ID: 323215
Cookbook: browseurl.jbs
Time: 14:39:22
Date: 26/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

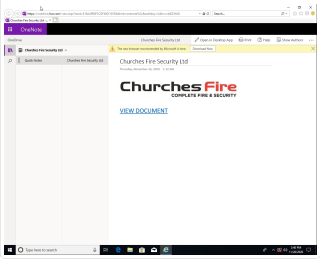
Analysis Report https://1drv.ms/o/s!BI30zfKwT4rhiAIlb7…

Overview

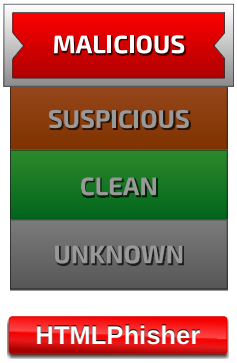
General Information

Sample URL:	http://https://1drv.ms/o/s!BI30zfKwT4rhiAIlb77-MxGeYRpS?e=94ZeN_PuoUemTbfJGTBFqw&at=9
Analysis ID:	323215

Most interesting Screenshot:



Detection

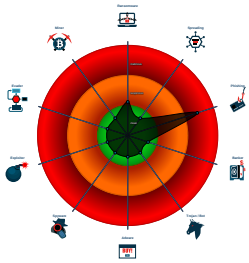


Score:	64
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Yara detected HtmlPhish_10
- Phishing site detected (based on im…
- Phishing site detected (based on log…
- HTML body contains low number of …
- HTML title does not match URL
- Submit button contains javascript call
- Suspicious form URL found

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 5908 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 1200 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5908 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 6896 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5908 CREDAT:82960 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- dllhost.exe (PID: 1240 cmdline: C:\Windows\system32\DllHost.exe /Processid:{49F171DD-B51A-40D3-9A6C-52D674CC729D} MD5: 2528137C6745C4EADD87817A1909677E)
  - explorer.exe (PID: 3388 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

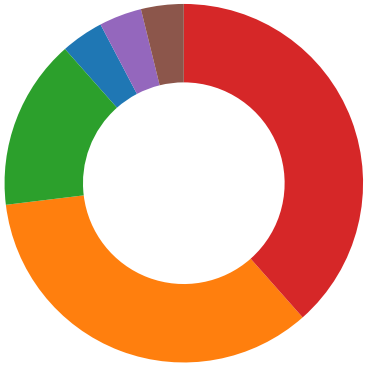
Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\ppq8mv6lfjzaqwrntj9kw0pl[1].htm	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Phishing
- Networking
- System Summary
- Malware Analysis System Evasion
- HIPS / PFW / Operating System Protection Evasion

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Phishing:

Yara detected HtmlPhish_10

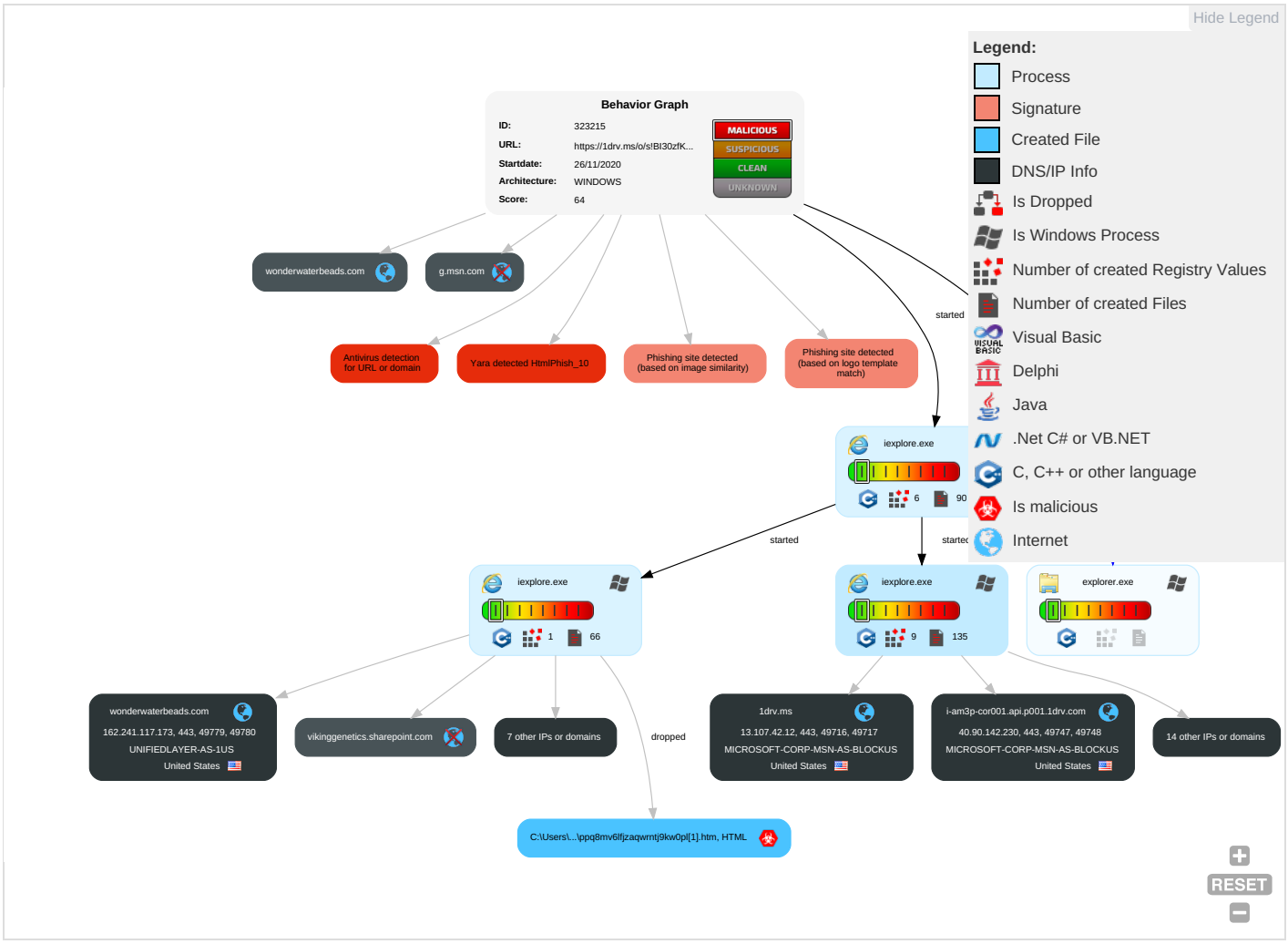
Phishing site detected (based on image similarity)

Phishing site detected (based on logo template match)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impac
Valid Accounts	Scripting 1	Path Interception	Process Injection 2	Masquerading 1	OS Credential Dumping	Security Software Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify Syster Partiti
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 2	LSASS Memory	Process 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	Device Lockc
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Scripting 1	Security Account Manager	File and Directory Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrie Billing Fraud

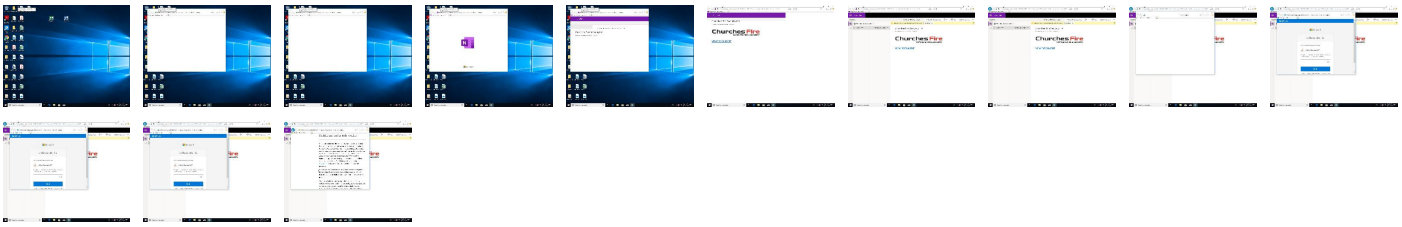
Behavior Graph

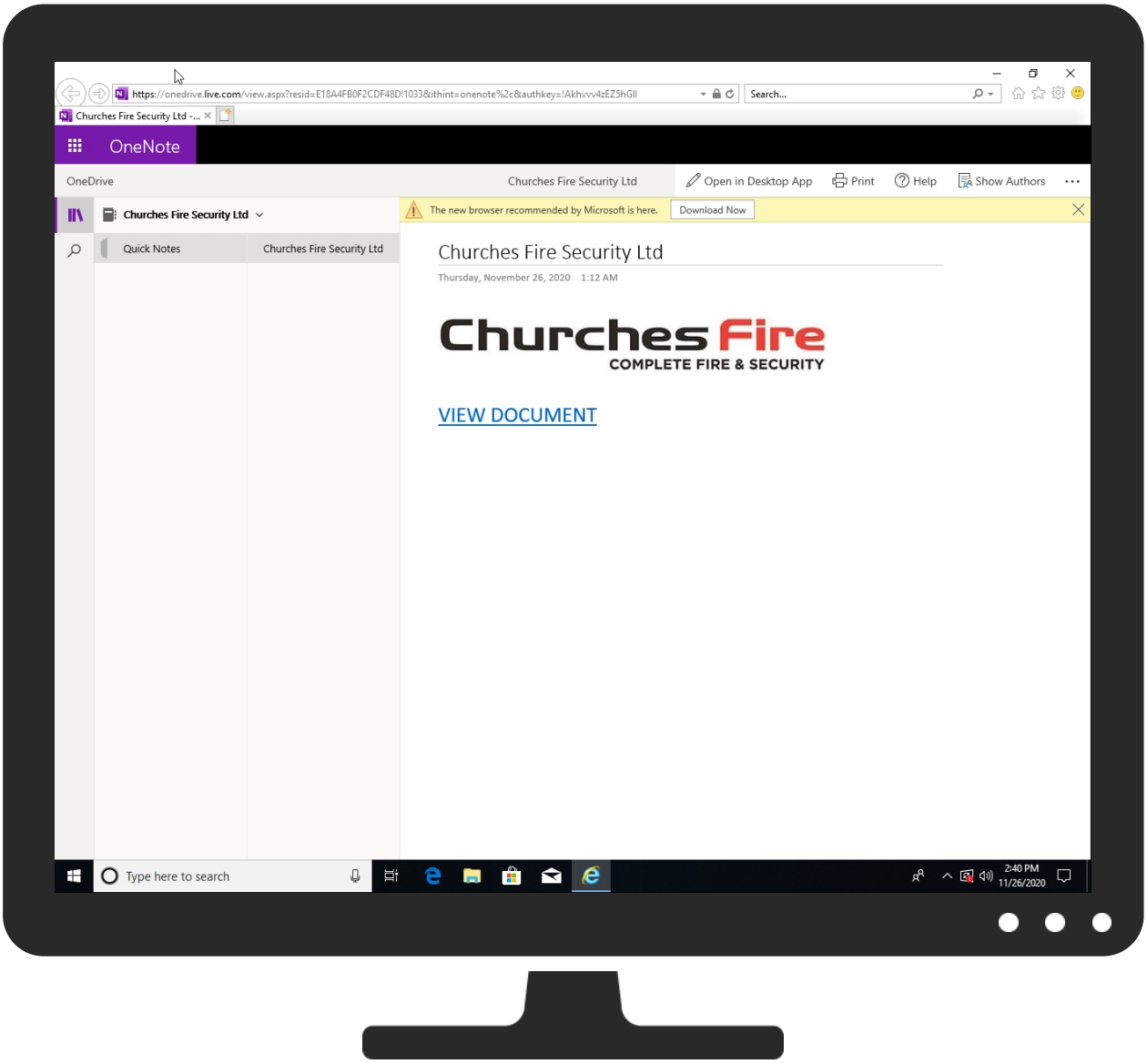


Screenshots

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
http://https://1drv.ms/o/s!BI30zfKwT4rhiAllb77-MxGeYRpS?e=94ZeN_PuoUemTbfJGTBFqw&at=9	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
wonderwaterbeads.com	5%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://wonderwaterbeads.com/Stephanie/Drive	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	

