AccountStatements.html	Get hash	malicious	Browse	• 18.209.113.162
GOOGLEUS	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
	http://https://largemail.r1.rpost.net/files/7xU97qcFgCvB3Uv1wDC4qvS2ZriLfublohKWA5V3/ln/en-us	Get hash	malicious	Browse	• 172.217.23.161

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
7dcce5b76c8b17472d024758970a406b	Fennec Pharma.xlsx	Get hash	malicious	Browse	• 74.125.140.156 • 54.84.56.113
	ACH & WIRE REMITTANCE ADVICE.xlsx	Get hash	malicious	Browse	• 74.125.140.156 • 54.84.56.113
	PO 20-11-2020.pps	Get hash	malicious	Browse	• 74.125.140.156 • 54.84.56.113
	Avion Quotation Request.doc	Get hash	malicious	Browse	• 74.125.140.156 • 54.84.56.113
	http://https://www.lnepia.com.cn/app/4gnf/tiaoban.php	Get hash	malicious	Browse	• 74.125.140.156 • 54.84.56.113
	#U0648#U0631#U0634#U0629 #U0639#U0645#U0644 #U062a#U062f#U0631#U06cc#U0628#U06cc#U0629.doc	Get hash	malicious	Browse	• 74.125.140.156 • 54.84.56.113
	doc2227740.xls	Get hash	malicious	Browse	• 74.125.140.156 • 54.84.56.113
	POSH XANADU Order-SP-20093000-xlxs.xlsx	Get hash	malicious	Browse	• 74.125.140.156 • 54.84.56.113
	d11311145.xls	Get hash	malicious	Browse	• 74.125.140.156 • 54.84.56.113
	MV GRAN LOBO 008.xlsx	Get hash	malicious	Browse	• 74.125.140.156 • 54.84.56.113
	ACH WIRE PAYMENT REMITTANCE.xlsx	Get hash	malicious	Browse	• 74.125.140.156 • 54.84.56.113
	ACH - WIRE PAYMENT REMITTANCE.xlsx	Get hash	malicious	Browse	• 74.125.140.156 • 54.84.56.113
	ACHWIRE REMITTANCE ADVICE..xlsx	Get hash	malicious	Browse	• 74.125.140.156 • 54.84.56.113
	ACH WIRE REMITTANCE PAYMENT.xlsx	Get hash	malicious	Browse	• 74.125.140.156 • 54.84.56.113
	ACH & WIRE REMITTANCE.xlsx	Get hash	malicious	Browse	• 74.125.140.156 • 54.84.56.113
	ACH & WIRE REMITTANCE.xlsx	Get hash	malicious	Browse	• 74.125.140.156 • 54.84.56.113
	ACH WIRE REMITTANCE COPY.xlsx	Get hash	malicious	Browse	• 74.125.140.156 • 54.84.56.113
	ACH WIRE REMITTANCE..xlsx	Get hash	malicious	Browse	• 74.125.140.156 • 54.84.56.113
	ACH WIRE REMITTANCE.xlsx	Get hash	malicious	Browse	• 74.125.140.156 • 54.84.56.113
	POSH XANADU Order-SP-20-V241e.xlsx	Get hash	malicious	Browse	• 74.125.140.156 • 54.84.56.113

Dropped Files

No context

Created / dropped Files

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

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\MP98E46N\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):	6470
Entropy (8bit):	5.0200630717708785
Encrypted:	false
SSDEEP:	192:OfycecXycecDycecDycecLycecjycecNycecNvcecNvcecPvcec1vcecp:OfycecXycecDycecDycecLycecjycecX
MD5:	755A289645BD1E1D9C561C6AEAA0E9E0
SHA1:	C0A9E91C78F972DFADC2053054CE575864BCDC2A
SHA-256:	D1076278810889321874498374 5DB555CAE8C3AC234AC16852A5AA3DE0F5F083
SHA-512:	286E310830239A2914B3E4253C5BAC8F4701846E7C41BA22BD1998542C4EE4E2D4DA991DFEDF9FE293484DF9BD4722A466131762D98421083C4F770A54E66E2C
Malicious:	false
Reputation:	low
Preview:	<root></root><root><item name="mostRecentlyOpenedWindowId" value="1605953229455-0.5485350475385505" ltime="318480016" htime="30851054" /></root><root> <item name="mostRecentlyOpenedWindowId" value="1605953229455-0.5485350475385505" ltime="318480016" htime="30851054" /><item name="userstorage.user_id" value="-1" ltime="320560016" htime="30851054" /><item name="userstorage.format_version" value="3" ltime="320560016" htime="30851054" /></root><root><item name="mostRecentlyOpenedWindowId" value="1605953229455-0.5485350475385505" ltime="318480016" htime="30851054" /><item name="userstorage.user_id" value="-1" ltime="320560016" htime="30851054" /><item name="userstorage.format_version" value="3" ltime="320560016" htime="30851054" /><item name="use rstorage.appcache_id" value="2020-11-21 01:07:17.978870" ltime="320580016" htime="30851054" /></root><root><item name="mostRecentlyOpenedWindowId" val ue="1605953229455-0.5485350475385505" ltime="318480016" htime="30851054" /><item name="userstorage.u

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{4D8EA030-2BE1-11EB-ADCF-ECF4BBB5915B}.dat	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	33368
Entropy (8bit):	1.8682359182233892
Encrypted:	false
SSDEEP:	48:IvAGcpU9Gwp0KcG/apnK1crGIpHK1LJGvnZpEK1L15GoRVqpqK1L1IIGo4tF5pZq:MkKnKJpr9JHaL0ht353tuaRi3
MD5:	BE4C5A148D093F9AE72F1AEBB9F37CDD
SHA1:	C7ECF4AA5CA7504530F082815DAEA664A6644E28
SHA-256:	5BBBC574870D6DCD9B5DA67FDDC0DF8191315F68BA8505B8007F294470911CC0
SHA-512:	ECB849567B1064B95075F035BBF8D9E1F730E069640641082FB85B317002B33FFB2BFE1E438AC9CEE035A9416213EA3A81DE3699CB1197FF8A0E3FDE261867F1
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\{4D8EA032-2BE1-11EB-ADCF-ECF4BBB5915B}.dat	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	77010

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{4D8EA032-2BE1-11EB-ADCF-ECF4BBB5915B}.dat	
Entropy (8bit):	2.3546402693604365
Encrypted:	false
SSDEEP:	768:BPY2WOYOYjZKIi6aLZY2vcNpyBP9eFa1NL/w:9ofl7BoWQ0pypsAHrw
MD5:	8C372D7FA087FFAA3C36ECA190F430A3
SHA1:	E45FEE9C6B49B175C45C0E2A1BE9A5B5BB6413B6
SHA-256:	8EBE518EA318C406EF17DDED92F336A7B1DC84AAD812DF45E1DDC3E61985AB85
SHA-512:	7465E210C128FCD1EBEB399AF12EEA65203B67FEF24D6833F472031834EF755BB1C578CCF17EA9EF431B0907E821E41B9C2B74D3C2C4BADF4F9AE087E1FF0CI A
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\{63490D46-2BE1-11EB-ADCF-ECF4BBB5915B}.dat	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5666262711770778
Encrypted:	false
SSDEEP:	48:Iv0GcpURGwpNcG4pPQGrapgS3rGQpZpG7HpCpsTGIpG:MoKLb8JueS3F/I0p4A
MD5:	FB33C587FFEC2760F559648B87AA28CF
SHA1:	AF2361097A43CCE9EEBD9EB88E13CD1562B87899
SHA-256:	32163CD17CC268E8DB895D4363D7733685C136881639BF5409367535BE9D967D
SHA-512:	914CFE998CAB11CCFDF2DFEF0168AFE1443F8917D912E3B09B43E48F2FBC4614083EC5E2B3BAC2CAD743A19816D28411BE730ACF4A867BED9830FA3EDBDD4 DD0
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\lr5drzg\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	370820
Entropy (8bit):	4.812196469332186
Encrypted:	false
SSDEEP:	1536:UD48rp0/IBXhIyug/7rbkQblJ0AAdNP2I1u:P8e/IBXjLAXeI1u
MD5:	07B89D73BAFD9E0F4F5E05279213907F
SHA1:	A664D8028BB1FA5A5DA177E874EEF2BD6970D6B1
SHA-256:	489C783F8471A485B69A3E81ED9340EB96921C15CA2F2314D30F4DE06B2D5E98
SHA-512:	FDDB636D06D97AA1020FC7CF116F85F03AACE5D1B1797DCB311813CEF61FFACFD67105BCEB4680E58C31DED9D1EEBB39CB07EA410DA79C688703402A5E869 C0
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\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\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):	5.427827420772605
Encrypted:	false
SSDEEP:	384:doPdCvSS/yNrbLXTkc4SRzKeO0bT9GVYlTrcSUn0t0aOuPgl5YGm3TF9:doPNwcDPDbT/tQSUn7aOPmGm3Tv
MD5:	EDD0E7054E0AFB0C108A450DD0BAEB0A
SHA1:	0268CBBABD7FC34F27A45B16C7EA94290FEBC5C1
SHA-256:	363340B8C89CAB46D86371F32C07A4FC5BC89C4F1AC08E94E02C845B3F94F94E

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\Tdcv9KOl0AuohEPl[1].htm	
SHA-512:	14D2E02DD933B473B3BEA341EF95B860C49A6EB91C38F6C3D71DC1292C09623BE5B840309BA9425CCC8FBB42E38E067A5758AC5B639D76CE78C2FD3C4CF910AB
Malicious:	false
Reputation:	low
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\Temporary Internet Files\Content.IE5\5JC0A1KN\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:	49298181F084D342B04993DB1D59A443933D153C6B2D378E2AF4B95769785CC13053E2213473800EF8F0AD0E240E98DBE93DAB1805272BEEAC8E0A1D90AD93B8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://workflowy.com/media/js/adf9fc155506e2fa3fbf.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\Temporary Internet Files\Content.IE5\5JC0A1KN\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:	79F2D634CE675709189 39DF10A075576
SHA1:	BA47B7DACB11250F9B1B3974B34954B188E3ECAD
SHA-256:	D10C94B6CDB747904BAEE9070F003BB45849DA46F8100B1320F286C21CBCAAA1
SHA-512:	155FAB1EC68F300DDCB948D024995539C721A2AB0FD89C220F0EFFA68C3863507CBEF806F087F5C84EAB38D4C53DA94BC893894E8FC9DED388DACFE3244E18E
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	NREUM.setToken({'stn':1,'err':1,'ins':1,'cap':0,'spa':1})

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\favicon[1].ico	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 4-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	237
Entropy (8bit):	6.1480026084285395
Encrypted:	false
SSDEEP:	6:6v/lhPIF6R/C+u1fXNg1XQ3yslRtNO+cKvAElRApGCp:6v/7b/C1fm1ZslRTvAElR47
MD5:	9FB559A691078558E77D6848202F6541
SHA1:	EA13848D33C2C7F4F4BAA39348AEB1DBFAD3DF31
SHA-256:	6D8A01DC7647BC218D003B58FE04049E24A9359900B7E0CEBAE76EDF85B8B914
SHA-512:	0E08938568CD123BE8A20B87D9A3AAF5CB05249DE7F8286FF99D3FA35FC7AF7A9D9797DD6EFB6D1E722147DCFB74437DE520395234D0009D452FB96A8ECE23B
Malicious:	false
Reputation:	high, very likely benign file
IE Cache URL:	http://www.bing.com/favicon.ico