Source	Detection	Scanner	Label	Link
http://https://wonderwaterbeads.com/Stephanie/Drive	100%	UrlScan	phishing brand: sharepoint microsoft	Browse
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://https://wonderwaterbeads.com/Stephanie/Drive/	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://https://augmentation.osi.office-int.net/OfficeAugmentation/SearchWeb/	0%	URL Reputation	safe	
http://https://augmentation.osi.office-int.net/OfficeAugmentation/SearchWeb/	0%	URL Reputation	safe	
http://https://augmentation.osi.office-int.net/OfficeAugmentation/SearchWeb/	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://cgi.search.biglobe.ne.jp/favicon.ico	0%	Avira URL Cloud	safe	
http://https://cdn.onenote.net/officeaddins/images/meetings/insert_outlook_meeting_details16x16.png	0%	URL Reputation	safe	
http://https://cdn.onenote.net/officeaddins/images/meetings/insert_outlook_meeting_details16x16.png	0%	URL Reputation	safe	
http://https://cdn.onenote.net/officeaddins/images/meetings/insert_outlook_meeting_details16x16.png	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://buscar.ozu.es/	0%	Avira URL Cloud	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://fontello.comiconsRegulariconsiconsVersion	0%	URL Reputation	safe	
http://fontello.comiconsRegulariconsiconsVersion	0%	URL Reputation	safe	
http://fontello.comiconsRegulariconsiconsVersion	0%	URL Reputation	safe	
http://https://vikinggenetics-my.sharepoint.com/personal/datho_vikinggenetics_com_au/_layouts/15/images/pdf	0%	Avira URL Cloud	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://www.ozu.es/favicon.ico	0%	Avira URL Cloud	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://https://wonderwaterbeads.com/Stephanie/Drive/ppq8mv6lfjzaqwrntj9kw0pl.php?8i6	0%	Avira URL Cloud	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://search.orange.co.uk/favicon.ico	0%	URL Reputation	safe	
http://search.orange.co.uk/favicon.ico	0%	URL Reputation	safe	
http://search.orange.co.uk/favicon.ico	0%	URL Reputation	safe	
http://www.iask.com/	0%	URL Reputation	safe	
http://www.iask.com/	0%	URL Reputation	safe	
http://www.iask.com/	0%	URL Reputation	safe	
http://https://wonderwaterbeads.com/Stephanie/Drive/images/favicon.ico?rev=45co	0%	Avira URL Cloud	safe	
http://service2.bfast.com/	0%	URL Reputation	safe	
http://service2.bfast.com/	0%	URL Reputation	safe	
http://service2.bfast.com/	0%	URL Reputation	safe	
http://www.news.com.au/favicon.ico	0%	URL Reputation	safe	
http://www.news.com.au/favicon.ico	0%	URL Reputation	safe	
http://www.news.com.au/favicon.ico	0%	URL Reputation	safe	
http://www.kkbox.com.tw/	0%	URL Reputation	safe	
http://www.kkbox.com.tw/	0%	URL Reputation	safe	
http://www.kkbox.com.tw/	0%	URL Reputation	safe	
http://search.goo.ne.jp/favicon.ico	0%	URL Reputation	safe	
http://search.goo.ne.jp/favicon.ico	0%	URL Reputation	safe	
http://search.goo.ne.jp/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/	0%	URL Reputation	safe	
http://www.etmall.com.tw/	0%	URL Reputation	safe	
http://www.etmall.com.tw/	0%	URL Reputation	safe	
http://www.amazon.co.uk/	0%	URL Reputation	safe	
http://www.amazon.co.uk/	0%	URL Reputation	safe	
http://www.amazon.co.uk/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/favicon.ico	0%	URL Reputation	safe	
http://www.asharqalawsat.com/favicon.ico	0%	URL Reputation	safe	
http://www.asharqalawsat.com/favicon.ico	0%	URL Reputation	safe	
http://search.ipop.co.kr/	0%	URL Reputation	safe	
http://search.ipop.co.kr/	0%	URL Reputation	safe	
http://search.ipop.co.kr/	0%	URL Reputation	safe	
http://www.auction.co.kr/auction.ico	0%	URL Reputation	safe	
http://www.auction.co.kr/auction.ico	0%	URL Reputation	safe	
http://www.auction.co.kr/auction.ico	0%	URL Reputation	safe	
http://www.google.co.uk/	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
i-am3p-cor001.api.p001.1drv.com	40.90.142.230	true	false		high
wonderwaterbeads.com	162.241.117.173	true	false	• 5%, Virustotal, Browse	unknown
1drv.ms	13.107.42.12	true	false		high
onenoteonlinesync.onenote.com	unknown	unknown	false		high
messaging.office.com	unknown	unknown	false		high
assets.onestore.ms	unknown	unknown	false		unknown
c.live.com	unknown	unknown	false		high
ajax.aspnetcdn.com	unknown	unknown	false		high
skyapi.onedrive.live.com	unknown	unknown	false		high
static.sharepointonline.com	unknown	unknown	false		unknown
site-cdn.onenote.net	unknown	unknown	false		unknown
g.msn.com	unknown	unknown	false		high
onedrive.live.com	unknown	unknown	false		high
vikinggenetics-my.sharepoint.com	unknown	unknown	false		unknown
p.sfx.ms	unknown	unknown	false		high
spoprod-a.akamaihd.net	unknown	unknown	false		high
www.onenote.com	unknown	unknown	false		high
cdn.onenote.net	unknown	unknown	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://wonderwaterbeads.com/Stephanie/Drive	true	• 100%, UrlScan, Browse • SlashNext: Fake Login Page type: Phishing & Social Engineering	unknown
http://https://onedrive.live.com/redir?resid=E18A4FB0F2CDF48D%211033&authkey=%21Akhvvv4zEZ5hGII&page=View&wd=target%28Quick%20Notes.one%7C59b6d8c7-2f45-419a-9f35-69d9c2e82a57%2FChurches%20Fire%20Security%20Ltd%7C5c549c67-0b8d-4a98-b3ea-3ee489d9e79b%2F%29	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://search.chol.com/favicon.ico	iexplore.exe, 00000001.00000002.388042140.000001E3ECF83000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.287594950.000000E2B3000.00000002.00000001.sdmp	false		high
http://www.mercadolivre.com.br/	iexplore.exe, 00000001.00000002.388042140.000001E3ECF83000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.287594950.000000E2B3000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.merlin.com.pl/favicon.ico	iexplore.exe, 00000001.00000002.388042140.000001E3ECF83000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.287594950.000000E2B3000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.dailymail.co.uk/	iexplore.exe, 00000001.00000002.388042140.000001E3ECF83000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.287594950.000000E2B3000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000006.00000000.284825562.0000000008B40000.00000002.00000001.sdmp	false		high
http://fr.search.yahoo.com/	iexplore.exe, 00000001.00000002.388042140.000001E3ECF83000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.287594950.000000E2B3000.00000002.00000001.sdmp	false		high
http://in.search.yahoo.com/	iexplore.exe, 00000001.00000002.388042140.000001E3ECF83000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.287594950.000000E2B3000.00000002.00000001.sdmp	false		high
http://img.shopzilla.com/shopzilla/shopzilla.ico	iexplore.exe, 00000001.00000002.388042140.000001E3ECF83000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.287594950.000000E2B3000.00000002.00000001.sdmp	false		high
http://https://wonderwaterbeads.com/Stephanie/Drive/	iexplore.exe, 00000001.00000002.397292448.000001E3EF9E6000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000006.00000000.284825562.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://msk.afisha.ru/	iexplore.exe, 00000001.00000002.388042140.000001E3ECF83000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.287594950.000000E2B3000.00000002.00000001.sdmp	false		high
http://www.reddit.com/	msapplication.xml4.1.dr	false		high
http://busca.igbusca.com.br//app/static/images/favicon.ico	iexplore.exe, 00000001.00000002.388042140.000001E3ECF83000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.287594950.000000E2B3000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.ya.com/favicon.ico	iexplore.exe, 00000001.00000002.388042140.000001E3ECF83000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.287594950.00000000E2B3000.00000002.00000001.sdmp	false		high
http://www.etmall.com.tw/favicon.ico	iexplore.exe, 00000001.00000002.388042140.000001E3ECF83000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.287594950.00000000E2B3000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com/favicon.icooft	iexplore.exe, 00000001.00000002.396948137.000001E3EF87D000.00000004.00000001.sdmp	false		high
http://https://augmentation.osi.office-int.net/OfficeAugmentation/SearchWeb/	OneNote.box4.dll1[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://it.search.dada.net/favicon.ico	iexplore.exe, 00000001.00000002.388042140.000001E3ECF83000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.287594950.00000000E2B3000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.hanafos.com/favicon.ico	iexplore.exe, 00000001.00000002.388042140.000001E3ECF83000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.287594950.00000000E2B3000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cgi.search.biglobe.ne.jp/favicon.ico	iexplore.exe, 00000001.00000002.388042140.000001E3ECF83000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.287594950.00000000E2B3000.00000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://spoprod-a.akamaihd.net/files/odsp-next-prod_2018-11-02-sts_20181108.001/require-a19851d1.js	ppq8mv6lfjzaqwrntj9kw0pl[1].htm.15.dr	false		high
http://https://cdn.onenote.net/officeaddins/images/meetings/insert_outlook_meeting_details16x16.png	Meetings_manifest[1].xml.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.msn.co.jp/results.aspx?q=	explorer.exe, 00000006.00000000.287594950.000000000E2B3000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://buscar.ozu.es/	iexplore.exe, 00000001.00000002.388042140.000001E3ECF83000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.287594950.00000000E2B3000.00000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.microsofttranslator.com/BVPrev.aspx?ref=IE8Activity	iexplore.exe, 00000001.00000002.388042140.000001E3ECF83000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.287594950.00000000E2B3000.00000002.00000001.sdmp	false		high
http://www.ask.com/	iexplore.exe, 00000001.00000002.388042140.000001E3ECF83000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.287594950.00000000E2B3000.00000002.00000001.sdmp	false		high
http://www.google.it/	iexplore.exe, 00000001.00000002.388042140.000001E3ECF83000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.287594950.00000000E2B3000.00000002.00000001.sdmp	false		high
http://search.auction.co.kr/	iexplore.exe, 00000001.00000002.388042140.000001E3ECF83000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.287594950.00000000E2B3000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.amazon.de/	iexplore.exe, 00000001.00000002.388042140.000001E3ECF83000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.287594950.00000000E2B3000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://fontello.comiconsRegulariconsiconsVersion	icons[1].eot.15.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://sads.myspace.com/	iexplore.exe, 00000001.00000002.388042140.000001E3ECF83000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.287594950.00000000E2B3000.00000002.00000001.sdmp	false		high
http://https://vikinggenetics-my.sharepoint.com/personal/datho_vikinggenetics_com_au/_layouts/15/images/pdf	ppq8mv6lfjzaqwrntj9kw0pl[1].htm.15.dr	false	• Avira URL Cloud: safe	unknown
http://www.pchome.com.tw/favicon.ico	iexplore.exe, 00000001.00000002.388042140.000001E3ECF83000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.287594950.00000000E2B3000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://browse.guardian.co.uk/favicon.ico	iexplore.exe, 00000001.00000002.388042140.000001E3ECF83000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.287594950.00000000E2B3000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://google.pchome.com.tw/	iexplore.exe, 00000001.00000002.388042140.000001E3ECF83000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.287594950.00000000E2B3000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://list.taobao.com/browse/search_visual.htm?n=15&q=	iexplore.exe, 00000001.00000002.388042140.000001E3ECF83000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.287594950.00000000E2B3000.00000002.00000001.sdmp	false		high
http://www.rambler.ru/favicon.ico	iexplore.exe, 00000001.00000002.388042140.000001E3ECF83000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.287594950.00000000E2B3000.00000002.00000001.sdmp	false		high
http://uk.search.yahoo.com/	iexplore.exe, 00000001.00000002.388042140.000001E3ECF83000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.287594950.00000000E2B3000.00000002.00000001.sdmp	false		high
http://www.ozu.es/favicon.ico	iexplore.exe, 00000001.00000002.388042140.000001E3ECF83000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.287594950.00000000E2B3000.00000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.sify.com/	iexplore.exe, 00000001.00000002.388042140.000001E3ECF83000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.287594950.00000000E2B3000.00000002.00000001.sdmp	false		high
http://openimage.interpark.com/interpark.ico	iexplore.exe, 00000001.00000002.388042140.000001E3ECF83000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.287594950.00000000E2B3000.00000002.00000001.sdmp	false		high
http://search.yahoo.co.jp/favicon.ico	iexplore.exe, 00000001.00000002.388042140.000001E3ECF83000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.287594950.00000000E2B3000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://wonderwaterbeads.com/Stephanie/Drive/ppq8mv6lfjzaqwrntj9kw0pl.php?8i6	iexplore.exe, 00000001.00000002.398510874.000001E3F0A84000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.gmarket.co.kr/	iexplore.exe, 00000001.00000002.388042140.000001E3ECF83000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.287594950.00000000E2B3000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

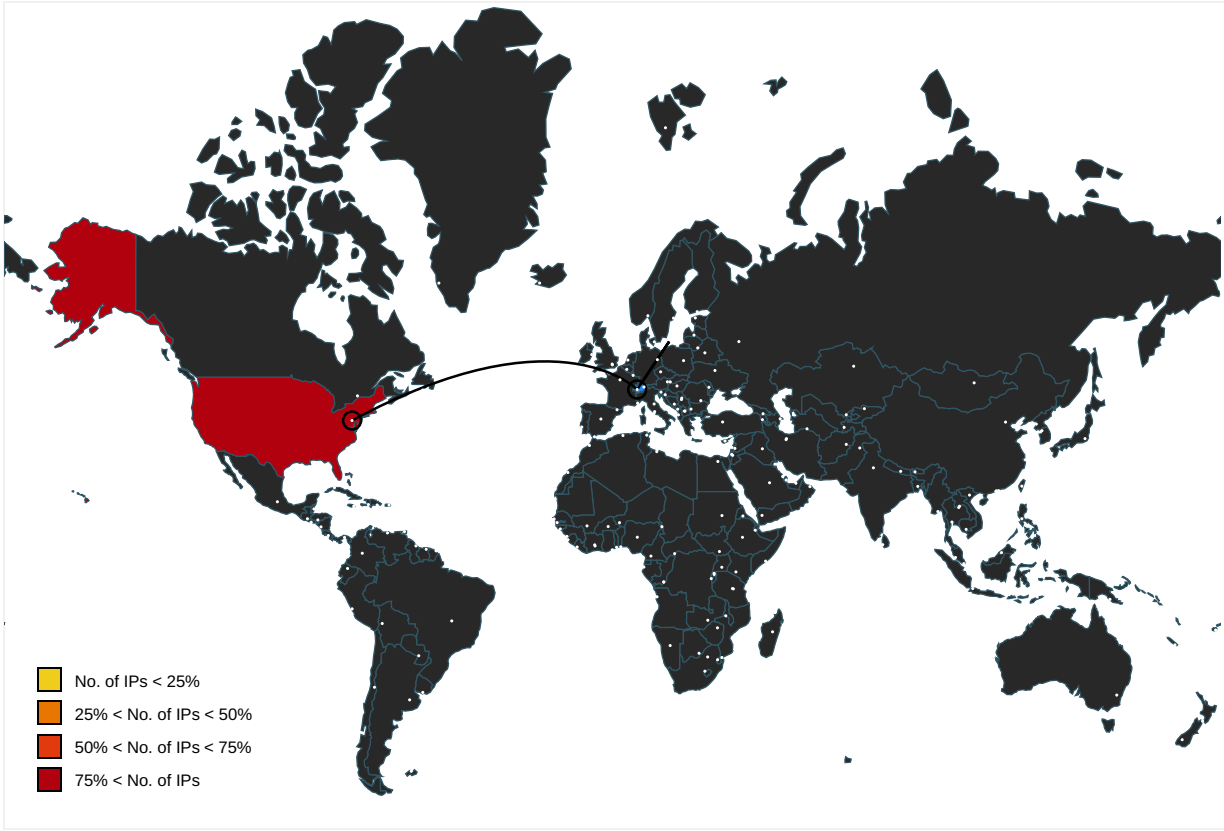
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000006.00000000.284825562.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.nifty.com/	iexplore.exe, 00000001.00000002.388042140.000001E3ECF83000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.287594950.000000000E2B3000.00000002.00000001.sdmp	false		high
http://www.google.si/	iexplore.exe, 00000001.00000002.388042140.000001E3ECF83000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.287594950.000000000E2B3000.00000002.00000001.sdmp	false		high
http://https://onedrive.live.com/re	iexplore.exe, 00000001.00000002.398510874.000001E3F0A84000.00000004.00000001.sdmp	false		high
http://www.soso.com/	iexplore.exe, 00000001.00000002.388042140.000001E3ECF83000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.287594950.000000000E2B3000.00000002.00000001.sdmp	false		high
http://https://onedrive.live.com/redir?resid=E18A4FB0F2CDF48D%211033&authkey=%21Akhvvv4zEZ5hGII&page=View&w	{580E898A-3038-11EB-90E4-ECF4BB862DED}.dat.1.dr	false		high
http://https://ajax.aspnetcdn.com/ajax/jQuery/jquery-2.1.3.min.js	learningtools[1].htm.2.dr	false		high
http://busca.orange.es/	iexplore.exe, 00000001.00000002.388042140.000001E3ECF83000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.287594950.000000000E2B3000.00000002.00000001.sdmp	false		high
http://cnweb.search.live.com/results.aspx?q=	iexplore.exe, 00000001.00000002.388042140.000001E3ECF83000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.287594950.000000000E2B3000.00000002.00000001.sdmp	false		high
http://www.twitter.com/	iexplore.exe, 00000001.00000002.397031842.000001E3EF915000.00000004.00000001.sdmp	false		high
http://auto.search.msn.com/response.asp?MT=	iexplore.exe, 00000001.00000002.387365747.000001E3ECE90000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.286432182.000000000E1C0000.00000002.00000001.sdmp	false		high
http://www.target.com/	iexplore.exe, 00000001.00000002.388042140.000001E3ECF83000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.287594950.000000000E2B3000.00000002.00000001.sdmp	false		high
http://search.orange.co.uk/favicon.ico	iexplore.exe, 00000001.00000002.388042140.000001E3ECF83000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.287594950.000000000E2B3000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.iask.com/	iexplore.exe, 00000001.00000002.388042140.000001E3ECF83000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.287594950.000000000E2B3000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://wonderwaterbeads.com/Stephanie/Drive/images/favicon.ico?rev=45co	iexplore.exe, 00000001.00000002.397052047.000001E3EF92F000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://search.centrum.cz/favicon.ico	iexplore.exe, 00000001.00000002.388042140.000001E3ECF83000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.287594950.000000000E2B3000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://service2.bfast.com/	iexplore.exe, 00000001.00000002.388042140.000001E3ECF83000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.287594950.00000000E2B3000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ariadna.elmundo.es/	iexplore.exe, 00000001.00000002.388042140.000001E3ECF83000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.287594950.00000000E2B3000.00000002.00000001.sdmp	false		high
http://www.news.com.au/favicon.ico	iexplore.exe, 00000001.00000002.388042140.000001E3ECF83000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.287594950.00000000E2B3000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.cdiscount.com/	iexplore.exe, 00000001.00000002.388042140.000001E3ECF83000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.287594950.00000000E2B3000.00000002.00000001.sdmp	false		high
http://www.tiscali.it/favicon.ico	iexplore.exe, 00000001.00000002.388042140.000001E3ECF83000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.287594950.00000000E2B3000.00000002.00000001.sdmp	false		high
http://it.search.yahoo.com/	iexplore.exe, 00000001.00000002.388042140.000001E3ECF83000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.287594950.00000000E2B3000.00000002.00000001.sdmp	false		high
http://www.ceneo.pl/favicon.ico	iexplore.exe, 00000001.00000002.388042140.000001E3ECF83000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.287594950.00000000E2B3000.00000002.00000001.sdmp	false		high
http://www.servicios.clarin.com/	iexplore.exe, 00000001.00000002.388042140.000001E3ECF83000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.287594950.00000000E2B3000.00000002.00000001.sdmp	false		high
http://search.daum.net/favicon.ico	iexplore.exe, 00000001.00000002.388042140.000001E3ECF83000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.287594950.00000000E2B3000.00000002.00000001.sdmp	false		high
http://www.kkbox.com.tw/	iexplore.exe, 00000001.00000002.388042140.000001E3ECF83000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.287594950.00000000E2B3000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.goo.ne.jp/favicon.ico	iexplore.exe, 00000001.00000002.388042140.000001E3ECF83000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.287594950.00000000E2B3000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.msn.com/results.aspx?q=	explorer.exe, 00000006.00000000.287594950.000000000E2B3000.00000002.00000001.sdmp	false		high
http://list.taobao.com/	iexplore.exe, 00000001.00000002.388042140.000001E3ECF83000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.287594950.00000000E2B3000.00000002.00000001.sdmp	false		high
http://www.nytimes.com/	iexplore.exe, 00000001.00000002.397031842.000001E3EF915000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.taobao.com/favicon.ico	iexplore.exe, 00000001.00000002.388042140.000001E3ECF83000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.287594950.000000000E2B3000.00000002.00000001.sdmp	false		high
http://www.etmall.com.tw/	iexplore.exe, 00000001.00000002.388042140.000001E3ECF83000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.287594950.000000000E2B3000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ie.search.yahoo.com/os?command=	iexplore.exe, 00000001.00000002.388042140.000001E3ECF83000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.287594950.000000000E2B3000.00000002.00000001.sdmp	false		high
http://www.cnet.com/favicon.ico	iexplore.exe, 00000001.00000002.388042140.000001E3ECF83000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.287594950.000000000E2B3000.00000002.00000001.sdmp	false		high
http://www.linternaute.com/favicon.ico	iexplore.exe, 00000001.00000002.388042140.000001E3ECF83000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.287594950.000000000E2B3000.00000002.00000001.sdmp	false		high
http://www.amazon.co.uk/	iexplore.exe, 00000001.00000002.388042140.000001E3ECF83000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.287594950.000000000E2B3000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.cdiscount.com/favicon.ico	iexplore.exe, 00000001.00000002.388042140.000001E3ECF83000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.287594950.000000000E2B3000.00000002.00000001.sdmp	false		high
http://www.asharqalawsat.com/favicon.ico	iexplore.exe, 00000001.00000002.388042140.000001E3ECF83000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.287594950.000000000E2B3000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.google.fr/	iexplore.exe, 00000001.00000002.388042140.000001E3ECF83000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.287594950.000000000E2B3000.00000002.00000001.sdmp	false		high
http://search.gismeteo.ru/	iexplore.exe, 00000001.00000002.388042140.000001E3ECF83000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.287594950.000000000E2B3000.00000002.00000001.sdmp	false		high
http://www.rtl.de/	iexplore.exe, 00000001.00000002.388042140.000001E3ECF83000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.287594950.000000000E2B3000.00000002.00000001.sdmp	false		high
http://www.soso.com/favicon.ico	iexplore.exe, 00000001.00000002.388042140.000001E3ECF83000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.287594950.000000000E2B3000.00000002.00000001.sdmp	false		high
http://www.univision.com/favicon.ico	iexplore.exe, 00000001.00000002.388042140.000001E3ECF83000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.287594950.000000000E2B3000.00000002.00000001.sdmp	false		high
http://search.ipop.co.kr/	iexplore.exe, 00000001.00000002.388042140.000001E3ECF83000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.287594950.000000000E2B3000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.auction.co.kr/auction.ico	iexplore.exe, 00000001.00000002.388042140.000001E3ECF83000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.287594950.00000000E2B3000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.orange.fr/	iexplore.exe, 00000001.00000002.388042140.000001E3ECF83000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.287594950.00000000E2B3000.00000002.00000001.sdmp	false		high
http://video.globo.com/favicon.ico	iexplore.exe, 00000001.00000002.388042140.000001E3ECF83000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.287594950.00000000E2B3000.00000002.00000001.sdmp	false		high
http://www.google.co.uk/	iexplore.exe, 00000001.00000002.388042140.000001E3ECF83000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.287594950.00000000E2B3000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	explorer.exe, 00000006.00000000.284825562.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://uci.officeapps.live-int.com/OfficeInsights/Agave/Web/	OneNote.box4.dll1[1].js.2.dr	false		high
http://https://skyapi.onedrive.live.com/api/proxy?v=3	iexplore.exe, 00000001.00000002.396948137.000001E3EF87D000.00000004.00000001.sdmp, {580E898A-3038-11EB-90E4-ECF4BB862DED}.dat.1.dr	false		high
http://https://wonderwaterbeads.com/favicon.ico	iexplore.exe, 00000001.00000002.397131669.000001E3EF98A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://buscador.terra.com/favicon.ico	iexplore.exe, 00000001.00000002.388042140.000001E3ECF83000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.287594950.00000000E2B3000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search1.taobao.com/	iexplore.exe, 00000001.00000002.388042140.000001E3ECF83000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.287594950.00000000E2B3000.00000002.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
162.241.117.173	unknown	United States		46606	UNIFIEDLAYER-AS-1US	false
40.90.142.230	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
13.107.42.12	unknown	United States		8068	MICROSOFT-CORP-MSN-AS-BLOCKUS	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	323215
Start date:	26.11.2020
Start time:	14:39:22
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 24s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://1drv.ms/o/s!BI30zfKwT4rhiAIlb77-MxGeYRpS?e=94ZeN_PuoUemTbfJGTBFqw&at=9
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	20
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL