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\favicon[1].ico	
Preview:	.PNG.....IHDR.....R....sRGB.....gAMA.....a.....pHYs.....o.d...-PLTE.....(..5..X..h.....J4.I...IIDAT.[c`..&.(.....F....cX.(@.j.+@..K.(..2L....1.{.....c`]L 9.&2.I...I..E.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\httpErrorPagesScripts[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	8714
Entropy (8bit):	5.312819714818054
Encrypted:	false
SSDEEP:	192:xmjriGCiOciwd1BtvjrG8tAGGGHmjOWnvyJVUXiki3ayimi5ezxiV:xmjriGCi/i+1Btvjy815HmjqVUXiki3g
MD5:	3F57B781CB3EF114DD0B665151571B7B
SHA1:	CE6A63F996DF3A1CCCB81720E21204B825E0238C
SHA-256:	46E019FA34465F4ED096A9665D1827B54553931AD82E98BE01EDB1DDBC94D3AD
SHA-512:	8CBF4EF582332AE7EA605F910AD6F8A4BC28513482409FA84F08943A72CAC2CF0FA32B6AF4C20C697E1FAC2C5BA16B5A64A23AF0C11EEFBF69625B8F9F90C8 A
Malicious:	false
Reputation:	high, very likely benign file
IE Cache URL:	res://ieframe.dll/httpErrorPagesScripts.js
Preview:	...function isExternalUrlSafeForNavigation(urlStr)..{..var regEx = new RegExp("^(http(s?)|ftp|file)://", "i");..return regEx.exec(urlStr);..}..function clickRefresh()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.su bstring(poundIndex+1)))..{..window.location.replace(location.substring(poundIndex+1));..}..}..function navCancelInit()..{..var location = window.location.href;..var pound Index = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..var bElement = document.createElement("A");..bElement.innerText = L_REFRESH_TEXT;..bElement.href = 'javascript:clickRefresh()';..navCancelContainer.appendChild(bElement);..}..else..{..var textNode = document.createTextNode(L_RELOAD_TEXT);..navCancelContainer.appendChild(textNode);..}..}..function expandCollapse(elem,

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\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:	01507CB531465D496E475994A901D2E54E654810BDADE13BEB0480E9CA75FC92B0E4A5689646CC17FC2B10F93F00C1B000CD5B7C9B024F4A7A60F97905C1658
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\Temporary Internet Files\Content.IE5\5JC0A1KN\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:	1EAAE52797DDC5ECC686D6351BFB152DB1276C644E33DAFE9ACA9B81EE9AA75D29FA04A12A64B3B281E0163C318E9832861D9553C67A984D3958E90EF57FE5 C
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\Temporary Internet Files\Content.IE5\T4O403JZ\Tdcv9KOl0AuohEPI[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\Tdcv9KOl0AuohEPI[1].htm	
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	15359
Entropy (8bit):	5.428213061571943
Encrypted:	false
SSDEEP:	384:doPdCvSS/yNrbLXTkc4SRzKeO0bT9GVYlTrcMUn050aOuPgl5YGm3TF9:doPNwcDPDbT/tQMUnHaOPmGm3Tv
MD5:	F7A8F1BF1B39C510AAEB9BA8277AA138
SHA1:	1BA9D479FB4C1854929FE6582D267AF91471EBC9
SHA-256:	F122C256F319D5C9122CEF63B37810A28D72FE5EA3891452A5D08428FBAEA2DB
SHA-512:	B455DDD55324DDAA0B2D4E8DB6EA6AAE858BD70FF4683858710EC19D76857C26ABAECD38E8EF43631831C7E313D25AF86C72D5011E169325739F46B5D07A05F
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\Temporary Internet Files\Content.IE5\T4O403JZ\dnserror[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	1857
Entropy (8bit):	4.6050684780693905
Encrypted:	false
SSDEEP:	24:rCUcWh0sEimVM4mVMyIjyAV28EFySd8/k+C2E93vjqF4IAr4:uUjEiV4VtLV2lFjq29vjNRr4
MD5:	73C70B34B5F8F158D38A94B9D7766515
SHA1:	E9EAA065BD6585A1B176E13615FD7E6EF96230A9
SHA-256:	3EBD34328A4386B4EBA1F3D5F1252E7BD13744A6918720735020B4689C13FCF4
SHA-512:	927DCD4A8CFDEB0F970CB4EE3F059168B37E1E4E04733ED3356F77CA0448D2145E1ABDD4F7CE1C6CA23C1E3676056894625B17987CC56C84C78E73F60E08FCD
Malicious:	false
IE Cache URL:	res://ieframe.dll/dnserror.htm
Preview:	.<!DOCTYPE HTML>..<html>.... <head>.. <link rel="stylesheet" type="text/css" href="NewErrorPageTemplate.css" >.... <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.. <title>This page can’t be displayed</title>.... <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="javascript:getInfo();">.. .. This page can’t be displayed .. .. <ul id="cantDisplayTasks" class="tasks">.. <li id="task1-1">Make sure the web address is correct. .. <li id="task1-2">Look for the page with your search

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\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\Temporary Internet Files\Content.IE5\T4O403JZ\eaeea54ab7[2].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	modified
Size (bytes):	24
Entropy (8bit):	2.459147917027245
Encrypted:	false
SSDEEP:	3:CUXJ/lH:Dl
MD5:	BC32ED98D624ACB4008F986349A20D26

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\eaeea54ab7[2].gif	
SHA1:	2D3DF8C11D2168CE2C27E0937421D11D85016361
SHA-256:	0C9CF152A0AD00D4F102C93C613C104914BE5517AC8F8E0831727F8BFBE8B300
SHA-512:	71ACC6DA78D5D5BF0EEA30E2EE0AC5C992B00EFEC959077DFE0AB769F1DBBD9AF12D5C5C155046283D5416BEB606A9EF323FB410E903768B1569B69F37075E4E
Malicious:	false
Preview:	GIF89a.......,..........

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\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\Temporary Internet Files\Content.IE5\T4O403JZ\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:qVoB3tUROGclXqyvXboAcMBXqWSZUXqXlIVLLPbCXqwcWWGu:q43tISl6kXiMIWSU6XlI5LPJpfGu
MD5:	7B4F513528A3D65397F0E7F6DEF7AD4A
SHA1:	5DA8E55D7F30D9530BDEFB6FD670C273FF9DDD66
SHA-256:	5075788CBBDF48D111B4882949D3E50856C81CA87630A85D7C8DD1E600CDC691
SHA-512:	1EAAE52797DDC5ECC686D6351BFB152DB1276C644E33DAFE9ACA9B81EE9AA75D29FA04A12A64B3B281E0163C318E9832861D9553C67A984D3958E90EF57FE5C
Malicious:	false
Preview:	<html>..<head><title>301 Moved Permanently</title></head>..<body>..<center> 301 Moved Permanently </center>..<hr><center>nginx/1.19.4</center>.. </body>..</html>..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\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\Temporary Internet Files\Content.IE5\T4O403JZ\urlblockindex[1].bin	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	data
Category:	downloaded
Size (bytes):	16
Entropy (8bit):	1.6216407621868583
Encrypted:	false
SSDEEP:	3:PF/l:
MD5:	FA518E3DFAE8CA3A0E495460FD60C791
SHA1:	E4F30E49120657D37267C0162FD4A08934800C69
SHA-256:	775853600060162C4B4E5F883F9FD5A278E61C471B3EE1826396B6D129499AA7
SHA-512:	D21667F3FB081D39B579178E74E9BB1B6E9A97F2659029C165729A58F1787DC0ADADD980CD026C7A601D416665A81AC13A69E49A6A2FE2FDD0967938AA645C0
Malicious:	false
IE Cache URL:	http://https://r20swj13mr.microsoft.com/ieblocklist/v1/urlblockindex.bin
Preview:	.p.J2.....

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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\e42577a28f6c3e306a7f[1].js	
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\Temporary Internet Files\Content.IE5\XNHC0JWC\errorPageStrings[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	3470
Entropy (8bit):	5.076790888059907
Encrypted:	false
SSDEEP:	96:z9UUiqRxqH211CUIRHERyRyntQRXaR8RS6C87a/5/+mhPcF+5g+mOC53B5Fqs1qP:JsUOHaQyYX4yJQOWCbz1Qb5
MD5:	6B26ECFA58E37D4B5EC861FCDD3F04FA
SHA1:	B69CD71F68FE35A9CE0D7EA17B5F1B2BAD9EA8FA
SHA-256:	7F7D1069CA8A852C1C8EB36E1D988FE6A9C17ECB8EFF1F66FC5EBFEB5418723A
SHA-512:	1676D43B977C07A3F6A5473F12FD16E56487803A1CB9771D0F189B1201642EE79480C33A010F08DC521E57332EC4C4D888D693C6A2323C97750E97640918C3F4
Malicious:	false
IE Cache URL:	res://ieframe.dll/errorPageStrings.js
Preview:	.//Split out for localization...var L_GOBACK_TEXT = "Go back to the previous page.";..var L_REFRESH_TEXT = "Refresh the page.";..var L_MOREINFO_TEXT = "More information";..var L_OFFLINE_USERS_TEXT = "For offline users";..var L_RELOAD_TEXT = "Retype the address.";..var L_HIDE_HOTKEYS_TEXT = "Hide tab shortcuts";..var L_SHOW_HOTKEYS_TEXT = "Show more tab shortcuts";..var L_CONNECTION_OFF_TEXT = "You are not connected to the Internet. Check your Internet connection.";..var L_CONNECTION_ON_TEXT = "It appears you are connected to the Internet, but you might want to try to reconnect to the Internet.";..../used by invalidcert.js and hstscerterror.js..var L_CertUnknownCA_TEXT = "The security certificate presented by this website was not issued by a trusted certificate authority.";..var L_CertExpired_TEXT = "The security certificate presented by this website has expired or is not yet valid.";..var L_CertCNMismatch_TEXT = "The security certificate presented by this website was issued for a di

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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\logo-bullet-lines-blue[1].svg	
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\Temporary Internet Files\Content.IE5\ZAE7RW1P\NewErrorPageTemplate[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	1310
Entropy (8bit):	4.810709096040597
Encrypted:	false
SSDEEP:	24:5Y0bn73pHIUZtJD0lFBohpZlJiHqw87xTeB0yVFaFG:5b73HJq0TJiHp89TOwU
MD5:	CDF81E591D9CBFB47A7F97A2BCDB70B9
SHA1:	8F12010DFAACDECAD77B70A3E781C707CF328496
SHA-256:	204D95C6FB161368C795BB63E538FE0B11F9E406494BB5758B3B0D60C5F651BD
SHA-512:	977DCC2C6488ACAF0E5970CEF1A7A72C9F9DC6BB82DA54F057E0853C8E939E4AB01B163EB7A5058E093A8BC44ECAD9D06880FDC883E67E28AC67FEE4D070A4CC
Malicious:	false
IE Cache URL:	res://ieframe.dll/NewErrorPageTemplate.css
Preview:	.body..{.. background-repeat: repeat-x;.. background-color: white;.. font-family: "Segoe UI", "verdana", "arial";.. margin: 0em;.. color: #575757;..}.....mainContent..{.. margin-top:80px;.. width: 700px;.. margin-left: 120px;.. margin-right: 120px;..}.....title..{.. color: #2778ec;.. font-size: 38pt;.. font-weight: 300;.. vertical-align:bottom;.. margin-bottom: 20px;.. font-family: "Segoe UI", "verdana";.. position: relative;..}.....errorExplanation..{.. color: #000000;.. font-size: 12pt;.. font-family: "Segoe UI", "verdana", "arial";.. text-decoration: none;..}.....taskSection..{.. margin-top: 20px;.. margin-bottom: 40px;.. position: relative; ..}.....tasks..{.. color: #000000;.. font-family: "Segoe UI", "verdana";.. font-weight:200;.. font-size: 12pt;.. padding-top: 5px;..}....li..{.. margin-top: 8px;..}.....diagnoseButton..{.. outline: none;.. font-size: 9pt;..}.....launchInternetOptionsBu

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\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\Temporary Internet Files\Content.IE5\ZAE7RW1P\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:	E8429B1EA465EAE47132E08149EA7976176A63CF1A72E55918DC8A6C107B3EC270B838902492DF8E78640DC96BF434CC943AEDE9D5E78CE88DA28D4400661736
Malicious:	false
IE Cache URL:	http://https://workflowy.com/login/?next=/s/this-document-is-too/Tdcv9KOl0AuohEPI