Classification:	mal64.phis.win@6/149@21/3
EGA Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browsing link: https://wonderw aterbeads.com/Stephanie/Drive • Browsing link: https://go.microsoft.com/fwlink/?linkid=845480
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, dllhost.exe, BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, SgrmBroker.exe, svchost.exe • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • Excluded IPs from analysis (whitelisted): 184.24.15.126, 13.107.42.13, 104.43.139.144, 92.122.213.248, 92.122.213.216, 13.95.147.73, 13.107.6.171, 23.210.249.64, 52.109.88.52, 52.109.88.177, 23.210.248.85, 52.147.198.201, 52.109.124.71, 104.103.81.75, 52.142.114.2, 40.77.18.167, 204.79.197.200, 13.107.21.200, 152.199.19.160, 52.109.76.2, 184.24.28.12, 184.24.31.229, 104.43.193.48, 51.104.139.180, 152.199.19.161, 40.67.251.132, 184.24.28.208, 13.107.136.9, 92.122.145.53, 92.122.213.194, 92.122.213.240, 23.210.249.93, 184.24.14.70, 92.122.213.247, 20.54.26.129, 52.142.114.176 • Excluded domains from analysis (whitelisted): odwebp.trafficmanager.net, assets.onestore.ms.edgekey.net, osiprod-sea-patriarch-000.cloudapp.net, c1-wildcard.cdn.office.net-c.edgekey.net.globalredir.akadns.net, i.s-microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, wns.notify.windows.com.akadns.net, cdn.onenote.net.edgekey.net, a1945.g2.akamai.net, db5p.wns.notify.windows.com.akadns.net, prod-eu.reverseproxy-onenote.com.akadns.net, prod.omexmessaging.live.com.akadns.net, statics-marketingsites-eus-ms-com.akamaized.net, omexmessaging.osi.office.net, prod-eur.onenoteonlinesync-onenote.com.akadns.net, dual-a-0001.a-msedge.net, westeurope1-odwebp.cloudapp.net, ris-prod.trafficmanager.net, e19254.dscg.akamaiedge.net, site-cdn.onenote.net.edgekey.net, assets.onestore.ms.akadns.net, skypedataprdcolcus15.cloudapp.net, c-s.cms.ms.akadns.net, ris.api.iris.microsoft.com, c.bing.com, a1531.g2.akamai.net, e1553.dspg.akamaiedge.net, spoprod-a.akamaihd.net.edgesuite.net, c.s-microsoft.com-c.edgekey.net, europe.configsvc1.live.com.akadns.net, cs9.wpc.v0cdn.net, spo-0004.spo-msedge.net, appsforoffice.microsoft.com, odc-web-brs.onedrive.akadns.net, c-bing-com.a-0001.a-msedge.net, i.s-microsoft.com, iecvlist.microsoft.com, e5684.g.akamaiedge.net, par02p.wns.notify.windows.com.akadns.net, odwebpl.trafficmanager.net.l-0004.dc-msedge.net.l-0004.l-msedge.net, go.microsoft.com, prod.fs.microsoft.com.akadns.net, onenote.officeapps.live.com, odc-web-geo.onedrive.akadns.net, cs22.wpc.v0cdn.net, ie9comview.vo.msecnd.net, c1-wildcard.cdn.office.net-c.edgekey.net, prod.reverseproxy-onenote.com.akadns.net, skypedataprdcoleus16.cloudapp.net, common-geo.onedrive.trafficmanager.net, browser.events.data.microsoft.com, c.s-microsoft.com, config.officeapps.live.com, go.microsoft.com.edgekey.net, prod.onenoteonlinesync-onenote.com.akadns.net, e13678.dspb.akamaiedge.net, 17825-ipv4.farm.prod.aa-rt.sharepoint.com.spo-0004.spo-msedge.net, e2682.g.akamaiedge.net, arc.msn.com.nsatc.net, browser.events.data.trafficmanager.net, appsforoffice.microsoft.com.edgekey.net, e11290.dspg.akamaiedge.net, b-0016.b-msedge.net, www.microsoft.com-c-3.edgekey.net,

sea-000.omexmessaging.osi.office.net, officeclient.microsoft.com, watson.telemetry.microsoft.com, e10583.dspg.akamaiedge.net, fs.microsoft.com, onenote.wac.trafficmanager.net.b-0016.b-msedge.net, 17825-ipv4e.farm.prod.sharepointonline.com.akadns.net, skypedataprdcolcus16.cloudapp.net, skypedataprdcolcus13.cloudapp.net, blobcollector.events.data.trafficmanager.net, c1-officeapps-15.cdn.office.net, e1780.dspg.akamaiedge.net, privacy.microsoft.com.edgekey.net, browser.pipe.aria.microsoft.com, c-msn-com-nsatc.trafficmanager.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, g-msn-com-nsatc.trafficmanager.net, www.microsoft.com-c-3.edgekey.net.globalredir.akadns.net, l-0004.l-msedge.net, c1-onenote-15.cdn.office.net, mscomajax.vo.msecnd.net, emea1.notify.windows.com.akadns.net, img-prod-cms-rt-microsoft-com.akamaized.net, static.sharepointonline.com-c.edgekey.net, client.wns.windows.com, prod.configsvc1.live.com.akadns.net, e1723.g.akamaiedge.net, prod-weu.onenoteonlinesync-onenote.com.akadns.net, c-msn-com-europe-vip.trafficmanager.net, privacy.microsoft.com, e13678.dscg.akamaiedge.net, www.microsoft.com

- Report size getting too big, too many NtCreateFile calls found.
- Report size getting too big, too many NtDeviceIoControlFile calls found.
- Report size getting too big, too many NtReadVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
14:40:35	API Interceptor	1x Sleep call for process: dllhost.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\4KT237GC\wonderwaterbeads[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	13
Entropy (8bit):	2.469670487371862
Encrypted:	false
SSDEEP:	3:D90aKb:JFKb
MD5:	C1DDEA3EF6BBEF3E7060A1A9AD89E4C5
SHA1:	35E3224FCBD3E1AF306F2B6A2C6BBEA9B0867966
SHA-256:	B71E4D17274636B97179BA2D97C742735B6510EB54F22893D3A2DAFF2CEB28DB
SHA-512:	6BE8CEC7C862AFAE5B37AA32DC5BB45912881A3276606DA41BF808A4EF92C318B355E616BF45A257B995520D72B7C08752C0BE445DCEADE5CF79F73480910FE D
Malicious:	false
Reputation:	low
Preview:	<root></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\QY0TBVVD\onedrive.live[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	13
Entropy (8bit):	2.469670487371862
Encrypted:	false
SSDEEP:	3:D90aKb:JFKb
MD5:	C1DDEA3EF6BBEF3E7060A1A9AD89E4C5
SHA1:	35E3224FCBD3E1AF306F2B6A2C6BBEA9B0867966
SHA-256:	B71E4D17274636B97179BA2D97C742735B6510EB54F22893D3A2DAFF2CEB28DB
SHA-512:	6BE8CEC7C862AFAE5B37AA32DC5BB45912881A3276606DA41BF808A4EF92C318B355E616BF45A257B995520D72B7C08752C0BE445DCEADE5CF79F73480910FE D
Malicious:	false
Reputation:	low
Preview:	<root></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\SW9F13GA\onenote.officeapps.live[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	modified
Size (bytes):	86739
Entropy (8bit):	4.956884711630281
Encrypted:	false
SSDEEP:	768:hQSOB58B5OAZ/O3QSOB58B5OAZ/ObQSOB58B5OAZ/O3QSOB58B5OAZ/OqQSOB58d:+
MD5:	49A0201C3A1AFE911444028B136425BA
SHA1:	084A10C887A83E25BEA0FDCE07512B5227E10346
SHA-256:	2ADE5AACED751781A28A3601B0209756982BE6D9770BA42FCA82ABB0295A1B3E
SHA-512:	40FFABA2254CB24145897685628A1E5A90B319F2CB655E1B0030AD6EBF612C2BA426D563F3896CE58EEC9F37EC80C6DA61E2AB71302DB73B776E22259C2A4B6 B
Malicious:	false
Reputation:	low
Preview:	<root></root><root><item name="obf-CampaignDefinitions" value="[{"CampaignId":"281ff77f-ec20-4b5b-88dc-674ede3473ee","StartTimeUtc":"2018-09-04T00:00:00Z","EndTimeUtc":"2025-01-01T00:00:00Z","GovernedChannelType":0,"AdditionalDataRequested":["EmailAddress"],"NominationScheme":{"Type":0,"PercentageNumerator":25,"PercentageDenominator":100,"NominationPeriod":{"Type":0,"IntervalSeconds":1296000},"CooldownPeriod":{"Type":0,"IntervalSeconds":7776000},"FallbackSurveyDurationSeconds":120},"SurveyTemplate":{"Type":4,"ActivationEvent":{"Type":1,"Sequence":[{"Type":0,"Activity":"AppUsageNPS","IsAggregate":true,"Count":300},{"Type":0,"Activity":"AppUsageTimeSatisfiedNPS",&

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\ZQBPW6AA\www.onenote[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\ZQBPW6AA\www.onenote[1].xml	
Size (bytes):	139
Entropy (8bit):	4.9233256744639515
Encrypted:	false
SSDEEP:	3:D90aK1ryRtFwsOHQYMALfVAqbRH2T7HD4MI9cTTyE9qSSXU1FKb:JFK1rUFKlMufVAqdWHMdElSXSkb
MD5:	8F2B9E146D549428EA5546EEB2C9CC51
SHA1:	56ED4725E0EEDADF25655A5D25C48A24843790EB
SHA-256:	50A3D1E6F7DEA7790A3889818859C6DE4681C6B86F790C34D0CB9F986CE7B9CA
SHA-512:	8C1114FC887DE8EF93A104A0CA4F5A4C391ABD515F87A24899E3785F805B4A549797CF1A4F6CE123F97266946D8BF6540A4E511BAF4D15F786DC6F4E775B7E4E
Malicious:	false
Reputation:	low
Preview:	<root></root><root><item name="Office API client" value="fb527b60-671d-a240-91c1-ee2d1ad587bc" ltime="661664160" htime="30852165" /></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{580E8988-3038-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	51400
Entropy (8bit):	2.0693839966111747
Encrypted:	false
SSDEEP:	192:rOZFZy2/9WAt9fORMbjnfTsrgThWWmnh+g:rarx/UE1PbjfCgEWmh5
MD5:	3ACB01FEB8AF0A5DBB58D136DCC3274D
SHA1:	DF0CFA1DFC5B6818D08C0F1B8CC53F60180E7745
SHA-256:	632C9334C05BF8D777B01791A52F3FF363FDA1F5A0F97F93A2DD0A5D6349FA2C
SHA-512:	CE922BB183E33475FFFEAF506FC787266B1B9678930895FF0087B506CF984B4C9D2499601D625E21223670872DCA9ABE05EC2067F6EDB6ABDD70EB91AF0E3FD
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\{580E898A-3038-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	64268
Entropy (8bit):	2.9364904261344744
Encrypted:	false
SSDEEP:	1536:O6fC3kBiXfB6/EakfoyaJEak/oyKEak/oys:O6fC3kBiXfB6/KfoyaJK/oyKK/oys
MD5:	3CABD82E1B841A97AE7D1AF3AF5FDA48
SHA1:	969C24095A6373EA005D2963F0F9016112F344C0
SHA-256:	3B28AA450A128EF09494FEC298E5E31C638FBB88B233A95480F5096D1C7BD86F
SHA-512:	A943E297BB5C0A1031E527A7788D037E71ECCF8C58B967E904868769A817B0F08B93C4FA9DC8376D64561955E8D9EB9345E599C5EBA3DC6E5FE27D9CB66EE84 9
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\{62AFCF24-3038-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.563386536196635
Encrypted:	false
SSDEEP:	48:IwFf7GcprEGwpasG4pQxhGrapbSIrGQpKqG7HpRGsTGIpG:rZhZ8Qs6xxBSIFAFTG4A
MD5:	7F2DD882D5E6BF6093B7665B0FB886FC
SHA1:	AF402D71E7AAC1DC7EB3E8E264F5BAE672286D5C
SHA-256:	8740EBCFCBB98DDC132BA730E01981150D83291961F8C8D748FCAB2357C69C93
SHA-512:	756E56DFD0B3B8FA2A9210006E05867B0446111E1A380730CD8D2263A59C3CC5C0EBE71605E6A679EA31A87E7B647142EBE8FF804C6389895BAFEC3419BEE76
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{62AFCF24-3038-11EB-90E4-ECF4BB862DED}.dat	
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{72DBDD28-3038-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	44580
Entropy (8bit):	2.501068148129436
Encrypted:	false
SSDEEP:	192:rgZjQD65k8Fjx24kW5MMYKsB1Qmt/ZuhzASgZebr0/qsma:rQsmK8hg8CM/a1QmDJv8v0/qc
MD5:	1FE7A087B5E872A055F8BB46D7C49039
SHA1:	9B93A777D79844B89CFD45ABB9A3033701B47C7C
SHA-256:	443AE3CFC1C096224915F58654531D02A2CCC26EFD26EC8F864F3BB2E05A3C11
SHA-512:	1040C0AAA220FF01A67575BF790C77A5A444EE7627435740F33D059F63D6031B8E5D912BDF3015DC6F3C992E27F2B77D63113FF169CC1C843DD02BF104D368B3
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\{7BEC0D8C-3038-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.564185625667412
Encrypted:	false
SSDEEP:	48:IwKGcprXGwpamG4pQ+GrapbSDrGQpKRG7HpR1sTGIpG:ruZBQW6wBSDFAAT14A
MD5:	CA8D4FF5727B73DB6BEE6D20226F7D38
SHA1:	5649953A5FBFFF24A9D1737E374DB3848DC4E270
SHA-256:	DC530805FC5009BBB8567DEB09B4D0D5589B835A986FCA69DD4B64B2436B2917
SHA-512:	658901535056E94C1C5F9F104268D0D4EDEF9CE7B3002C4AFE247061137E1C03F16DE72124E7301E9B734278521E9A8CE843E6E8F315C3D44BAA5CEE496FCAB
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.096239981965663
Encrypted:	false
SSDEEP:	12:TMHdNMNxOEYO/JnWimI002EtM3MHdNMNxOEYO/JnWimI00ObVbkEtMb:2d6NxOUSZHKd6NxOUSZ76b
MD5:	F8CB63CD207721F6CA14048F5141C052
SHA1:	FEE5B13F3DE9FB581521A87E736147DB9A88FCF2
SHA-256:	5B2B1305AD2FCA4E1A9AFE22F357DB1A3720C52D11F39E049AB23B7D501D31A0
SHA-512:	44AEAFBA8EA74F1329002607CE2F2DC49001DBC5F03A86B5FDEF07F81372DEA935AE0E74AF5BE1FC7F98BD3A68E0E1461AD71AEA381766A4A0CC599957FBEE 83
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x31d2af4e,0x01d6c445</date>< accdate>0x31d2af4e,0x01d6c445</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x31d2af4e,0x01d6c445</date><accdate>0 x31d2af4e,0x01d6c445</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Twitter.url"/></tile ></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.149060538645467
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kfOYJnWimI002EtM3MHdNMNxe2kfOYJnWimI00Obkak6EtMb:2d6NxrWSZHKd6NxrWSZ7Aa7b
MD5:	B67A0957EE85F8729ECA558D4FF15282
SHA1:	F45B187B9D7EBF4BCBC31760EEB257E043117824
SHA-256:	B25BA00926C91843821137BFFEA40B5E97B2700184A94A5E54B488ADE88E7CC0
SHA-512:	E7D6C9DF63EFA8727541C787E9E463FFDA25FCFEBB155646A700E2A5B94A5ED091426C8B63BC6B350DAB17C581EB8B9149FE511F235699F0156E4E32F62143F
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x31bf9c67,0x01d6c445</date><accdate>0x31bf9c67,0x01d6c445</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x31bf9c67,0x01d6c445</date><accdate>0x31bf9c67,0x01d6c445</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Amazon.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	662
Entropy (8bit):	5.130583521331764
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLb1HOg1HJnWimI002EtM3MHdNMNxvLb1HOg1HJnWimI00ObmZEtMb:2d6Nxv/LrSZHKd6Nxv/LrSZ7mb
MD5:	BB9D81497C6ED661BD40449246749024
SHA1:	090B0917679E88084C4524505B5DAAFB0F3A2FB5
SHA-256:	1FFE0D62598B09279ADA1F246C51424FA893B20BB5F4064769159D25B391EFB3
SHA-512:	F0439CA8051A750E7D577D1435DDA05EC1785ED9A41C9FD47580851C44D4C1997121D1246961A0F3B6DB9DED42AF0DCD9D574A8754CB636905414213E393BCF
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x31d51197,0x01d6c445</date><accdate>0x31d51197,0x01d6c445</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x31d51197,0x01d6c445</date><accdate>0x31d51197,0x01d6c445</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Wikipedia.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	647
Entropy (8bit):	5.13229277449301
Encrypted:	false
SSDEEP:	12:TMHdNMNxi4+KOh+KJnWimI002EtM3MHdNMNxi4+KOh+KJnWimI00Obd5EtMb:2d6NxIeuSZHKd6NxIeuSZ7Jjb
MD5:	AA3DEF8BBDFD3CFB746BB62E5A626272
SHA1:	ED4D27ADC8039E56302D4D8002A359DEA65A57F8
SHA-256:	4043E49D4A24C38E4454191A770C94B28547C2451EB20BC6C4143E5A79B8E6D9
SHA-512:	EEF24021857EC5947D2DF9752762EC94313266FB5BB8027BA74024C8298D5F52E860C57942B23955AEB4BB6220C613DF206EB9296E90E3A6E8587ECD0959C105
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x31c925ed,0x01d6c445</date><accdate>0x31c925ed,0x01d6c445</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x31c925ed,0x01d6c445</date><accdate>0x31c925ed,0x01d6c445</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Live.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.1347690871576175
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
SSDEEP:	12:TMHdNMNxhGwJ3OU3JnWimI002EtM3MHdNMNxhGwJ3OU3JnWimI00Ob8K075EtMb:2d6NxQCSZHKd6NxQCSZ7YKajb
MD5:	09A898CDA8942A6820973C09213CBC90
SHA1:	CD1DA75F0C63199CF1CF121995576B85E901514C
SHA-256:	3CD8DDDC28A10B9F06C9CD190AEDA7B5EAA369825611F827FCC51C3399222D0E
SHA-512:	64A98303E0D3AE6C1E949CEFA6C6462579299882602912C304DCA3F556A2F03744DDEFEA00C7ADDA6B2EE8E9DC2FEA29764C09732693F4585753AAF9040EC63
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x31d77405,0x01d6c445</date><accdate>0x31d77405,0x01d6c445</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x31d77405,0x01d6c445</date><accdate>0x31d77405,0x01d6c445</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Youtube.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.105600374537227
Encrypted:	false
SSDEEP:	12:TMHdNMNx0nwXJHONXJHJnWimI002EtM3MHdNMNx0nwXJHONXJHJnWimI00ObxEty:2d6Nx0wsXSZHKd6Nx0wsXSZ7nb
MD5:	FD560E22E048043677BDFF6B1EC23F82
SHA1:	FFBEA1CAE76ABD0574D960F8F0136DBCC30DCDC7
SHA-256:	DC9419387BFBAF08EBB09697FF33E1C36A102A92955E17048E5BACDC7568E23C
SHA-512:	9DF4376A85F1020C4FEE2CC65AF06FF7D9470D3D5AA9BFA1F104787B9F494AB71F00ABEE5B603257E097BCF3640193BE8199928DF4B5B35BC7867663FBAB37E
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x31cdea92,0x01d6c445</date><accdate>0x31cdea92,0x01d6c445</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x31cdea92,0x01d6c445</date><accdate>0x31cdea92,0x01d6c445</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Reddit.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.156052100624938
Encrypted:	false
SSDEEP:	12:TMHdNMNxxnKOUKJnWimI002EtM3MHdNMNxxnKOUKJnWimI00Ob6Kq5EtMb:2d6Nx7SZHKd6Nx7SZ7ob
MD5:	3A12FFA051FBE69F0A1186C40BF3F390
SHA1:	05C72A781611B607E02E96EE64D2E2D6201A2E4A
SHA-256:	4B42AC76E1F706F1E27AC587E842FF35FDCD8E84173685EB031C5A5930C3780C
SHA-512:	F630CBBCE44E7E05B09CB0A3EC0814E460859D9F1C5CFD36CEFAEFB19B8C8E13F438B8A9B658D0C65B8C6A45D3372AB763714F013A056D1BAF3473BBFA75E71
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x31cb8836,0x01d6c445</date><accdate>0x31cb8836,0x01d6c445</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x31cb8836,0x01d6c445</date><accdate>0x31cb8836,0x01d6c445</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\NYTimes.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	659
Entropy (8bit):	5.071440900184945
Encrypted:	false
SSDEEP:	12:TMHdNMNxc7OgJnWimI002EtM3MHdNMNxc7OgJnWimI00ObVEtMb:2d6Nx+SZHKd6Nx+SZ7Db
MD5:	EFCE9F889664D4546CEBBCB14264024F
SHA1:	FE812B45412DE8E03A94B3028E20407C40310BD5
SHA-256:	033B0774F83F0D74EF124F372E76F3C4003DA368B0ED4A1D0D8B69808AEB6A3B