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\login[1].htm	
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\Temporary Internet Files\Content.IE5\ZAE7RW1P\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\Temporary Internet Files\Content.IE5\ZAE7RW1P\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:jwj4cNN8AfppuL5EVJSWhGUUkIkKyOd0JbAWAbEbaxx33GNNqkUka6WqyZXOREmi: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
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\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\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
MD5:	D06B9C7BBDB584E891AF7470C540373F
SHA1:	9E09177E303D5EC1876E1183842BFE60D4BCBC17
SHA-256:	1D96DED3CBB2E05D247CA03185BA021F790DBE8AABDD03DF56BBC27AB84BD7D6
SHA-512:	C53D4C04BA93098544DC3C9EDA61CA61D72153F3B871E36786F5961CBB6E6BB8FB567D215D8B04B487825535E4313A313DDB4F0D38CCFB6E7EFB45DE5900C9E
Malicious:	false
IE Cache URL:	http://https://workflowy.com/media/js/site.min.js

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\site.min[1].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\Temporary Internet Files\Content.MSO\2CB71C2A.png	
Process:	C:\Program Files\Microsoft Office\Office14\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
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\Temporary Internet Files\Content.MSO\424A15C8.wmf	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Targa image data - Map - RLE 65536 x 65536 x 0 "\004"
Category:	dropped
Size (bytes):	932
Entropy (8bit):	3.2043787588174073
Encrypted:	false
SSDEEP:	24:i0p+vdddddBgKm3TkXXUun/gnTsBuuuuOobK:Ms3QLoYu
MD5:	6D97AE53BC6D99F3088C2C3AF12626F8
SHA1:	0BBA44EC62E837E0F63CDA2CDE2747C949F62A6E
SHA-256:	6CDC4891CA97A0113A709ABD04A2CE37DAD638E3FC0422D812C9B582BC14DFC5
SHA-512:	CD4EA6092608FD2356150B7E330A4C5125F8DAD2225A28D41021A8D30B449301568B497B6C970687C39783A1B162178BE63BA02CDD3CFCF35D3AD965C566D77
Malicious:	false
Preview:	.....@."Calibri.....-.....-.....-.....-.....-.....2.R..... .6.....Dr.....-..... .....-.....$.....-.....-.....7c....-.....-.....$.....-.....-.....'.....'.....{.....@."Calibri..... .....-.....-.....-.....-.....-.....2.....'.....OpenX.F.B.G.....2.....'..... .N.....{.....@. Calibri.....-.....-.....-.....-.....- .....-.....@.!.....'.....-.....'."System.....0.....'.....-.....-.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\59D359E7.png	
Process:	C:\Program Files\Microsoft Office\Office14\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....$E..kl..,..d...p...$..."(....x.....s.$J." ..\2...%g.(....=.}F.....}....?.O....U..:5d.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\8D1C9ABC.png	
Process:	C:\Program Files\Microsoft Office\Office14\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....lkk}.=...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\Temporary Internet Files\Content.MSO\AC76C38D.png	
Process:	C:\Program Files\Microsoft Office\Office14\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:	54D5BE5CA569AA474A05C84B65B56687AA3D76CBE048A4622C50AAA0AF608CB9ECB99779953DF2CA82FFA2D9D6349AAFCB57ECCFF8BD2934C1F5BD4C597F2E5F
Malicious:	false
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..'.....$...1)P0G0.c.hL%hf{.F@.....EqB8..p...Tr+.....!.....QGB...o`.;.d/..B.`v.(%w.!.**....>..O.dWG.!...# ".....N%.:.....m..K.....p+F~...Nm..~...-..~...%..*..b..1r.u...6.....CH..~..b1...D5wy...?9.p2/}4..9....r4..M.vW."[1r....I..V..P.B...6.H`....s....P...D.ph,@..Aj.....9F...."....P....(...T`...:....0..P_..m.>R7P.^.Q>...?.b=..y..@Y.....f..:..~.X..Xt.\.[..;}hW{'.v.R}5.u.k.. ./../...i.....~.Y;..".R.nq.W.....iL..r~h.....&..O.@.m..=...M.^....@.m.....}.....*...CV`..k^...,n....Ts..2.....$..1....._....Y..6..<.....3X..r.^.Fg.\..@.....[...`.....F..t .[.<LJ~l.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\Temporary Internet Files\Content.MSO\FA9F2A23.png	
Process:	C:\Program Files\Microsoft Office\Office14\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
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\Temporary Internet Files\Content.Word\~WRS{0863C5D3-5908-4917-8FD7-8909E0160183}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	7680
Entropy (8bit):	3.946342578354506
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{0863C5D3-5908-4917-8FD7-8909E0160183}.tmp	
SSDEEP:	96:7xOjeQ1g9TUzHXAqArK9LUkAl9ewDZ19vMeyHs2YbnFlX8G8:7IjeQ1g1EX/Q83aDZXMeyr03N8
MD5:	A681FBCE42F7EA8A71D1D74A0E2C6AC2
SHA1:	F6DB152B304C1F58E6CFE6CE3B301AC5D45E63A7
SHA-256:	E1FE8AA38F3A6D6174446D26BDC7A308E634D537EDC73A3E27164AA10880A2EA
SHA-512:	A50809DBC6CF5D686A05DDA163D4D284AE1A7A25F01A04357F325F700667CACBA3A2BC7228AB1321812CBC426876458769ECD0E22C85761432D1EA7D7FF2831
Malicious:	false
Preview:	..... .!."#.$.%.&.'.(.).*.+.,.-.../.0.1.2.3.4.5.6.7.8.9.:.;.<.=.>...../..... .M.a.r.k. .G.o.w.l.a.n.d. .s.h.a.r.e.d. .a. .f.i.l.e. .w.i.t.h. .y.o.u...../. .T.h.i.s. .l.i.n.k. .w.i.l.l. .w.o.r.k. .f.o.r. .e.v.e.r.y.o.n.e...../...-. .P.a.y.m.e.n.t. .R.u.n..... . . . . .T.h.i.s. .l.i.n.k. .e.x.p.i.r.e.s. .i.n. .2.4. .h.o.u.r.s..... .....x.....b..... ..$..d.....a$.gdH.L.l..... .....g...$..$.If....!v..h.#v..y.:V....]..t.....6`.....k.....0.....y..6.....,....5.....y.2.....2.....3.....4.....B....`.....p..... ....yt.k.....$..d.....a$.gdH.L.l..... ..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{B5D78783-1A3F-4CA6-941D-F5C2CCA9C0AC}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\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:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28B A4
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Temp\msoC39D.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\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:	C7B765B9AFBB9810B6674DBC5C5064ED96A2682E78D5DFFAB384D81EDBC77D01E0004F230D4207F2B7D89CEE9008D79D5FBADC5CB486DA4BC43293B7AA878 41
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\~DF162A030C2D645432.TMP	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.33319110222619813
Encrypted:	false
SSDEEP:	24:3NILONILKMNIIkNIIAMNlRxMNIRCMNlTwNlT4VMNISS/NISSGVMNlaAaMNlaAG:LyWvlxmdw4fSaSGeasG
MD5:	7450AD212389BD4EC710C0462F21E821
SHA1:	DCECB2617B1A197DAEB6D603590C39EB8F5E1CA2
SHA-256:	7CFAE7CB404D1A484C8E282CBAA2DE68AD04CD0DAE96884239 64AD766D178270
SHA-512:	D38715574D05285CF6D6E9F3F0ED40DD16C36FE587E142BF9517A73243233E3550976740CF541FC1FCC74B8C6F2C95779515A4796B3FC9BCA58817A06F6AA05F
Malicious:	false

C:\Users\user\AppData\Local\Temp\~DF162A030C2D645432.TMP	
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF2A13DD1A919A2BA2.TMP	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	75325
Entropy (8bit):	1.5626215421318816
Encrypted:	false
SSDEEP:	384:LyBvtM9emVp63NxUtq1GDjq1qGxqfqdfsYH4bH44sBsNsJAEsOcrs4crsZybJHsx:PgAFSdkYWCSOUO141Zy6B7H
MD5:	D4CA73C2ECF647FE227CE72A6FE1E0F1
SHA1:	EF140A2BE102ECC8B5AF622FA9B8EFCE3372BEE7
SHA-256:	61BAD9C1AA4D6AAC850EDBE78F561AD4904AF3F2F433FFA74ED813348434138F
SHA-512:	FD503244700112B8D03C9ABD8B93A1AA8B70D04282E5407CACA59CCCFE6372E1B42EA803A00C3EC3AD5E6028CD6C8A6CB0A758918E080AE7ED119DF78D19A4F
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... .....C.....K.j.j.a.q.f.a.j.N.2.c.0.u.z.g.v.1.l.4.q.y.5.n.f.W.e.....8.....X..... ....

C:\Users\user\AppData\Local\Temp\~DF48D934FA04C84F45.TMP	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13077
Entropy (8bit):	0.7256385150057252
Encrypted:	false
SSDEEP:	48:LypvqKqIKwQL5mobQL5QiK1LD5ILcycKcZ5iIio:LypvqBIZQL5dQL5Qii
MD5:	D0670624C33E7067738BCF6891A565D0
SHA1:	62F947E82F4BFFB3AE2E97D6EC8852701163BCED
SHA-256:	F03E8A4E1CF862BE7FAC18E9DA3D1AF46FDE987141953434613A7DD147E3F6B3
SHA-512:	5865FC49CCAE57056F38A6D4AD88D77817AE2AC8248C8980832FC68EB797815E7833A4AB24018746E5F3F6B55223E04B2D4462EECCEA64548AE2B30363C87D73
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Fennec Pharma .LNK	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Aug 26 14:08:13 2020, mtime=Wed Aug 26 14:08:13 2020, atime=Sat Nov 21 09:06:34 2020, length=49414, window=hide
Category:	dropped
Size (bytes):	2078
Entropy (8bit):	4.580177245734371
Encrypted:	false
SSDEEP:	48:83Xon/XT3IkHuJcbsAQh23Xon/XT3IkHuJcbsAQ/:83M/XLIkOebvQh23M/XLIkOebvQ/
MD5:	148BAA29BC5C8628C73C8F1146B1B157
SHA1:	031BD6BC3F08889A9FE2ED4843148053C03A2ABC
SHA-256:	998C7848D38348BFA949B55BB7A9252B3F9F4F1331A04F21E3A7EF9491E05441
SHA-512:	ABE78BBD8AD80FA247665E04C068F45546F67BEA84AF5333CA9B6D3D9F829F20FBFF40118EEC99B8F0A5F9F0CB7FE06B605A4E2AD0796BC62C66866B941A89D9
Malicious:	false
Preview:	L.....F.... ....I<..{...I<..{...@.....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....Q.y..Desktop.d.....QK.X.Q.y*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....p.2.....uQ.P .FENNEC~1.DOC..T.....Q.y.Q.y*...8.....F.e.n.n.e.c. .P.h.a.r.m.a. ...d.o.c.x.....}.....-...8...[.....?J.....C:\Users\..#.....\\841675\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.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....841675.....D_....3N...W...9F.C.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Category:	dropped
Size (bytes):	82
Entropy (8bit):	4.35722838343894
Encrypted:	false
SSDEEP:	3:HoAL/FXSzC7oFXSzCmxWoAL/FXSzCv:HdxSeeSexSI
MD5:	E85E4CBE668D138D52C4F57FD67362A3
SHA1:	B48BCF5A655C1420131627633C4F001AA5916324
SHA-256:	467053108BC5EB8C9DAA4B2EA865C06ACBF40517F211005B07CB005491567E71
SHA-512:	D92A2A0184B70E646CEFD0F9884B2A0072A9DC357E7208F0196C5E1DC18A1CCC495A570FEF9798F33D5AB118FFA285E851A21B9907BE859EBAE870AC7F64371
Malicious:	false
Preview:	[misc]..Fennec Pharma .LNK=0..Fennec Pharma .LNK=0..[misc]..Fennec Pharma .LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyokKOg5Gll3GwSKG/f2+1/ln:vdsCkWtW2IIID9l
MD5:	39EB3053A717C25AF84D576F6B2EBDD2
SHA1:	F6157079187E865C1BAADCC2014EF58440D449CA
SHA-256:	CD95C0EA3CEAEC724B510D6F8F43449B26DF97822F25BDA3316F5EAC3541E54A
SHA-512:	5AA3D344F90844D83477E94E0D0E0F3C96324D8C255C643D1A67FA2BB9EEBDF4F6A7447918F371844FCEDFCD6BBAAA4868FC022FDB666E62EB2D1BAB902891C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....w.....w.....P.w.....w.....z.....w.....x...