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml	
SHA-512:	0795A605788A564199EFEC863D3E78A3E8DF7E823C27075F1E2F59A4748702D42FCAD28D5057D6B6BFD1D01756BF74BAD182EB655DA0AEF33CD7107D4A13C47E
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x31c1fecc,0x01d6c445</date><accdate>0x31c1fecc,0x01d6c445</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x31c1fecc,0x01d6c445</date><accdate>0x31c1fecc,0x01d6c445</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Facebook.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.087420129408385
Encrypted:	false
SSDEEP:	12:TMHdNMNxfnOCVoKO1CVoKJnWimI002EtM3MHdNMNxfnOCVoKO1CVoKJnWimI00Ou:2d6NxWBcSZHKd6NxWBcSZ7ijb
MD5:	F52E315B4A8E336E0AF2F18ADBDFC2B9
SHA1:	6C587EC329F0902A899C0C62681E12D1D539A14F
SHA-256:	5C8219A5F8D60FDE186D5EF202A4CC57F2DAF8E28D58AA5D16B54186A2CC66CD
SHA-512:	37EAB42CF0C3FF66A712B2458EC8D4ADAE501A9E72B36100AA1E880165888393001B818D360DBEAE3DE35A09E86C5153C49BD582853267BAB08A37F579618E9
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x31c4611f,0x01d6c445</date><accdate>0x31c4611f,0x01d6c445</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x31c4611f,0x01d6c445</date><accdate>0x31c4611f,0x01d6c445</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Google.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\ynfz0jx\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	modified
Size (bytes):	26344
Entropy (8bit):	3.78453648665459
Encrypted:	false
SSDEEP:	96:au0iZQRfC66fD98yFVNTJiVDDQ98b7/OIP97NiINioNiVNiwNiwQQQQQYNi/:ZORfM7nvix/1iQiwiXiIiYi/
MD5:	B30DEE4AAED7DC41DBDEDFA0174D4EA7
SHA1:	1C47C71D67E5986CC441B4480C7BBB4BFBF1602C
SHA-256:	953EE7D9CDBF6BEA66BD0C11EE48E1C7590B9E7BDA83B074338C8D78E91DEF8B
SHA-512:	0E99075E4CC23973183D27B64D31392F77DDA2D4C8B31826F14FECA6B5B3EBDF825E49B65F49967D92B4D23B6594CE9EE26BC24E63DF0B2E22197C43D4D9733A
Malicious:	false
Reputation:	low
Preview:	F.h.t.t.p.s.:././.w.o.n.d.e.r.w.a.t.e.r.b.e.a.d.s...c.o.m./.S.t.e.p.h.a.n.i.e./.D.r.i.v.e./.i.m.a.g.e.s./.f.a.v.i.c.o.n...i.c.o.?.r.e.v.=.4.5..... ....(... ...@..... ....l.....o...o.6.n.f.m...m...l...l..... .....s.0.s.Z.r...q...p...o...o...n...m...m...l...l.....w...v.K.v.x.u...u...t...s...s...r...q...p...o...o...n...m...m...l...l..... .....w...v...v...u...u...t...s...s...r...q...p...o...o...n...m...m...l...l...p...p...n...l.D.....w...v...v...u...u...t...s...s...r...q...p...o...o...n...m...m...l...l.....t...l.?.....w...v...v...u...u..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\50-f1e180[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	133458
Entropy (8bit):	5.224381274909031
Encrypted:	false
SSDEEP:	3072:1f/HuFVppxvIeJ0i9d1EwgXA9JKEODCE5n:1f/Hu/FIeRKn
MD5:	365A10154187380204CA942771D68129
SHA1:	B34E3B77D8D2D6CBF29F57AEE3C14BE3F567EF39
SHA-256:	0FA4389403FD21C7C419C3EDD787F90E198D8D05639967D85BB8D391294B7B75
SHA-512:	1A41E4E5EA1D8F4B73AD8DD720A66DE033F68D48C235FB9BE0923BB575902451E4289C7899E76632C327569BEBCC3DFC0B991F49E9E0BC18482FA9A2FF4B281D
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\50-f1e180[1].js	
IE Cache URL:	http://https://www.microsoft.com/onerfstatics/marketingsites-eus-prod/shell/_scrf/js/themes=default/54-af9f9f/c0-247156/de-099401/e1-a50eee/e7-954872/d8-97d509/f0-251fe2/46-be1318/77-04a268/11-240c7b/63-077520/a4-34de62/bb-d7480b/db-bc0148/dc-7e9864/6d-c07ea1/29-1ec5a9/23-c64e70/cd-23d3b0/6d-1e7ed0/b7-cadaa7/c4-898cf2/ca-40b7b0/4e-ee3a55/3e-f5c39b/c3-6454d7/f9-7592d3/92-10345d/79-499886/7e-cda2d3/b2-7087f0/ea-1a640b/e0-3c9860/91-97a04f/1f-100dea/33-abe4df/50-f1e180?ver=2.0&iife=1
Preview:	(function(){/**. * @license almond 0.3.3 Copyright jQuery Foundation and other contributors.. * Released under MIT license, http://github.com/requirejs/almond/LICENSE. */ .var requirejs,require,define,__extends;(function(n){function r(n,t){return w.call(n,t)}function s(n,t){var o,s,f,e,h,p,c,b,r,l,w,k,u=t&&t.split("/"),a=i.map,y=a&&a["*"]||{};if(n){ for(n=n.split("/"),h=n.length-1,i.nodeIdCompat&&v.test(n[h])&&(n[h]=n[h].replace(v,"")),n[0].charAt(0)==="."&&u&&(k=u.slice(0,u.length-1),n=k.concat(n)),r=0;r<n.length;r+ +)if(w=n[r],w==="."")n.splice(r,1),r-=1;else if(w===".."){if(r===0||r===1&&n[2]===".."||n[r-1]===".")continue;else r>0&&(n.splice(r-1,2),r-=2);n=n.join("/")}if((u||y)&&a){ for(o=n.split("/"),r=o.length;r>0;r-=1){if(s=o.slice(0,r).join("/"),u)for(l=u.length;l>0;l-=1)if(f=a[u.slice(0,l).join("/")],f&&(f=f[s],f)){e=f;p=r;break}if(e)break;!c&&y&&y[s]&&(c =y[s],b=r)}!e&&c&&(e=c,p=b);e&&(o.splice(0,p,e),n=o.join("/"))}return n}function y(t,i){return function(){var r=b.call(arguments,0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\7d-3b8b80[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	168619
Entropy (8bit):	5.044040083782762
Encrypted:	false
SSDEEP:	3072:OzCPZkTP3bDLH0tfRqQ0xtLfj4ZDSIpTt813viY8R1j35Ap7LQZLPPJH7PAbOCx8:clZAXLkeeds
MD5:	7A091EA3F595695C19CED8B52228FF48
SHA1:	587B8C1FFF5C84755C8BE6C2029FC0B46C0F76B3
SHA-256:	C55B3700FA0698B9F057F40512CFD3B9D6AED620598BACE734338F4F6DAF7A86
SHA-512:	522DC920EDA85D8C7F6FA56E959552C477133E1C5C39939331962A221E5C5AEAEC0643FE8F6AFF4384125B4B58E3930751A21CEB7C60C309AD037ED12865AF8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.microsoft.com/onerfstatics/marketingsites-eus-prod/west-european/shell/_scrf/css/themes=default.device=uplevel_web_pc/4a-f2fa13/d2-97697e/15-b02cf6/8d-8de298/30-e5ac82/cd-1bda0a/e7-838d86/7d-3b8b80?ver=2.0
Preview:	@charset "UTF-8";./*! | Copyright 2017 Microsoft Corporation | This software is based on or incorporates material from the files listed below (collectively, "Third Party Code"). Microsoft is not the original author of the Third Party Code. The original copyright notice and the license under which Microsoft received Third Party Code are set forth below together with the full text of such license. Such notices and license are provided solely for your information. Microsoft, not the third party, licenses this Third P arty Code to you under the terms in which you received the Microsoft software or the services, unless Microsoft clearly states that such Microsoft terms do NOT apply for a particular Third Party Code. Unless applicable law gives you more rights, Microsoft reserves all other rights not expressly granted under such agreement(s), whether by implication, estoppel or otherwise.*/./*! normalize.css v3.0.3 | MIT License | github.com/necolas/normalize.css */.body{margin:0}.context-uh

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\CommonIntl[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):	92411
Entropy (8bit):	5.147146253857141
Encrypted:	false
SSDEEP:	1536:/KMLN5vGL78J0JsCxtzXnCG+Uhk0Bvj0Bac3w:7WJ2G+8Bvz
MD5:	D9AB6B448431A81766CE3E58AFD640E6
SHA1:	A3C8A9C9D6AF7D7B03565FBFF98DF9733D0F6F5D
SHA-256:	F860F3F3F0BD0C35EEF1E5D3292E627DC434F3E75BE6B2654F93C1192B17AC74
SHA-512:	83207F3859F0F5E0AF07A834C00C50B87E766D3304247664302B225746C5AC897CA5C00021BA04FCCC7C369E4B9FC2A65A19C4779F3998ED56E48942C4E2222C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c1-officeapps-15.cdn.office.net/o/s/161351641006_App_Scripts/1033/CommonIntl.js
Preview:	CommonStrings={qpsPloc_Name:"Pseudo",qpsPloca_Name:"Pseudo (Pseudo Asia)",qpsPlocm_Name:"Pseudo (Pseudo Mirrored)",afrikaans:"Afrikaans",albanian:"Alb anian",alsatian:"Alsatian",amharic:"Amharic",arabic:"Arabic",arabic_Algeria:"Arabic (Algeria)",arabic_Bahrain:"Arabic (Bahrain)",arabic_Egypt:"Arabic (Egypt)",arabic_Iraq :"Arabic (Iraq)",arabic_Jordan:"Arabic (Jordan)",arabic_Kuwait:"Arabic (Kuwait)",arabic_Lebanon:"Arabic (Lebanon)",arabic_Libya:"Arabic (Libya)",arabic_Morocco:"Arabic (Morocco)",arabic_Oman:"Arabic (Oman)",arabic_Qatar:"Arabic (Qatar)",arabic_Saudi_Arabia:"Arabic (Saudi Arabia)",arabic_Syria:"Arabic (Syria)",arabic_Tunisia:"Arabic (Tunisia)",arabic_UAE:"Arabic (U.A.E.)",arabic_Yemen:"Arabic (Yemen)",armenian:"Armenian",assamese:"Assamese",azerbaijani:"Azerbaijani",azerbaijani_Cyrillic :"Azerbaijani (Cyrillic)",azerbaijani_Latin:"Azerbaijani (Latin)",bangla_Bangladesh:"Bangla (Bangladesh)",bangla_India:"Bangla (India)",bashkir:"Bashkir",basque:"Basque", belarusian:"Belarusi

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\MicrosoftAjax[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	108297
Entropy (8bit):	5.337478406407795
Encrypted:	false
SSDEEP:	1536:MGLiogSomRYvoGtT+KHsVS0bT79DSsi46j/LPyR7kmE1KzV:MGLXGFKT79DSs6WBEKV
MD5:	1EFF9A061B550B4540A721E8AA2561DF
SHA1:	5EB3712E7C153C0136C38ADDA2E0404D6B8E5782
SHA-256:	EC3E0FECD8521498ACA392912219497D50C10EE21FCD8E670F04B86BD7D7B225

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\MicrosoftAjax[1].js	
SHA-512:	7831E45A05F1F589F379449808C49F9AA8B615E9981331703F7FB588DCC0AB059084DF4C807DD2AA007A2BF4F34F67F72C4C9E2572E28B1DE473595E6AD1D1F2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c1-officeapps-15.cdn.office.net/o/s/161351641006_App_Scripts/MicrosoftAjax.js
Preview:	//----------..// Copyright (C) Microsoft Corporation. All rights reserved...//----------..// MicrosoftAjax.js..Function.__typeName="Function";Function.__class=true;Function.createCallback=function(b,a){return function(){var e=arguments.length;if(e>0){var d=[];for(var c=0;c<e;c++)d[c]=arguments[c];d[e]=a;return b.apply(this,d)}return b.call(this,a)}};Function.createDelegate=function(a,b){return function(){return b.apply(a,arguments)}};Function.emptyFunction=Function.emptyMethod=function(){};Function.validateParameters=function(c,b,a){return Function._validateParams(c,b,a)};Function._validateParams=function(g,e,c){var a,d=e.length;c=c||typeof c==="undefined";a=Function._validateParameterCount(g,e,c);if(a){a.popStackFrame();return a}for(var b=0,i=g.length;b<i;b++){var f=e[Math.min(b,d-1)],h=f.name;if(f.parameterArray)h+="["+(b-d+1)+"]";else if(!c&&b>=d)break;a=Function._validateParameter(g[b],f

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\OneNote.box4.dll2[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	1387913
Entropy (8bit):	5.607144640344505
Encrypted:	false
SSDEEP:	24576:gB41AimZVGrNI0S7qZ9hZL2EZp92k7bBYhntpehiYqwhrEO1wExWfkHmfryRbA:gB41AimZVGrNI0S7qZ9hZL2EZp92k7bM
MD5:	D4CD10DC2482BFBF0DB877125A86B0DC
SHA1:	E0501BFE366BA52537AC01E79C972787221F73CE
SHA-256:	5A10A7012AC2B2EA01CF3206F5C9BA1306E52FA8D5336D0A05DCC32FF3DB3F91
SHA-512:	257931645F992C182FA5A6FECA75311F63E03067BA535D8326334B520AD0DC6CCF89C0274B43E81FEDD993B5ED42899FA3356FAAB5C4404FBCAD2DE8032B814
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c1-onenote-15.cdn.office.net/o/s/161351641006_App_Scripts/OneNote.box4.dll2.js
Preview:	function wac_M4(){return wac_p3b.qa()}var wac_N4=!1;function wac_O4(a){a&&!wac_M4().kc(a.Aj)&&String.format("Tag Indent Type not defined for tag {0}.",a.Aj)}function wac_L9b(a){if(wac_42(a))return null;var b=a.indexOf(":");return 0<=b&&a.length>b+1?a.substr(b+1):null}var wac_M9b=null;function wac_N9b(a){if(!a)return null;wac_O4(a);var b="";1===wac_M4().H(a.Aj)?b="\n":2===wac_M4().H(a.Aj)?b="":wac_M4().H(a.Aj)||(b="\n");wac_N4=!wac_42(b);return b}.function wac_O9b(a,b,c){if(!b)return null;wac_O4(b);if(c&&1===wac_M4().H(b.Aj))return wac_N4=!0,"\n";if(c)return"";a=a?2===wac_M4().H(b.Aj)?"":"\n":1===wac_M4().H(b.Aj)?"\n":"";wac_N4=!wac_42(a);return a}function wac_P9b(a){if(!a)return null;wac_O4(a);if(!wac_42(a.Qd))return"";var b=new Sys.StringBuilder("");if(wac_N4||1===wac_M4().H(a.Aj)){for(var c=0;c<a.Vub;c++)b.append("\t");return b.toString()}return""}.function wac_Q9b(a,b,c){if(!a)return null;wac_O4(a);var d=new Sys.StringBuilder("");if(!(a.hi&&1===wac_M4().H(a.hi.Aj)||wac_N4||2!==wac_M