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\20008D2I.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	634
Entropy (8bit):	4.74188873839168
Encrypted:	false
SSDEEP:	12:QUU1tH4PYNo9QCDo9TVTRtNS9TVCV3N4iRiv+OV9TVRFjJe49TVXL3tNtBYYy9TA:QUUbYPidxOAZRiv+olFjJe4XZmG
MD5:	A5303C0653F113F66D5EAD08CF4809FA
SHA1:	6FF71F753FE894D990782EDEA8D160ACC8DA5E9A
SHA-256:	5A6CC7F554C03C3A3944CBBC010D77228A440515A3F315F43663B50026D8FC3A
SHA-512:	F15E8EF210B4607A7A632E80EF912E2D815072127C08238E450B06745832A81942FB51ED44F685E4FA5E872CB00F41C33DD62380A164412B69D80AA38CFABF01
Malicious:	false
Preview:	sessionid.8sg9cp8nervvwao1rn2kfg3mukuomzy2.workflowy.com/.9729.4207743360.30887590.1023768698.30851054.*.__utma.218586911.216721650.1605953227.1605953227.1.workflowy.com/.1600.790485120.30997905.1033697778.30851054.*.__utmb.218586911.3.10.1605953227.workflowy.com/.1600.1853000832.30851058.1033747779.30851054.*.__utmz.218586911.1605953227.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none).workflowy.com/.1600.4193499264.30887766.1033772780.30851054.*.__utmt.1.workflowy.com/.1600.1997902720.30851055.295395351.30851054.*.__utmv.218586911.|1=Cohort=2020-11-20=1.workflowy.com/.1600.790485120.30997905.1033797780.30851054.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\5YOAGXA2.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	632
Entropy (8bit):	4.729647852716512
Encrypted:	false
SSDEEP:	12:QUU1tH4PYNo9QCDo9TVatNbt9TV6VN4iRiv+OV9TVwFjrh49TVXL3tNtBYYy9TVK:QUUbYPidmte3Riv+oEFjrh4XZmor
MD5:	B09ED27ECC074695A6F6640CC2628F11
SHA1:	C4891B4514457C8E451CCC585297224DB51DC7E0
SHA-256:	1A9CE3D638AF2E66EFB034817A051C622CCDFBA9D3BBE2B577619E69B94B8F03
SHA-512:	5ACED22544E25A38B186E0762CAF54EAE1582F9D1648F9FB7DF74AD61E58118D717B9059762E8068481D5A4DC2012506E7A00C37ABBF19C93DC69EC302BC700
Malicious:	false

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\5YOAGXA2.txt	
Preview:	sessionid.8sg9cp8nervvwao1rn2kfg3mukuomzy2.workflowy.com/.9729.4207743360.30887590.1023768698.30851054.*.__utma.218586911.216721650.1605953227.1605953227.1.workflowy.com/.1600.780485120.30997905.1025328701.30851054.*.__utmb.218586911.2.10.1605953227.workflowy.com/.1600.1843000832.30851058.1025328701.30851054.*.__utmz.218586911.1605953227.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none).workflowy.com/.1600.418349926.30887766.1025328701.30851054.*.__utmt.1.workflowy.com/.1600.1997902720.30851055.295395351.30851054.*.__utmv.218586911.|1=Cohort=2020-11-20=1.workflowy.com/.1600.70485120.30997905.321311407.30851054.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\8UM1TNP9.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	634
Entropy (8bit):	4.7283714252854105
Encrypted:	false
SSDEEP:	12:QUU1tH4PYNo9QCDo9TVatNbt9TV6VN4iRiv+OV9TVwFjrh49TVXL3tNtBYYy9TVs:QUUbYPidmte3Riv+oEFjrh4XZmeX
MD5:	7F4D4F2B57AECC3784A3515947F72E64
SHA1:	60F0B9B3693E6F4ABD6AE95565340BD2AA11E08D
SHA-256:	107B35F187269D6821B43A7670E6E85819F6F1461E714ABFC44F651C126F0C96
SHA-512:	C924C8280A72456056F5F72DADFADC551DB794FFC034217B79325B7A479C604C0DBD6F562A01926214508D3594BC6755A4C0E4ACBBAC871905D6F7B057030F6
Malicious:	false
Preview:	sessionid.8sg9cp8nervvwao1rn2kfg3mukuomzy2.workflowy.com/.9729.4207743360.30887590.1023768698.30851054.*.__utma.218586911.216721650.1605953227.1605953227.1.workflowy.com/.1600.780485120.30997905.1025328701.30851054.*.__utmb.218586911.2.10.1605953227.workflowy.com/.1600.1843000832.30851058.1025328701.30851054.*.__utmz.218586911.1605953227.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none).workflowy.com/.1600.418349926.30887766.1025328701.30851054.*.__utmt.1.workflowy.com/.1600.1997902720.30851055.295395351.30851054.*.__utmv.218586911.|1=Cohort=2020-11-20=1.workflowy.com/.1600.780485120.30997905.1025484701.30851054.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\A3HA6TUX.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	630
Entropy (8bit):	4.7416365417542385
Encrypted:	false
SSDEEP:	12:QUU1tH4PYNo9QCDo9TVatNbt9TVrgN4iRiv+OV9TVjFjBiG49TVXL3tNtBYYy9T0:QUUbYPidmtaRiv+ofFjN4XZmor
MD5:	79186F895FB7C1AC20946645DFFAA227
SHA1:	9F371E1760782105581E8B5B389C68D601CFB35F
SHA-256:	09FC4CC03B1E92BC50D5B8F28DA29FBB4585B1A78BFBC76FD8F8FB6050D360CD
SHA-512:	6B170B25F8AAF291D0D3EC3C45D1ABC9424252AF54744015791FC3D2E7B0952EE5C1D6B9A70DBB508721453A1560D559517574892A25A6C0753A362AA3BDB17
Malicious:	false
Preview:	sessionid.8sg9cp8nervvwao1rn2kfg3mukuomzy2.workflowy.com/.9729.4207743360.30887590.1023768698.30851054.*.__utma.218586911.216721650.1605953227.1605953227.1.workflowy.com/.1600.780485120.30997905.1025328701.30851054.*.__utmb.218586911.2.10.1605953227.workflowy.com/.1600.1133000832.30851058.321236406.30851054.*.__utmz.218586911.1605953227.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none).workflowy.com/.1600.3473499264.30887766.321286407.30851054.*.__utmt.1.workflowy.com/.1600.1997902720.30851055.295395351.30851054.*.__utmv.218586911.|1=Cohort=2020-11-20=1.workflowy.com/.1600.70485120.30997905.321311407.30851054.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\D9YU0K3A.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	634
Entropy (8bit):	4.741239679820203
Encrypted:	false
SSDEEP:	12:QUU1tH4PYNo9QCDo9TVTRtNS9TVCV3N4iRiv+OV9TVRFjJe49TVXL3tNtBYYy9TE:QUUbYPidxOAZRiv+olFjJe4XZmq
MD5:	D9941DF34DF7CAED12A3541F721F9C6A
SHA1:	E30CECB94C5F88FF606AE5064337BD24A0367ACE
SHA-256:	63B8988EF43EE82C455DC621A1F19C9CCA1327D8B3D0CD83B98B80891CD18D65
SHA-512:	35BEADB3A69D8231A6ED3AC22884393947BA424D98F36E175FE459C3EF11E46316B82DF87B9CA8E31D8BB5E46485701ADD770A211F3142304854F5ACC657B445
Malicious:	false
Preview:	sessionid.8sg9cp8nervvwao1rn2kfg3mukuomzy2.workflowy.com/.9729.4207743360.30887590.1023768698.30851054.*.__utma.218586911.216721650.1605953227.1605953227.1.workflowy.com/.1600.790485120.30997905.1033697778.30851054.*.__utmb.218586911.3.10.1605953227.workflowy.com/.1600.1853000832.30851058.1033747779.30851054.*.__utmz.218586911.1605953227.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none).workflowy.com/.1600.419349926.30887766.1033772780.30851054.*.__utmt.1.workflowy.com/.1600.1997902720.30851055.295395351.30851054.*.__utmv.218586911.|1=Cohort=2020-11-20=1.workflowy.com/.1600.780485120.30997905.1025640701.30851054.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\DGYF4AAU.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\DGYF4AAU.txt	
Category:	dropped
Size (bytes):	458
Entropy (8bit):	4.7809806372565005
Encrypted:	false
SSDEEP:	12:QUU1lITQtNo9QCDo9TVTpZNtt9TVfN4iRiv+OV9TVVFjXgvH:QUUjjdPpltFRiv+oxFjI
MD5:	35D7ED32D4FEAC9AA53C7927B609D4D3
SHA1:	C6238BBB31C45438B03A015BE91887B0EB38CDE2
SHA-256:	7251523F06A09B9AB78C2B4E4966B78A353A47FDE0AE6CF961A3AEE1EFCAB142
SHA-512:	42C8E53EADAB8E2468325403B14B5CC4F138A7D2CAF56BD68A627B31D4FD13F5E2341D85E5E11E6AB4155F32831A0EF180FBC176BC382DD61BBC172F898E2F 5
Malicious:	false
Preview:	sessionid.8sg9cp8nervvwao1rn2kfg3mukuomzy2.workflowy.com/.9729.3467743360.30887590.286828980.30851054.*.__utma.218586911.216721650.160595322 7.1605953227.1605953227.1.workflowy.com/.1600.50485120.30997905.294771350.30851054.*.__utmb.218586911.0.10.1605953227.workflowy.com/.1600.11 13000832.30851058.294771350.30851054.*.__utmz.218586911.1605953227.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none).workflowy.com/.1600.3453499264.30 887766.294927350.30851054.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\DKL9R64F.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	634
Entropy (8bit):	4.7352999234564725
Encrypted:	false
SSDEEP:	12:QUU1tH4PYNo9QCDo9TVTRtNS9TVl/N4iRiv+OV9TVwFjDi349TVXL3tNtBYYy9TE:QUUbYPidxObRiv+oEFj64XZmq
MD5:	2308B34473F794F0E20E2F4248F43711
SHA1:	CEEF262CF38DE71B911FBE1F0C07C972783CCDF2
SHA-256:	98031CE0B63B5547393BFD096E057502CFFC2BA4E9DDDC62741B92A0211C1C45
SHA-512:	45AE211C8A9704DDE3E45D8738FE10F5C78C0CAF399305F14B47765DBFBEB87D405CA978C6E39E6C093E4690961A3E8B4592BAA9F79D680E1C76603E9253EC0
Malicious:	false
Preview:	sessionid.8sg9cp8nervvwao1rn2kfg3mukuomzy2.workflowy.com/.9729.4207743360.30887590.1023768698.30851054.*.__utma.218586911.216721650.16059532 27.1605953227.1605953227.1.workflowy.com/.1600.790485120.30997905.1033697778.30851054.*.__utmb.218586911.3.10.1605953227.workflowy.com/.1600 .1843000832.30851058.1025640701.30851054.*.__utmz.218586911.1605953227.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none).workflowy.com/.1600.418349926 4.30887766.1025640701.30851054.*.__utmt.1.workflowy.com/.1600.1997902720.30851055.295395351.30851054.*.__utmv.218586911.|1=Cohort=2020-11-20=1.workflo wy.com/.1600.780485120.30997905.1025640701.30851054.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\EGSLUL40.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	528
Entropy (8bit):	4.7293546463164695
Encrypted:	false
SSDEEP:	12:QUU1lITQtNo9QCDo9TVTFNg9TVE+N4iRiv+OV9TVVFjXgvG49TVXLq:QUUjjdPUgoRiv+oxFjn4Xq
MD5:	399D485E691D5A5B05B4A5E0AB2734EF
SHA1:	3D2566DB6FEE7EDFEFEAC5C999B8842B4CDF3728
SHA-256:	9BA19E43A71154FD315E9AD029D2CEB3A0CB2E56C123D7A14BA3FEB23F5A5D32
SHA-512:	391B81A443D9F34EDCD88330A219C3C0B3FEFCC4B94DF64A6A877680345D51F14ADDEE9111F6F45A1A1A7E4024C6A1BB6B1E0755EDDFBC3B9F69AA67862B8D 98
Malicious:	false
Preview:	sessionid.8sg9cp8nervvwao1rn2kfg3mukuomzy2.workflowy.com/.9729.3467743360.30887590.286828980.30851054.*.__utma.218586911.216721650.160595322 7.1605953227.1605953227.1.workflowy.com/.1600.50485120.30997905.295395351.30851054.*.__utmb.218586911.1.10.1605953227.workflowy.com/.1600.11 13000832.30851058.295395351.30851054.*.__utmz.218586911.1605953227.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none).workflowy.com/.1600.3453499264.30 887766.294927350.30851054.*.__utmt.1.workflowy.com/.1600.1997902720.30851055.295395351.30851054.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\EPZ40RY5.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	631
Entropy (8bit):	4.7384167168711855
Encrypted:	false
SSDEEP:	12:QUU1tH4PYNo9QCDo9TVatNbt9TV6VN4iRiv+OV9TVjFjBiG49TVXL3tNtBYYy9T0:QUUbYPidmte3Riv+ofFjN4XZmor
MD5:	9F5625B458369829FDAEFA715EBE5CE2
SHA1:	AAB7BE1503693E60C0D9214927FED293AD407475
SHA-256:	9C7CA1CDA2688DD2CABFA02EB6238F0EF9BCDB01236D8924E3DD794CBCDF262B

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\EPZ40RY5.txt	
SHA-512:	2A67CEB398BD681A466BDDC67F03EC6E92C6CE5DC2269927888CD0C53DA94E07BC146068452E8D3DEB57A3B1C44BA5189231CEAAADCD6290B7A945A6807B2C8
Malicious:	false
Preview:	sessionid.8sg9cp8nervvwao1rn2kfg3mukuomzy2.workflowy.com/.9729.4207743360.30887590.1023768698.30851054.*.__utma.218586911.216721650.1605953227.1605953227.1605953227.1.workflowy.com/.1600.780485120.30997905.1025328701.30851054.*.__utmb.218586911.2.10.1605953227.workflowy.com/.1600.1843000832.30851058.1025328701.30851054.*.__utmz.218586911.1605953227.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none).workflowy.com/.1600.3473499264.30887766.321286407.30851054.*.__utmt.1.workflowy.com/.1600.1997902720.30851055.295395351.30851054.*.__utmv.218586911.|1=Cohort=2020-11-20=1.workflowy.com/.1600.70485120.30997905.321311407.30851054.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\FY8C5745.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	634
Entropy (8bit):	4.740712402882477
Encrypted:	false
SSDEEP:	12:QUU1tH4PYNo9QCDo9TVXebNT9TVCVQeDN4iRiv+OV9TVRFjk49TVXL3tNtBYYy9N:QUUbYPid7ehAQe1Riv+olFjk4XZmT
MD5:	128BAAA77B9C71EA97642485B6B23C76
SHA1:	7005548796D2C6C89796EF710997B1E93DEE02DF
SHA-256:	55243C536AFFB4CCF2EB75422E54F41B08B0FE51B9D7F08B13F7C2F1C89AD746
SHA-512:	690A393BEE520A83012E2A69D366C92FDDF5ECF2C8A37286148BBD1AFD0B16A4F6BB9BB26E3D030B0AD3CFAEC8B4CA2C860C369F9770C7AE9D701CBD96351ED9
Malicious:	false
IE Cache URL:	workflowy.com/
Preview:	sessionid.8sg9cp8nervvwao1rn2kfg3mukuomzy2.workflowy.com/.9729.4207743360.30887590.1023768698.30851054.*.__utma.218586911.216721650.1605953227.1605953227.1605953227.1.workflowy.com/.1600.790485120.30997905.1033872781.30851054.*.__utmb.218586911.4.10.1605953227.workflowy.com/.1600.1853000832.30851058.1033872781.30851054.*.__utmz.218586911.1605953227.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none).workflowy.com/.1600.4193499264.30887766.1033847781.30851054.*.__utmt.1.workflowy.com/.1600.1997902720.30851055.295395351.30851054.*.__utmv.218586911.|1=Cohort=2020-11-20=1.workflowy.com/.1600.790485120.30997905.1033847781.30851054.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\LD3L2UX2.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	634
Entropy (8bit):	4.739557892074562
Encrypted:	false
SSDEEP:	12:QUU1tH4PYNo9QCDo9TVTRtNS9TVCV3N4iRiv+OV9TVwFjDi349TVXL3tNtBYYy9w:QUUbYPidxOAZRiv+oEFj64XZmq
MD5:	A91AE54D1A3E4C64F9BA2A612F2A308E
SHA1:	5D9299E4936E04DA38099FEA3DD8B598F586F934
SHA-256:	C9601A08CE7943ADFFFBC7F7E2E7444032E4505AE483C7CF2826404EC3966F49
SHA-512:	72EFF2BFCDBF8B0F6F19E4221800D01009F99C5B18742D1D9584DB4A93F5618EE22D260B2EBC0BE9B2C0F574C203C9686851D7A3828AD6BE85AFF990C484EBA0
Malicious:	false
Preview:	sessionid.8sg9cp8nervvwao1rn2kfg3mukuomzy2.workflowy.com/.9729.4207743360.30887590.1023768698.30851054.*.__utma.218586911.216721650.1605953227.1605953227.1605953227.1.workflowy.com/.1600.790485120.30997905.1033697778.30851054.*.__utmb.218586911.3.10.1605953227.workflowy.com/.1600.1853000832.30851058.1033747779.30851054.*.__utmz.218586911.1605953227.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none).workflowy.com/.1600.4183499264.30887766.1025640701.30851054.*.__utmt.1.workflowy.com/.1600.1997902720.30851055.295395351.30851054.*.__utmv.218586911.|1=Cohort=2020-11-20=1.workflowy.com/.1600.780485120.30997905.1025640701.30851054.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\MTKGX0S4.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	627
Entropy (8bit):	4.744089114542656
Encrypted:	false
SSDEEP:	12:QUU1lITQtNo9QCDo9TV8UNg9TVbN4iRiv+OV9TVjFjBw49TVXL3tNtBYYy9TV8W:QUUjjdoTRRiv+ofFju4XZmoW
MD5:	9DB788D4BE18BF47156D56428C13E9D8
SHA1:	E0016BA93DA8E26FC35656EF437FB3D62676BA82
SHA-256:	FCBE8EA2A39F13112BDCF19A02867D31863A2A98FE7380A1517A30AF45F561A8
SHA-512:	E666A8A10849287FB9916406F821F11A122326F2ED28CAA4B5BE3F35673E051274C379DF0107CF9C2DC44D6749A602C7717EF4F334B7AA24A9C19D5A3ED63FF4
Malicious:	false