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\OneNoteIntl[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):	31303
Entropy (8bit):	4.889964601637444
Encrypted:	false
SSDEEP:	384:+gNpdtptTNzZ6TJcB/pw+UkNqJ3ncwKVXYMCwnp5molHuE7:+2dtptTNzrpmkNqJ3c1xYhwp5n97
MD5:	604B1BF80A1E538250F0CFD06F6ECF62
SHA1:	509A7B4451A912B14543F87A492E608C438AFE5E
SHA-256:	E523127A92153576DAC2A7742ED21531743D527A7EFD7941A4B7F8310106351A
SHA-512:	73867EE7A22FDA935EA1B7C454BC31D77AAE0C80298F6D0CCC768C0F61B3DBA415985727566DAA2DC2A1D80545CF6328917540FA78859F98435E25FD885F040
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c1-onenote-15.cdn.office.net/o/s/161351641006_App_Scripts/1033/OneNoteIntl.js
Preview:	Type.registerNamespace("OneNoteIntl");OneNoteIntl.OneNoteStrings=function(){};OneNoteIntl.OneNoteStrings.registerClass("OneNoteIntl.OneNoteStrings");OneNoteIntl.OneNoteStrings.L_BrowseVersions="Page Versions";OneNoteIntl.OneNoteStrings.L_Camera="Camera";OneNoteIntl.OneNoteStrings.L_CopyNotebook="Copy Notebook";OneNoteIntl.OneNoteStrings.L_Covid19Message="We\u2019re temporarily limiting certain capabilities in {appshort}.";OneNoteIntl.OneNoteStrings.L_Covid19Link="Learn more";OneNoteIntl.OneNoteStrings.L_Covid19MessageViewMode="To ensure the best possible experience for our users, OneNote will be read only by default.";OneNoteIntl.OneNoteStrings.L_CopyToCloudDescription="Edit and view this notebook on all your devices";OneNoteIntl.OneNoteStrings.L_DeleteSectionConfirmationTitle="Permanently Delete Section";OneNoteIntl.OneNoteStrings.L_DeleteSectionConfirmationDescription="Deleting a section can't be undone. Do you want to permanently delete this section and all of its pages?";OneNoteInt

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\RE1Mu3b[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 216 x 46, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	4054
Entropy (8bit):	7.797012573497454
Encrypted:	false
SSDEEP:	48:zICvnyRHJ3BRZPcSPQ72N2xoiR4fTJX/rj4sFNMkk5/p1k2lPUmbm39o4aL7V9XH:10nvE724xoiRQJPrjpLKSFl9oX31Z1d
MD5:	9F14C20150A003D7CE4DE57C298F0FBA
SHA1:	DAA53CF17CC45878A1B153F3C3BF47DC9669D78F

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\RE1Mu3b[1].png	
SHA-256:	112FEC798B78AA02E102A724B5CB1990C0F909BC1D8B7B1FA256EAB41BBC0960
SHA-512:	D4F6E49C854E15FE48D6A1F1A03FDA93218AB8FCDB2C443668E7DF478830831ACC2B41DAEFC25ED38FCC8D96C4401377374FED35C36A5017A11E63C8DAE5C87
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://img-prod-cms-rt-microsoft-com.akamaized.net/cms/api/am/imageFileData/RE1Mu3b?ver=5c31
Preview:	.PNG.....IHDR.....J.....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-c132 79.159284, 2016/04/19-13:13:40 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpMM:DocumentID="xmp.did:A00BC639840A11E68CBEB97C2156C7FD" xmpMM:InstanceID="xmp.iid:A00BC638840A11E68CBEB97C2156C7FD" xmp:CreatorTool="Adobe Photoshop CC 2015.5 (Windows)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:A2C931A470A111E6AEDFA14578553B7B" stRef:documentID="xmp.did:A2C931A570A111E6AEDFA14578553B7B"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>.....DIDATx..\..UU.>.7..3....h.L..& j2...h.@..".....`U.....R"..Dq.&.BJR 1.4`$.200...l.....wg.y.[k/

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\WoncaIntl[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):	28569
Entropy (8bit):	5.011682742007546
Encrypted:	false
SSDEEP:	384:NpM3QZmZwe3CDLqHOGRv/HYdd9KaAQnzkY01:NpM3QZbLqHO4XYdd9KvQnzkY01
MD5:	559C40D78B5DC4E058130F31058E7686
SHA1:	F7DB6921AB1E656F10A15F6878655D1C73FE4D96
SHA-256:	A4BD3FD7C4ADF16943873C9BB06534320BD8C4A16B905DE8A457664E2312C6A7
SHA-512:	F46505E6F73104DCFA77910EE2979CD035CA0A1EEF7C9C8AC0F90FE7D2FC0251FAE5D2EC138C9EE760C471A972BB599778A69C311F28DE37EEDDF1F538EF03EB
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c1-onenote-15.cdn.office.net/o/s/161351641006_App_Scripts/1033/WoncaIntl.js
Preview:	Type.registerNamespace("WoncaIntl");WoncaIntl.WoncaStrings=function(){};WoncaIntl.WoncaStrings.registerClass("WoncaIntl.WoncaStrings");WoncaIntl.WoncaStrings.L_RibbonLabel="Ribbon";WoncaIntl.WoncaStrings.L_TabHome="Home";WoncaIntl.WoncaStrings.L_TabInsert="Insert";WoncaIntl.WoncaStrings.L_TabWordDesign="Design";WoncaIntl.WoncaStrings.L_TabReferences="References";WoncaIntl.WoncaStrings.L_TabMailings="Mailings";WoncaIntl.WoncaStrings.L_TabReview="Review";WoncaIntl.WoncaStrings.L_TabView="View";WoncaIntl.WoncaStrings.L_TabDeveloper="Developer";WoncaIntl.WoncaStrings.L_TabAddIns="Add-ins";WoncaIntl.WoncaStrings.L_TabTableTools="Table Tools";WoncaIntl.WoncaStrings.L_TabLayout="Layout";WoncaIntl.WoncaStrings.L_TabPictureTools="Picture Tools";WoncaIntl.WoncaStrings.L_TabFormatPicture="Format";WoncaIntl.WoncaStrings.L_TabDesign="Design";WoncaIntl.WoncaStrings.L_TabHelp="Help";WoncaIntl.WoncaStrings.L_GroupUndoRedo="Undo";WoncaIntl.WoncaStrings.L_GroupClipboard="Clipboard";WoncaIntl.WoncaString

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\c[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):	42
Entropy (8bit):	3.0241026136709444
Encrypted:	false
SSDEEP:	3:CUXPQEsJ+q:1QEsJ+q
MD5:	32023BB33CFB2A1990A4EF2D85B6AC16
SHA1:	23DCC6D4B5BFE00357FD0248BB5955B8E36BB8F1
SHA-256:	99C2917EE5B2A01459A923BDD1C676F15EE73B62B87F696E6735312D26F51E12
SHA-512:	D052ECEC2839340876EB57247CFC2E777DD7F2E868DC37CD3F3F740C8DEB94917A0C9F2A4FC8229987A0B91B04726DE2D1E9F6BCBE3F9BEF0E4B7E0D7F65EA12
Malicious:	false
Reputation:	low
Preview:	GIF89a.....!.....,.....L.;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\clientstring[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):	3712
Entropy (8bit):	5.03306639798282
Encrypted:	false
SSDEEP:	48:9ryq+aNhZUcuyPlGWloNMT8acDts/oLjUEt5b+xHrb1Mk81wnkkW5If0j:9rjLZfuAGMoNM9M+tO5w+5u0j
MD5:	6B640FEF16FC53CA4DC8D4326E6FC420
SHA1:	660200F5B105C38C550B640E368A06E53756E8D2
SHA-256:	384DBE56F1938E93EC9730B9F20CF41FA3B46BEDBF530FA3CC73EEF3FE72DA07

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\clientstring[1].js	
SHA-512:	5D9F9F96C1B45E8762CBECEA701CCF9D88F3793DEB574C6A028F9C735487DF361614F48C5768D0191D493F06D885B09EC7F66241F3A92DBCA54B9873A7EDB15
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://onedrive.live.com/handlers/clientstring.mvc?mkt=en-US&group=GroupFolders&v=19.419.0221.2001&useRequiresJs=False
Preview:	(function () {window.GetString = function(s){var rootObject = this, parts = s.toLowerCase( ).split('.'), iCount = parts.length;for (var i = 0; i < iCount; i++){var currentPart = parts[i];rootObject = rootObject[currentPart];if (rootObject == null){return '';}}return typeof (rootObject) == "object" ? rootObject.___str : rootObject.toString();};.var LEEy = window.live=window.live||{};var DOWI=LEEy.shared=LEEy.shared||{};var VGGy=DOWI.skydrive=DOWI.skydrive||{};var aOyf=VGGy.gf=VGGy.gf||{};var jRHP=aOyf.createfolder=aOyf.createfolder||{};jRHP["addcoowners"]="Co-owners";jRHP["addcoownerslinktext"]="Add co-owners";jRHP["addeditors"]="Editors";jRHP["addeditorslinktext"]="Add editors";jRHP["permissionshelptext"]="You can collaborate with people by adding them as co-owners. Co-owners can add this folder to their own OneDrive and access it from anywhere.";jRHP["permissionshelptextforeditors"]="You can collaborate with people by adding them as editors. Editors can add this folder to their own One

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\common.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	401580
Entropy (8bit):	5.305202439087071
Encrypted:	false
SSDEEP:	6144:d7SWKOUlW0bVdydRljuj/ZExMbyOFpd6VA9:RSWKqH3sq
MD5:	168E2D0857E8971B47A075BA1412CB6E
SHA1:	CDA80FB437946CCE5500D4424E36C22EED6C2532
SHA-256:	4098ABDCC6481C728B7EAC24AD4146B741D892BE33914630E78BF6715A011E21
SHA-512:	7900EB143C116C60329AC8ABA9B202442B9F7BD3AEBAAF2144E4DD17452E8A983C001BF81CF6FFF01BC68028C899782C3170CC1ECE5A57CA26211516C2301D(
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c1-onenote-15.cdn.office.net/o/s/161351641006_App_Scripts/common.min.js
Preview:	(window.webpackJsonp_name_=window.webpackJsonp_name_||[]).push([[0],{0:function(e,t,n){"use strict";n.d(t,"d",(function(){return o})),n.d(t,"a",(function(){return i})),n.d(t,"h",(function(){return a})),n.d(t,"c",(function(){return u})),n.d(t,"f",(function(){return s})),n.d(t,"b",(function(){return l})),n.d(t,"e",(function(){return c})),n.d(t,"k",(function(){return d})),n.d(t,"g",(function(){return f})),n.d(t,"i",(function(){return p})),n.d(t,"j",(function(){return h}));./*! ********** ******.Copyright (c) Microsoft Corporation...Permission to use, copy, modify, and/or distribute this software for any.purpose with or without fee is hereby granted...THE SOFTWARE IS PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL WARRANTIES WITH.REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY.AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY SPECIAL, DIRECT,.INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHA

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\es6-promise.auto.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):	6498
Entropy (8bit):	5.084045736135045
Encrypted:	false
SSDEEP:	96:+0jAZG8kQrNkq5sr9KlGzbGQa5NUufRGorSqiZqW8+R7bBfj3IaJcMN5Mof:+OENx5oOAozG9V3nJ55Nf
MD5:	889F6A354B79C38BDF62A8792A65329D
SHA1:	34B3404AEE23C330527201DC2C3B6E78A7655F51
SHA-256:	5F1ADDAF2E9F5922AED63D802F2B8AFE01C543ED81A7BE99AD1E9FDD05C8E3B6
SHA-512:	4BF35D2EE9D5E083B5C4F21F6FD213F485E1CCE6DE320E96471031FBCBCE5760CCFA233AAF443A8A2A08C2B628548E6A1C490F54CBF5F66FF4F4D9CB22362EC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c1-onenote-15.cdn.office.net/o/s/161351641006_App_Scripts/es6-promise.auto.min.js
Preview:	!function(t,e){"object"==typeof exports&&"undefined"!=typeof module?module.exports=e():"function"==typeof define&&define.amd?define(e):t.ES6Promise=e()}(this,function(){"use strict";function t(t){var e=typeof t;return null!==t&&("object"===e||"function"===e)}function e(t){return"function"==typeof t}function n(t){W=t}function r(t){z=t}function o(){return function(){return process.nextTick(a)}}function i(){return"undefined"!=typeof U?function(){U(a)}:c()}function s(){var t=0,e=new H(a),n=document.createTextNode("");return e.observe(n,{characterData:!0}),function(){n.data=t=++t%2}}function u(){var t=new MessageChannel;return t.port1.onmessage=a,function(){return t.port2.postMessage(0)}}function c(){var t=setTimeout;return function(){return t(a,1)}}function a(){for(var t=0;t<N;t+=2){var e=Q[t],n=Q[t+1];e(n),Q[t]=void 0,Q[t+1]=void 0}N=0}function f(){try{var t=Function("return this")().require("vertx");return U=t.runOnLoop||t.runOnContext,i()}catch(e){return c()}}function l(t,e){var n=this,