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\MTKGX0S4.txt	
Preview:	sessionid.8sg9cp8nervvwao1rn2kfg3mukuomzy2.workflowy.com/.9729.3467743360.30887590.286828980.30851054.*.__utma.218586911.216721650.1605953227.1605953227.1605953227.1.workflowy.com/.1600.70485120.30997905.320836400.30851054.*.__utmb.218586911.1.10.1605953227.workflowy.com/.1600.1133000832.30851058.321036403.30851054.*.__utmz.218586911.1605953227.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none).workflowy.com/.1600.3473499264.30887766.321086404.30851054.*.__utmt.1.workflowy.com/.1600.1997902720.30851055.295395351.30851054.*.__utmv.218586911.|1=Cohort=2020-11-20=1.workflowy.com/.1600.70485120.30997905.321111404.30851054.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\RDOO2FAN.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	528
Entropy (8bit):	4.727819317988861
Encrypted:	false
SSDEEP:	12:QUU1lITQtNo9QCDo9TV8UNg9TVE+N4iRiv+OV9TVVFjXBG49TVXLq:QUUjjdoTgoRiv+oxFj44Xq
MD5:	8C22939404F5ABAF7CA8C4CAB8C4386B
SHA1:	8B6E7556285EEBDCF92BA675C9D59F83AAE491D5
SHA-256:	4A5377147A4A32945BDD6E96281DF8E21AB7FB19CA8BE406F4909EA21AB1EEAC
SHA-512:	1BD6E4B415FC23A4F8DB19CA576D105348365C399D52030942DFB9ABA44D4F136BCC41AE96CD51EDD320BC3DAF18638FE36748BA7FAFE348F5D627532C1B4AC3
Malicious:	false
Preview:	sessionid.8sg9cp8nervvwao1rn2kfg3mukuomzy2.workflowy.com/.9729.3467743360.30887590.286828980.30851054.*.__utma.218586911.216721650.1605953227.1605953227.1605953227.1.workflowy.com/.1600.70485120.30997905.320836400.30851054.*.__utmb.218586911.1.10.1605953227.workflowy.com/.1600.1113000832.30851058.295395351.30851054.*.__utmz.218586911.1605953227.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none).workflowy.com/.1600.3453499264.30887766.295551351.30851054.*.__utmt.1.workflowy.com/.1600.1997902720.30851055.295395351.30851054.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\SNDTUBR8.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	528
Entropy (8bit):	4.7401182215743
Encrypted:	false
SSDEEP:	12:QUU1lITQtNo9QCDo9TVTpZNtt9TVfN4iRiv+OV9TVVFjXgvG49TVXLq:QUUjjdPpltFRiv+oxFjn4Xq
MD5:	9F99761D95FC84CF99F35D780F9421D4
SHA1:	59CBB3DD17AD3A3F07ADCC87F15CCA95AF0510C9
SHA-256:	C2F59D683B9767762D1A20ECAED89E8C3A25500830256C52A95C86C20629517C
SHA-512:	34546FFAA0E729A2311D0BA373AAAB564B0F072DC473BDA8B559C1E30487EF4893AA0FAD9DF268187202F23FE5670E16FAAA16862BDD891AD2F806B98924717
Malicious:	false
Preview:	sessionid.8sg9cp8nervvwao1rn2kfg3mukuomzy2.workflowy.com/.9729.3467743360.30887590.286828980.30851054.*.__utma.218586911.216721650.1605953227.1605953227.1605953227.1.workflowy.com/.1600.50485120.30997905.294771350.30851054.*.__utmb.218586911.0.10.1605953227.workflowy.com/.1600.1113000832.30851058.294771350.30851054.*.__utmz.218586911.1605953227.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none).workflowy.com/.1600.3453499264.30887766.294927350.30851054.*.__utmt.1.workflowy.com/.1600.1997902720.30851055.295395351.30851054.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\TRO5Q8OE.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	528
Entropy (8bit):	4.7385079270145765
Encrypted:	false
SSDEEP:	12:QUU1lITQtNo9QCDo9TV8UNg9TVbN4iRiv+OV9TVjFjBw49TVXLq:QUUjjdoTRRiv+ofJu4Xq
MD5:	E3CB109D2CF447B0DA7848B49EFC16BE
SHA1:	E4B2D42FFE7905C934E9F0B881EFAC2FA2000351
SHA-256:	1A7FB7BF3141465FB2047F56BD4245006D036FD5595C4575206576958743CF12
SHA-512:	F2993BB58B26FD1DCF41A8E1AB9FCCB5AF112E2BC15A687505A14402B24EEBA3E99D90966336F42F5927125320BC18DDBECF1B29B74AC2A241160E527D3CE4A
Malicious:	false
Preview:	sessionid.8sg9cp8nervvwao1rn2kfg3mukuomzy2.workflowy.com/.9729.3467743360.30887590.286828980.30851054.*.__utma.218586911.216721650.1605953227.1605953227.1605953227.1.workflowy.com/.1600.70485120.30997905.320836400.30851054.*.__utmb.218586911.1.10.1605953227.workflowy.com/.1600.1133000832.30851058.321036403.30851054.*.__utmz.218586911.1605953227.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none).workflowy.com/.1600.3473499264.30887766.321086404.30851054.*.__utmt.1.workflowy.com/.1600.1997902720.30851055.295395351.30851054.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\U696PLWZ.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\U696PLWZ.txt	
Size (bytes):	634
Entropy (8bit):	4.730827156948816
Encrypted:	false
SSDEEP:	12:QUU1tH4PYNo9QCDo9TVFHNS9TVl/N4iRiv+OV9TVwFjrh49TVXL3tNtBYYy9TVKX:QUUbYPidKbRiv+oEFjrh4XZmeX
MD5:	03157595363BE270F5760559846DB0B9
SHA1:	8FF12AA2B24A19423EB690BF19979D91D6CCF873
SHA-256:	95F0F17C43AB8E12AC50097AFC3915D247E0EBFECBBDDE982CFF84A12B607FDB
SHA-512:	BE2F3252B7D107A301CAD2017FA7A3133C37F2D7077BA8F2ACE7C6B767EE7ECE5AFC434E739A3F022056AFF8C2E07DCC118B69D42341F9D800AD8F92EE00E2A4
Malicious:	false
Preview:	sessionid.8sg9cp8nervvwao1rn2kfg3mukuomzy2.workflowy.com/.9729.4207743360.30887590.1023768698.30851054.*.__utma.218586911.216721650.1605953227.1605953227.1605953227.1.workflowy.com/.1600.780485120.30997905.1025640701.30851054.*.__utmb.218586911.3.10.1605953227.workflowy.com/.1600.1843000832.30851058.1025640701.30851054.*.__utmz.218586911.1605953227.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none).workflowy.com/.1600.418349926.30887766.1025328701.30851054.*.__utmt.1.workflowy.com/.1600.1997902720.30851055.295395351.30851054.*.__utmv.218586911.|1=Cohort=2020-11-20=1.workflowy.com/.1600.780485120.30997905.1025484701.30851054.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\UE0MASFT.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	627
Entropy (8bit):	4.747880143483821
Encrypted:	false
SSDEEP:	12:QUU1lITQtNo9QCDo9TV85Nbt9TVrgN4iRiv+OV9TVjFjBv+49TVXL3tNtBYYy9TA:QUUjjdopaRiv+ofFjE4XZmoX
MD5:	DF51A5AF71DCA34D18445356E9080F23
SHA1:	65DF2EB99EFC358BBE73445CC7EBB68C05F7EAF9
SHA-256:	BD1466CD3B7BED03BE06F1485AA0C2E07E3139035991117AD21A27F6C42F3985
SHA-512:	BCC1598987758AC9464688A25D5B4B0DEA5F4F898E3532A07A3598FA0EBF3BA1FA7FC354A4B49217AA5740EB538356A43C34D678E42D6C1F3B4A547041DF673(
Malicious:	false
Preview:	sessionid.8sg9cp8nervvwao1rn2kfg3mukuomzy2.workflowy.com/.9729.3467743360.30887590.286828980.30851054.*.__utma.218586911.216721650.1605953227.1605953227.1605953227.1.workflowy.com/.1600.70485120.30997905.321236406.30851054.*.__utmb.218586911.2.10.1605953227.workflowy.com/.1600.1133000832.30851058.321236406.30851054.*.__utmz.218586911.1605953227.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none).workflowy.com/.1600.3473499264.30887766.321186405.30851054.*.__utmt.1.workflowy.com/.1600.1997902720.30851055.295395351.30851054.*.__utmv.218586911.|1=Cohort=2020-11-20=1.workflowy.com/.1600.70485120.30997905.321186405.30851054.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\UM7FU2S2.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	528
Entropy (8bit):	4.731103442534229
Encrypted:	false
SSDEEP:	12:QUU1lITQtNo9QCDo9TV8UNg9TVbN4iRiv+OV9TVVFjXBG49TVXLq:QUUjjdoTRRiv+oxFj44Xq
MD5:	313717B851C7483C696925DCF9CAE4EA
SHA1:	AB7A3D4A6829064A2DBEAD7C862B407FCCA04EB1
SHA-256:	56FD42DE07BB93F7DB4ED9861EFF1B09354B40A0D0599BA464203C0AD2686899
SHA-512:	8E4CD261DE1061EB93975B45DD811B34BE5D8BCA20BC41B492C7BB282D516ED055359EBEFA4FDC4EC52BE868D24DF6318268CD21E311461D707EFF2374F7718
Malicious:	false
Preview:	sessionid.8sg9cp8nervvwao1rn2kfg3mukuomzy2.workflowy.com/.9729.3467743360.30887590.286828980.30851054.*.__utma.218586911.216721650.1605953227.1605953227.1605953227.1.workflowy.com/.1600.70485120.30997905.320836400.30851054.*.__utmb.218586911.1.10.1605953227.workflowy.com/.1600.1133000832.30851058.321036403.30851054.*.__utmz.218586911.1605953227.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none).workflowy.com/.1600.3453499264.30887766.295551351.30851054.*.__utmt.1.workflowy.com/.1600.1997902720.30851055.295395351.30851054.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\UYOL6YWA.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	319
Entropy (8bit):	4.577939098261492
Encrypted:	false
SSDEEP:	6:+vUR2hF1VzcRhhTsdtNo9QCZJy8y8yeo9TVTPR6z6NtVJy29TVk7h:QUU1lITQtNo9QCDo9TVTpZNtt9TV4
MD5:	B3BA38AFFE9AA06102830AD316EE7ABF
SHA1:	7F42849C700F6619FC65749686A4557A540A8BB0
SHA-256:	D96319A43838EE17D7D1517747C50ADF5C5F35B15449A8372CA5F9EADD56C9F0

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\UYOL6YWA.txt	
SHA-512:	077F6615ABB98FAD5E7A86EA8E12EA73DB4D8E9503BB2CA8CEFF0620F3C6A22583857C6FE183A4A1CD3E1B3C51B885B5DB2806828D65820376D8A6C4E7F986 B
Malicious:	false
Preview:	sessionid.8sg9cp8nervvwao1rn2kfg3mukuomzy2.workflowy.com/.9729.3467743360.30887590.286828980.30851054.*.__utma.218586911.216721650.160595322 7.1605953227.1605953227.1.workflowy.com/.1600.50485120.30997905.294771350.30851054.*.__utmb.218586911.0.10.1605953227.workflowy.com/.1600.11 13000832.30851058.294771350.30851054.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\VVOXSWFO.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	104
Entropy (8bit):	4.7884555257841335
Encrypted:	false
SSDEEP:	3:RMvdWfCdLlUzqZfCXo6ESMOY1WRWgJvTdXdcdkQRR/n:+vUR2hF1VzcRhhTsdh
MD5:	AA2B6A6218DEE2DB2C3AFD221E24E3B9
SHA1:	FA2E7C85B980D6FE1CAAD7F42A1FA7669191E9D4
SHA-256:	EAD94FDD3C5D88257E435E0DAAC21CF96658BECEE8E54E38BAD79CA88BA2D1C5
SHA-512:	72677C1502A3519C1C366FEF6DE0EA63B675AD95677D40049CD773CA07FC02B321579F289B0E00084E7B2E16BC2D05CC25AC6C0FB6AFC3677DC5AFBAF6823D 6
Malicious:	false
Preview:	sessionid.8sg9cp8nervvwao1rn2kfg3mukuomzy2.workflowy.com/.9729.3467743360.30887590.286828980.30851054.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\WYBYWM6N.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	225
Entropy (8bit):	4.653568682850897
Encrypted:	false
SSDEEP:	6:+vUR2hF1VzcRhhTsdtNo9QCZJy8y8yeo9TVTPR6h:QUU1llTQtNo9QCDo9TVTpK
MD5:	A91969D1618677CD6F31E2ECA619AFFD
SHA1:	5FF6FD585E0B5C21F16A4EDB3DBF6BFA8878BE01
SHA-256:	FD4506BA292E07C1DA564EE5A596E292849FEE100463AD87D7DA01ABFB9B2561
SHA-512:	E7C2284E843831CBB2FAEA71E70041E59D829073A67E00D942B93644DCCD1E5BB53119FB3D3C29D211ABA547E5DAA02565CF5C4FD622384926D7680010D3F5C
Malicious:	false
Preview:	sessionid.8sg9cp8nervvwao1rn2kfg3mukuomzy2.workflowy.com/.9729.3467743360.30887590.286828980.30851054.*.__utma.218586911.216721650.160595322 7.1605953227.1605953227.1.workflowy.com/.1600.50485120.30997905.294771350.30851054.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\ZMM0BWVX.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	628
Entropy (8bit):	4.747481475591126
Encrypted:	false
SSDEEP:	12:QUU1tH4PYNo9QCDo9TV85Nbt9TVrgN4iRiv+OV9TVjFjBiG49TVXL3tNtBYYy9T0:QUUbYPidopaRiv+ofFjN4XZmor
MD5:	8C0F00079EA30F9C792DE0ABF90D3FDE
SHA1:	0A607BF81B01575C7B9D6479717DFFB053812EB6
SHA-256:	882C2C6616454E74D52CDBE08BCF3396BF9BDAA1982214CA27754895D7CA4B2D
SHA-512:	6DAF81D4331CAC885C1C23ACD00911E10DC38906260B9B42AFD61709FFB330680F0BADD75B08FDA9CFE51D50A6B487A98BECC3EDF51DFB5F662BED7EC18F9 A5
Malicious:	false
Preview:	sessionid.8sg9cp8nervvwao1rn2kfg3mukuomzy2.workflowy.com/.9729.4207743360.30887590.1023768698.30851054.*.__utma.218586911.216721650.16059532 27.1605953227.1605953227.1.workflowy.com/.1600.70485120.30997905.321236406.30851054.*.__utmb.218586911.2.10.1605953227.workflowy.com/.1600.1 133000832.30851058.321236406.30851054.*.__utmz.218586911.1605953227.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none).workflowy.com/.1600.3473499264.3 0887766.321286407.30851054.*.__utmt.1.workflowy.com/.1600.1997902720.30851055.295395351.30851054.*.__utmv.218586911.|1=Cohort=2020-11-20=1.workflowy.c om/.1600.70485120.30997905.321311407.30851054.*.

C:\Users\user\Desktop\~$nnec Pharma .docx	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162

C:\Users\user\Desktop\~$nnec Pharma .docx	
Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyokKOg5Gll3GwSKG/f2+1/ln:vdsCkWtW2lIlD9l
MD5:	39EB3053A717C25AF84D576F6B2EBDD2
SHA1:	F6157079187E865C1BAADCC2014EF58440D449CA
SHA-256:	CD95C0EA3CEAEC724B510D6F8F43449B26DF97822F25BDA3316F5EAC3541E54A
SHA-512:	5AA3D344F90844D83477E94E0D0E0F3C96324D8C255C643D1A67FA2BB9EEBDF4F6A7447918F371844FCEDFCD6BBAAA4868FC022FDB666E62EB2D1BAB902891C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....w.....w.....P.w.....w.....z.....w.....x...

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/CE0O2WtEHnIu62x5MHzcWwJ1PuA84Xon71y10lxllNicuO:+di6x8DT8Cm3+lA5UnwiRn41gBIZiIqX
File Content Preview:	PK.....!...wj...._.....[Content_Types].xml ...(..... ....

File Icon

Icon Hash:	e4e6a2a2a4b4b4a4

Network Behavior

Network Port Distribution

Total Packets: 61

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 21, 2020 02:07:17.350753069 CET	49168	443	192.168.2.22	54.84.56.113
Nov 21, 2020 02:07:17.350841045 CET	49167	443	192.168.2.22	54.84.56.113
Nov 21, 2020 02:07:17.453769922 CET	443	49167	54.84.56.113	192.168.2.22
Nov 21, 2020 02:07:17.453826904 CET	443	49168	54.84.56.113	192.168.2.22
Nov 21, 2020 02:07:17.453942060 CET	49167	443	192.168.2.22	54.84.56.113
Nov 21, 2020 02:07:17.453996897 CET	49168	443	192.168.2.22	54.84.56.113
Nov 21, 2020 02:07:17.474014997 CET	49167	443	192.168.2.22	54.84.56.113
Nov 21, 2020 02:07:17.476176977 CET	49168	443	192.168.2.22	54.84.56.113
Nov 21, 2020 02:07:17.576900959 CET	443	49167	54.84.56.113	192.168.2.22
Nov 21, 2020 02:07:17.578355074 CET	443	49167	54.84.56.113	192.168.2.22
Nov 21, 2020 02:07:17.578411102 CET	443	49167	54.84.56.113	192.168.2.22
Nov 21, 2020 02:07:17.578449011 CET	443	49167	54.84.56.113	192.168.2.22
Nov 21, 2020 02:07:17.578449965 CET	49167	443	192.168.2.22	54.84.56.113
Nov 21, 2020 02:07:17.578481913 CET	49167	443	192.168.2.22	54.84.56.113
Nov 21, 2020 02:07:17.578486919 CET	49167	443	192.168.2.22	54.84.56.113
Nov 21, 2020 02:07:17.578497887 CET	443	49167	54.84.56.113	192.168.2.22
Nov 21, 2020 02:07:17.578547001 CET	49167	443	192.168.2.22	54.84.56.113
Nov 21, 2020 02:07:17.578942060 CET	443	49168	54.84.56.113	192.168.2.22
Nov 21, 2020 02:07:17.580395937 CET	443	49168	54.84.56.113	192.168.2.22
Nov 21, 2020 02:07:17.580435991 CET	443	49168	54.84.56.113	192.168.2.22
Nov 21, 2020 02:07:17.580485106 CET	443	49168	54.84.56.113	192.168.2.22
Nov 21, 2020 02:07:17.580527067 CET	443	49168	54.84.56.113	192.168.2.22
Nov 21, 2020 02:07:17.580550909 CET	49168	443	192.168.2.22	54.84.56.113
Nov 21, 2020 02:07:17.580598116 CET	49168	443	192.168.2.22	54.84.56.113
Nov 21, 2020 02:07:17.580604076 CET	49168	443	192.168.2.22	54.84.56.113
Nov 21, 2020 02:07:17.585699081 CET	49167	443	192.168.2.22	54.84.56.113
Nov 21, 2020 02:07:17.592377901 CET	49168	443	192.168.2.22	54.84.56.113
Nov 21, 2020 02:07:17.688774109 CET	443	49167	54.84.56.113	192.168.2.22
Nov 21, 2020 02:07:17.688987970 CET	49167	443	192.168.2.22	54.84.56.113
Nov 21, 2020 02:07:17.695494890 CET	443	49168	54.84.56.113	192.168.2.22
Nov 21, 2020 02:07:17.695657969 CET	49168	443	192.168.2.22	54.84.56.113
Nov 21, 2020 02:07:17.902123928 CET	49167	443	192.168.2.22	54.84.56.113
Nov 21, 2020 02:07:18.045768023 CET	443	49167	54.84.56.113	192.168.2.22
Nov 21, 2020 02:07:18.046637058 CET	443	49167	54.84.56.113	192.168.2.22
Nov 21, 2020 02:07:18.046680927 CET	443	49167	54.84.56.113	192.168.2.22
Nov 21, 2020 02:07:18.046719074 CET	443	49167	54.84.56.113	192.168.2.22
Nov 21, 2020 02:07:18.046758890 CET	443	49167	54.84.56.113	192.168.2.22
Nov 21, 2020 02:07:18.046797991 CET	443	49167	54.84.56.113	192.168.2.22
Nov 21, 2020 02:07:18.046834946 CET	443	49167	54.84.56.113	192.168.2.22
Nov 21, 2020 02:07:18.046874046 CET	443	49167	54.84.56.113	192.168.2.22
Nov 21, 2020 02:07:18.046912909 CET	443	49167	54.84.56.113	192.168.2.22
Nov 21, 2020 02:07:18.046962976 CET	443	49167	54.84.56.113	192.168.2.22
Nov 21, 2020 02:07:18.047005892 CET	443	49167	54.84.56.113	192.168.2.22
Nov 21, 2020 02:07:18.051296949 CET	49167	443	192.168.2.22	54.84.56.113

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 21, 2020 02:07:18.051372051 CET	49167	443	192.168.2.22	54.84.56.113
Nov 21, 2020 02:07:18.051799059 CET	49167	443	192.168.2.22	54.84.56.113
Nov 21, 2020 02:07:18.154238939 CET	443	49167	54.84.56.113	192.168.2.22
Nov 21, 2020 02:07:18.154299021 CET	443	49167	54.84.56.113	192.168.2.22
Nov 21, 2020 02:07:18.155503035 CET	49167	443	192.168.2.22	54.84.56.113
Nov 21, 2020 02:07:18.374629021 CET	49167	443	192.168.2.22	54.84.56.113
Nov 21, 2020 02:07:18.375471115 CET	49168	443	192.168.2.22	54.84.56.113
Nov 21, 2020 02:07:18.379229069 CET	49169	443	192.168.2.22	54.84.56.113
Nov 21, 2020 02:07:18.477737904 CET	443	49167	54.84.56.113	192.168.2.22
Nov 21, 2020 02:07:18.478446960 CET	443	49167	54.84.56.113	192.168.2.22
Nov 21, 2020 02:07:18.479485035 CET	443	49168	54.84.56.113	192.168.2.22
Nov 21, 2020 02:07:18.479528904 CET	443	49168	54.84.56.113	192.168.2.22
Nov 21, 2020 02:07:18.482023954 CET	443	49169	54.84.56.113	192.168.2.22
Nov 21, 2020 02:07:18.483520985 CET	49167	443	192.168.2.22	54.84.56.113
Nov 21, 2020 02:07:18.483567953 CET	49169	443	192.168.2.22	54.84.56.113
Nov 21, 2020 02:07:18.483581066 CET	49168	443	192.168.2.22	54.84.56.113
Nov 21, 2020 02:07:18.486124039 CET	49169	443	192.168.2.22	54.84.56.113
Nov 21, 2020 02:07:18.486635923 CET	49167	443	192.168.2.22	54.84.56.113
Nov 21, 2020 02:07:18.588901997 CET	443	49169	54.84.56.113	192.168.2.22
Nov 21, 2020 02:07:18.589035034 CET	443	49169	54.84.56.113	192.168.2.22
Nov 21, 2020 02:07:18.589445114 CET	49169	443	192.168.2.22	54.84.56.113
Nov 21, 2020 02:07:18.591825008 CET	443	49167	54.84.56.113	192.168.2.22
Nov 21, 2020 02:07:18.591876984 CET	443	49167	54.84.56.113	192.168.2.22
Nov 21, 2020 02:07:18.591922045 CET	443	49167	54.84.56.113	192.168.2.22
Nov 21, 2020 02:07:18.591974020 CET	443	49167	54.84.56.113	192.168.2.22
Nov 21, 2020 02:07:18.592025042 CET	443	49167	54.84.56.113	192.168.2.22
Nov 21, 2020 02:07:18.592070103 CET	443	49167	54.84.56.113	192.168.2.22
Nov 21, 2020 02:07:18.592107058 CET	443	49167	54.84.56.113	192.168.2.22
Nov 21, 2020 02:07:18.592145920 CET	443	49167	54.84.56.113	192.168.2.22
Nov 21, 2020 02:07:18.592184067 CET	443	49167	54.84.56.113	192.168.2.22
Nov 21, 2020 02:07:18.592221975 CET	443	49167	54.84.56.113	192.168.2.22
Nov 21, 2020 02:07:18.592259884 CET	443	49167	54.84.56.113	192.168.2.22
Nov 21, 2020 02:07:18.592298031 CET	443	49167	54.84.56.113	192.168.2.22
Nov 21, 2020 02:07:18.592336893 CET	443	49167	54.84.56.113	192.168.2.22
Nov 21, 2020 02:07:18.592381001 CET	443	49167	54.84.56.113	192.168.2.22
Nov 21, 2020 02:07:18.592420101 CET	443	49167	54.84.56.113	192.168.2.22
Nov 21, 2020 02:07:18.592459917 CET	443	49167	54.84.56.113	192.168.2.22
Nov 21, 2020 02:07:18.592499018 CET	443	49167	54.84.56.113	192.168.2.22
Nov 21, 2020 02:07:18.592536926 CET	443	49167	54.84.56.113	192.168.2.22
Nov 21, 2020 02:07:18.592576027 CET	443	49167	54.84.56.113	192.168.2.22
Nov 21, 2020 02:07:18.592613935 CET	443	49167	54.84.56.113	192.168.2.22
Nov 21, 2020 02:07:18.595560074 CET	49167	443	192.168.2.22	54.84.56.113
Nov 21, 2020 02:07:18.595607996 CET	49167	443	192.168.2.22	54.84.56.113
Nov 21, 2020 02:07:18.596468925 CET	49167	443	192.168.2.22	54.84.56.113
Nov 21, 2020 02:07:18.596515894 CET	49167	443	192.168.2.22	54.84.56.113
Nov 21, 2020 02:07:18.638447046 CET	49169	443	192.168.2.22	54.84.56.113
Nov 21, 2020 02:07:18.698576927 CET	443	49167	54.84.56.113	192.168.2.22
Nov 21, 2020 02:07:18.698647022 CET	443	49167	54.84.56.113	192.168.2.22
Nov 21, 2020 02:07:18.698678970 CET	443	49167	54.84.56.113	192.168.2.22
Nov 21, 2020 02:07:18.698712111 CET	443	49167	54.84.56.113	192.168.2.22
Nov 21, 2020 02:07:18.698741913 CET	443	49167	54.84.56.113	192.168.2.22
Nov 21, 2020 02:07:18.698782921 CET	443	49167	54.84.56.113	192.168.2.22
Nov 21, 2020 02:07:18.698822021 CET	443	49167	54.84.56.113	192.168.2.22
Nov 21, 2020 02:07:18.698860884 CET	443	49167	54.84.56.113	192.168.2.22
Nov 21, 2020 02:07:18.698901892 CET	443	49167	54.84.56.113	192.168.2.22
Nov 21, 2020 02:07:18.698940992 CET	443	49167	54.84.56.113	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 21, 2020 02:07:16.439440012 CET	52197	53	192.168.2.22	8.8.8.8
Nov 21, 2020 02:07:16.476531982 CET	53	52197	8.8.8.8	192.168.2.22
Nov 21, 2020 02:07:17.307406902 CET	53099	53	192.168.2.22	8.8.8.8
Nov 21, 2020 02:07:17.345084906 CET	53	53099	8.8.8.8	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 21, 2020 02:07:18.930335045 CET	52838	53	192.168.2.22	8.8.8.8
Nov 21, 2020 02:07:18.976172924 CET	53	52838	8.8.8.8	192.168.2.22
Nov 21, 2020 02:07:19.295658112 CET	61200	53	192.168.2.22	8.8.8.8
Nov 21, 2020 02:07:19.352336884 CET	53	61200	8.8.8.8	192.168.2.22
Nov 21, 2020 02:07:20.940898895 CET	49548	53	192.168.2.22	8.8.8.8
Nov 21, 2020 02:07:20.943444967 CET	55627	53	192.168.2.22	8.8.8.8
Nov 21, 2020 02:07:20.947357893 CET	56009	53	192.168.2.22	8.8.8.8
Nov 21, 2020 02:07:20.949749947 CET	61865	53	192.168.2.22	8.8.8.8
Nov 21, 2020 02:07:20.952331066 CET	55171	53	192.168.2.22	8.8.8.8
Nov 21, 2020 02:07:20.954734087 CET	52496	53	192.168.2.22	8.8.8.8
Nov 21, 2020 02:07:20.978657961 CET	53	49548	8.8.8.8	192.168.2.22
Nov 21, 2020 02:07:20.981282949 CET	53	55627	8.8.8.8	192.168.2.22
Nov 21, 2020 02:07:20.985191107 CET	53	61865	8.8.8.8	192.168.2.22
Nov 21, 2020 02:07:20.992546082 CET	53	52496	8.8.8.8	192.168.2.22
Nov 21, 2020 02:07:20.995788097 CET	53	55171	8.8.8.8	192.168.2.22
Nov 21, 2020 02:07:20.998986006 CET	53	56009	8.8.8.8	192.168.2.22
Nov 21, 2020 02:07:21.563033104 CET	57564	53	192.168.2.22	8.8.8.8
Nov 21, 2020 02:07:21.600739956 CET	53	57564	8.8.8.8	192.168.2.22
Nov 21, 2020 02:07:21.972014904 CET	63009	53	192.168.2.22	8.8.8.8
Nov 21, 2020 02:07:22.000824928 CET	53	63009	8.8.8.8	192.168.2.22
Nov 21, 2020 02:07:22.264578104 CET	59319	53	192.168.2.22	8.8.8.8
Nov 21, 2020 02:07:22.291764021 CET	53	59319	8.8.8.8	192.168.2.22
Nov 21, 2020 02:07:47.127196074 CET	53070	53	192.168.2.22	8.8.8.8
Nov 21, 2020 02:07:47.167027950 CET	53	53070	8.8.8.8	192.168.2.22
Nov 21, 2020 02:07:48.133927107 CET	53070	53	192.168.2.22	8.8.8.8
Nov 21, 2020 02:07:48.169821024 CET	53	53070	8.8.8.8	192.168.2.22
Nov 21, 2020 02:07:49.148009062 CET	53070	53	192.168.2.22	8.8.8.8
Nov 21, 2020 02:07:49.187583923 CET	53	53070	8.8.8.8	192.168.2.22
Nov 21, 2020 02:07:51.160865068 CET	53070	53	192.168.2.22	8.8.8.8
Nov 21, 2020 02:07:51.196841955 CET	53	53070	8.8.8.8	192.168.2.22
Nov 21, 2020 02:07:51.582505941 CET	59770	53	192.168.2.22	8.8.8.8
Nov 21, 2020 02:07:51.622911930 CET	53	59770	8.8.8.8	192.168.2.22
Nov 21, 2020 02:07:52.353749990 CET	61523	53	192.168.2.22	8.8.8.8
Nov 21, 2020 02:07:52.391690969 CET	53	61523	8.8.8.8	192.168.2.22
Nov 21, 2020 02:07:53.354779005 CET	61523	53	192.168.2.22	8.8.8.8
Nov 21, 2020 02:07:53.390496016 CET	53	61523	8.8.8.8	192.168.2.22
Nov 21, 2020 02:07:54.368974924 CET	61523	53	192.168.2.22	8.8.8.8
Nov 21, 2020 02:07:54.404889107 CET	53	61523	8.8.8.8	192.168.2.22
Nov 21, 2020 02:07:55.164696932 CET	53070	53	192.168.2.22	8.8.8.8
Nov 21, 2020 02:07:55.202532053 CET	53	53070	8.8.8.8	192.168.2.22
Nov 21, 2020 02:07:56.381493092 CET	61523	53	192.168.2.22	8.8.8.8
Nov 21, 2020 02:07:56.419536114 CET	53	61523	8.8.8.8	192.168.2.22
Nov 21, 2020 02:08:00.391154051 CET	61523	53	192.168.2.22	8.8.8.8
Nov 21, 2020 02:08:00.427311897 CET	53	61523	8.8.8.8	192.168.2.22
Nov 21, 2020 02:08:26.422369957 CET	62791	53	192.168.2.22	8.8.8.8
Nov 21, 2020 02:08:26.466072083 CET	53	62791	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 21, 2020 02:07:17.307406902 CET	192.168.2.22	8.8.8.8	0x9175	Standard query (0)	workflowy.com	A (IP address)	IN (0x0001)
Nov 21, 2020 02:07:19.295658112 CET	192.168.2.22	8.8.8.8	0xd39	Standard query (0)	stats.g.doubleclick.net	A (IP address)	IN (0x0001)
Nov 21, 2020 02:07:21.563033104 CET	192.168.2.22	8.8.8.8	0xfeb6	Standard query (0)	js-agent.newrelic.com	A (IP address)	IN (0x0001)
Nov 21, 2020 02:07:21.972014904 CET	192.168.2.22	8.8.8.8	0xec14	Standard query (0)	bam-cell.nr-data.net	A (IP address)	IN (0x0001)
Nov 21, 2020 02:08:26.422369957 CET	192.168.2.22	8.8.8.8	0x7df6	Standard query (0)	workflowy.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 02:07:17.345084906 CET	8.8.8.8	192.168.2.22	0x9175	No error (0)	workflowy.com		54.84.56.113	A (IP address)	IN (0x0001)
Nov 21, 2020 02:07:17.345084906 CET	8.8.8.8	192.168.2.22	0x9175	No error (0)	workflowy.com		54.164.228.73	A (IP address)	IN (0x0001)
Nov 21, 2020 02:07:17.345084906 CET	8.8.8.8	192.168.2.22	0x9175	No error (0)	workflowy.com		107.23.99.91	A (IP address)	IN (0x0001)
Nov 21, 2020 02:07:19.352336884 CET	8.8.8.8	192.168.2.22	0xd39	No error (0)	stats.g.doubleclick.net	stats.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 02:07:19.352336884 CET	8.8.8.8	192.168.2.22	0xd39	No error (0)	stats.l.doubleclick.net		74.125.140.156	A (IP address)	IN (0x0001)
Nov 21, 2020 02:07:19.352336884 CET	8.8.8.8	192.168.2.22	0xd39	No error (0)	stats.l.doubleclick.net		74.125.140.157	A (IP address)	IN (0x0001)
Nov 21, 2020 02:07:19.352336884 CET	8.8.8.8	192.168.2.22	0xd39	No error (0)	stats.l.doubleclick.net		74.125.140.154	A (IP address)	IN (0x0001)
Nov 21, 2020 02:07:19.352336884 CET	8.8.8.8	192.168.2.22	0xd39	No error (0)	stats.l.doubleclick.net		74.125.140.155	A (IP address)	IN (0x0001)
Nov 21, 2020 02:07:21.600739956 CET	8.8.8.8	192.168.2.22	0xfeb6	No error (0)	js-agent.newrelic.com	f4.shared.global.fastly.net		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 02:07:22.000824928 CET	8.8.8.8	192.168.2.22	0xec14	No error (0)	bam-cell.nr-data.net	tls12.newrelic.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 02:08:26.466072083 CET	8.8.8.8	192.168.2.22	0x7df6	No error (0)	workflowy.com		54.164.228.73	A (IP address)	IN (0x0001)
Nov 21, 2020 02:08:26.466072083 CET	8.8.8.8	192.168.2.22	0x7df6	No error (0)	workflowy.com		54.84.56.113	A (IP address)	IN (0x0001)
Nov 21, 2020 02:08:26.466072083 CET	8.8.8.8	192.168.2.22	0x7df6	No error (0)	workflowy.com		107.23.99.91	A (IP address)	IN (0x0001)

HTTPS Packets

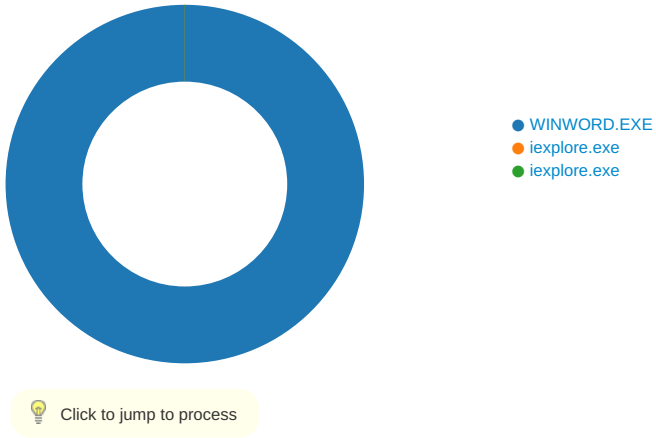
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Nov 21, 2020 02:07:17.578497887 CET	54.84.56.113	443	192.168.2.22	49167	CN=*.workflowy.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US 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	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Nov 21, 2020 02:07:17.580527067 CET	54.84.56.113	443	192.168.2.22	49168	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	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Nov 21, 2020 02:07:20.304831028 CET	74.125.140.156	443	192.168.2.22	49173	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	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Nov 21, 2020 02:07:20.305583000 CET	74.125.140.156	443	192.168.2.22	49172	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	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: WINWORD.EXE PID: 2004 Parent PID: 584

General

Start time:	02:06:34
Start date:	21/11/2020
Path:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding
Imagebase:	0x13f030000
File size:	1424032 bytes
MD5 hash:	95C38D04597050285A18F66039EDB456
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	7FEE91826B4	CreateDirectoryA
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\424A15C8.wmf	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FEE90A9AC0	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$nnec Pharma .docx	success or wait	1	7FEE90A9AC0	unknown

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\59D359E7.png	0	11108	success or wait	1	7FEE90A9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\8D1C9ABC.png	0	5572	success or wait	1	7FEE90A9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\FA9F2A23.png	0	1604	success or wait	1	7FEE90A9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\2CB71C2A.png	0	2058	success or wait	1	7FEE90A9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\AC76C38D.png	0	2528	success or wait	1	7FEE90A9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\424A15C8.wmf	unknown	914	success or wait	1	7FEE90A9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\424A15C8.wmf	unknown	8192	success or wait	1	7FEE90A9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\424A15C8.wmf	unknown	8192	end of file	1	7FEE90A9AC0	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	7FEE90BE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	7FEE90BE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	7FEE90BE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Proofing Tools\Grammar\MSGrammar\3.0\3081	success or wait	1	7FEE8FD1276	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Proofing Tools\Grammar\MSGrammar\3.0\3081\Option Set 0	success or wait	1	7FEE8FD13D9	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Proofing Tools\Grammar\MSGrammar\3.0\3081\Option Set 1	success or wait	1	7FEE8FD13D9	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F3DCB	success or wait	1	7FEE90A9AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Proofing Tools\Grammar\MSGrammar\3.0\3081	Options Version	dword	1	success or wait	1	7FEE8FD1672	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Proofing Tools\Grammar\MSGrammar\3.0\3081\Option Set 0	Name	unicode	Grammar & Style	success or wait	1	7FEE8FD14E6	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Proofing Tools\Grammar\MSGrammar\3.0\3081\Option Set 0	Data	binary	01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 00 01 01 01 02 02 02	success or wait	1	7FEE8FD870A	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Proofing Tools\Grammar\MSGrammar\3.0\3081\Option Set 1	Name	unicode	Grammar Only	success or wait	1	7FEE8FD14E6	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Proofing Tools\Grammar\MSGrammar\3.0\3081\Option Set 1	Data	binary	01 01 01 01 01 01 01 01 01 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 02 02	success or wait	1	7FEE8FD870A	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Wingdings	binary	05 00 00 00 00 00 00 00 00 00	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Tahoma	binary	02 0B 06 04 03 05 04 04 02 04	success or wait	1	7FEE90A9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
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	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F3DCB	F3DCB	binary	04 00 00 00 D4 07 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 3B DC 38 11 EE BF D6 01 CB 3D 0F 00 CB 3D 0F 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	success or wait	1	7FEE90A9AC0	unknown

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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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				

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\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1366622255	1366622256	success or wait	1	7FEE90A9AC0	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1366622256	1366622257	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F3DCB	F3DCB	binary	04 00 00 00 D4 07 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 3B DC 38 11 EE BF D6 01 CB 3D 0F 00 CB 3D 0F 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	04 00 00 00 D4 07 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 CB 3D 0F 00 CB 3D 0F 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	success or wait	1	7FEE90A9AC0	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 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 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 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 FF FF FF FF				

Analysis Process: iexplore.exe PID: 2568 Parent PID: 584

General

Start time:	02:07:04
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:	0x13fcc0000
File size:	814288 bytes
MD5 hash:	4EB098135821348270F27157F7A84E65
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: iexplore.exe PID: 2560 Parent PID: 2568

General

Start time:	02:07:04
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:2568 CREDAT:275457 /prefetch:2
Imagebase:	0x80000
File size:	815304 bytes
MD5 hash:	8A590F790A98F3D77399BE457E01386A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Disassembly