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\fabricmdl2icons[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 151924, version 0.0
Category:	downloaded
Size (bytes):	151924
Entropy (8bit):	**7.996755078799659**
Encrypted:	**true**
SSDEEP:	3072:izu4By5vR4gdzOjZHpybtAVOZ71Q1gcq0WTo7wSRhpFY/iw2yQ0X2+6L0aR/h:iznyHBmNMJcOd1ro719FY/ilyQ0Gp
MD5:	E80FF72E03E780056CFDBD85C63404CE
SHA1:	C450A1A6233F0FBC6DBFFB7FEE251E378F64EF32

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\fabricmdl2icons[1].woff	
SHA-256:	05828D625DCB5781D0A3CC67A2429CED535FDF848B8B8075D49751EB5B30C7AF
SHA-512:	D819D75CA896AF15F99185F87AF40A85A0FA6941B9E08974C6569123B601DCC8E043BE1C0F5C154E37A351A046B57D5196002B16FA7102761E3C0961D92CAC8D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://spoprod-a.akamaihd.net/files/fabric/assets/icons/fabricmdl2icons.woff
Preview:	wOFF......Qt...............................OS/2...X...H...`JZ}.VDMX............^.qcmap...............cvt ...\... ...*....fpgm...|.......Y...gasp...l............glyf...x..$...0.{.yyhead..7`...6...6% .d.hhea..7........$7.5.hmtx..7....M... .N..loca..<....q...D...maxp..K\|... ... .\|..name..K....8.......post..P........ .Q.wprep..P.........x...x.c`.`a......:....Q.B3_dHc..`e.bdb... .`@..`..... .os9.\|...V...)00......x...S......._..m.m.m.m.m;e..y.~.......<p..a.0t.&...a.pa.0B.1..F...Q.ha.0F.3.....q.xa.0A.0L.&...l.da.0E.2L....i.ta.0C.1..f...Y.la.0G.3.....y.\|a..@X0,.....E.ba. DX2,....e.ra..BX1..V...U.ja..FX3.....u.za..A.0l.6...M.fa.E.2l....m.va..C.1..v...].na..G.3......}.~a.p@80......C.a..pD82.....c.q..pB81..N...S.i..pF83.....s.y..pA.0\.....K.e..pE.2\.. ..k.u..pC.1..n...[.m..pG.3......{.}...@x0<.....G.c...Dx2<....g.s...Bx1..^...W.k...Fx3.....w.{...A.0\|.>...O.g...E.2\|....o.w...C.1..~..._.o..08........?..0$........x...wx.....;..j..fwf....R. %.....4.... .."<.w..A.<..H.C'.E.E..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\favicon[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 3 icons, 32x32, 32 bits/pixel, 24x24, 32 bits/pixel
Category:	downloaded
Size (bytes):	7886
Entropy (8bit):	3.762617760119907
Encrypted:	false
SSDEEP:	48:g8Ko0zeZPoRfis1Iv/X1kkPxVR6GUprVNTSyYpDCiaKDDpiVJ/OIyx:90iZQRfC66f+FVNTJiVDDo7/OIY
MD5:	50996DA127314E31E0B14D57B9847C9F
SHA1:	411999ACD54A0E92AF8B8DE9F46DF0CB87219C13
SHA-256:	02B047ABC51FF9C2ED37C976517A3DCDC5620F8A18665CDC37B6DAD40C9284B5
SHA-512:	AF82D9D997885E970F2F3F78CEA88A4E5430B419128B1C1C8F4B110FEB24C61093B77E22E021CE98EB9FD13CB5B552AA9C8277F08D438655AD3069BA9EBC1FFB
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://wonderwaterbeads.com/Stephanie/Drive/images/favicon.ico?rev=45
Preview:	....6......... .... .h...f...(... ...@..... ....l... ....o...o.6.n.f.m...m...l...l...s.0.s.Z.r...q...p...o...o...n...m...m...l...l...w...v.K.v.x.u...u ...t...s...s...r...q...p...o...o...n...m...m...l...l...w...v...v...u...u...t...s...s...r...q...p...o...o...n...m...m...l...l...p...p...n...l.D..w ...v...v...u...u...t...s...s...r...q...p...o...o...n...m...m...l...l.............t...l.?....................................w...v...v...u...u...t...s...s...r...q...p...o...o...n...m...m...l...l.................m........................... ....w...v

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\favicon[2].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 6 icons, 128x128, 16 colors, 72x72, 16 colors
Category:	downloaded
Size (bytes):	17174
Entropy (8bit):	2.9129715116732746
Encrypted:	false
SSDEEP:	24:QSNTmTFxg4lyyyyyyyyyyyyyio7eeeeeeeeekzgsLsLsLsLsLsQZp:nfgyyyyyyyyyyyyynzQQQQQO
MD5:	12E3DAC858061D088023B2BD48E2FA96
SHA1:	E08CE1A144ECEAE0C3C2EA7A9D6FBC5658F24CE5
SHA-256:	90CDAF487716184E4034000935C605D1633926D348116D198F355A98B8C6CD21
SHA-512:	C5030C55A855E7A9E20E22F4C70BF1E0F3C558A9B7D501CFAB6992AC2656AE5E41B050CCAC541EFA55F9603E0D349B247EB4912EE169D44044271789C719CDC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.microsoft.com/favicon.ico?v2
Preview:	..............h(..f...HH...........(..00......h.....6.. ....=..............@..........(....A..(....................(......................................"P.......................................""""""""""""""""""""""""""""""""" ...3 33333333333333333333333333333"""""""""""""""""""""""""""""""" ...33333333333333333333333333333"""""""""""""""""""""""""""""""" ...33333333333333333333333333333"""" """""""""""""""""""""""""""""" ...33333333333333333333333333333"""""""""""""""""""""""""""""""" ...33333333333333333333333333333"""""""""""""""""""""""""""""""" ...33333333333 333333333333333333"""""""""""""""""""""""""""""""" ...33333333333333333333333333333"""""""""""""""""""""""""""""""" ...33333333333333333333333333333"""""""""""""""""""""""""""""""""" """""""""" ...33333333333333333333333333333"""""""""""""""""""""""""""""""" ...33333333333333333333333333333"""""""""""""""""""""""""""""""" ...333333333333333333333 333333333"""""""""""""""""""""""""""""""" ...33333333333333333333333333333""""""""""""""""""""""""""""""""

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\iciconmap8w5v3[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 38 x 16, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	360
Entropy (8bit):	6.500748611072429
Encrypted:	false
SSDEEP:	6:6v/lhP5R/UDTCZA3teTKgnMc2he2GXlaARamMGJWaa0dfHe9U7cOCptjp:6v/7X/klMKCRGe2GXSm9WaPPe9UIOmN
MD5:	A3785FB010AAE2BB3FA284E2D32D2CB4
SHA1:	4850D5195C0A500F19162B5B905AB1E336339E98

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\iciconmap8w5v3[1].png	
SHA-256:	FC76B9828CEA03AD4732FB7764636CFDB2C4898F10BCEBE1CCDB7654D3CE721B
SHA-512:	25C94593DF4DDA661A215474DDE979286AF17879E971042E3257B2DE6B4D3A543507F9740D9DE95DFF01709CC413EAF4A5631634CF77717623EB4DB14BE2FF67
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://p.sfx.ms/ic/iciconmap8w5v3.png
Preview:	.PNG.....IHDR...&.....M.,....sRGB.....gAMA.....a.....pHYs.....d_.....tEXtSoftware.Paint.NET v3.5.100.r....<PLTE.....).....tRNS.."3DUfw.....F *.....tIDAT(..... .@.....].N.....!....5...Z..j.`b&...m1+..6.....u.....U..;....l~`...}.....4.IT..CB6.~.1..t.>. ..b.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\learningtools[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	2248
Entropy (8bit):	5.300870343603721
Encrypted:	false
SSDEEP:	48:EqQWqyRNWqyETY4TbgNWqytNWqyANWqyoNWqyDrogAdgyd1n791RapkHTKNqKNWE:hQWqwWqJbQWq8WqXWq/WqUG1nnsyHTKX
MD5:	3A6897F894BF8A4E8B8A6F8CFC917345
SHA1:	0F4FBB503DFD727B0B543094894FEC1B092911C4
SHA-256:	025C30A69DAC53C667763108B7B7608185E20CE4F1DF2C012BFC4754A62171D9
SHA-512:	4143EA4C426C00DB92C7B0A4BEDA473B3D661AF62C4D14D930A97CCCC5BF1356DCE2AE17CE8C93106D4DF5F28ABD4D543108DBBF278AD75919E9BA1B64FE818
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.onenote.com/officeaddins/learningtools/?et=
Preview:	......<!DOCTYPE html>..<html lang="en-US">..<head>...<meta charset="utf-8">...<title></title>.....<script type="text/javascript" src="https://cdn.onenote.net/officeaddins/161351940458_Scripts/CommonDiagnostics.js" crossorigin="anonymous"></script>...<script type="text/javascript" src="https://cdn.onenote.net/officeaddins/161351940458_Scripts/BrowserUls.js" crossorigin="anonymous"></script>.....<script>.....var EnableClientSideLogging = true;....</script>.....<script type="text/javascript" src="https://ajax.aspnetcdn.com/ajax/jQuery/jquery-2.1.3.min.js"></script>...<script type="text/javascript" src="https://cdn.onenote.net/officeaddins/161351940458_Scripts/ExternalResources/js-cookie.js" crossorigin="anonymous"></script>...<script type="text/javascript" src="https://cdn.onenote.net/officeaddins/161351940458_Scripts/pickadate.min.js" crossorigin="anonymous"></script>...<script type="text/javascript" src="https://cdn.onenote.net/officeaddins/161351940458_Scripts/Instrumentation.js" c

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\officebrowserfeedbackstrings[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):	5543
Entropy (8bit):	4.902895729722011
Encrypted:	false
SSDEEP:	96:iajfo6oEAVzgCM8tDSJoKwbtGUqDq0wUooq/tJ3gf8oAo/cf6DtYuSm9UDiX5Y+x:Tc6cPDSins/q0wUooq/t68oANf6pYvmj
MD5:	3B0BA1C6781E5364B8D4CCF9EDF2D068
SHA1:	48356B6FAA0BD65B2DEE2B59ECD89EC3C5568CA4
SHA-256:	F6C57447BA4EC4C8434FAA5921EC251A018DDE28B1955F3C9B5CA8EDE635BA6D
SHA-512:	CE8DC9AB884DC9F18F0A2011B9BDDA7A80CE7239794B9918ADF2A681A1D148263486343AE8FE5017C612AE803F1F5ADDCD7238E8FD58FEA3F978D8EC64424ADD
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c1-officeapps-15.cdn.office.net/o/s/161351641006_App_Scripts/Feedback/latest/Intl/en/officebrowserfeedbackstrings.js
Preview:	OfficeBrowserFeedback.setUiStrings({FeedbackSubtitle:"Send Feedback to Microsoft","_FeedbackSubtitle.comment":"Subtitle in the main feedback control",PrivacyStatement:"Privacy Statement","_PrivacyStatement.comment":"Text for the privacy statement link",Form:{CommentPlaceholder:"Please do not include any confidential or personal information in your comment","_CommentPlaceholder.comment":"Placeholder text in the comment input",CategoryPlaceholder:"Select a category (optional)","_CategoryPlaceholder.comment":"Placeholder text for category dropdown",EmailPlaceholder:"Email (optional)","_EmailPlaceholder.comment":"Placeholder text in the email input",RatingLabel:"Rating","_RatingLabel.comment":"Label for the rating control",ScreenshotLabel:"Include screenshot","_ScreenshotLabel.comment":"Label for the screenshot checkbox",Submit:"Submit","_Submit.comment":"Button text for the submit button",Cancel:"Cancel","_Cancel.comment":"Button text for the cancel button",EmailCheckBoxLabel:"You can con

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\oreolazylegacy[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	178185
Entropy (8bit):	5.318051417022481
Encrypted:	false
SSDEEP:	1536:6P4JABh+feZpBBZ95BM7Syn6lFhoDusHYCKf7SKENC3YPhtzn34bGYXT209lFem:hQBM2yn6VoXHxS207J
MD5:	4B2BB5EC10F6AE38EDB681DC3DB5D887
SHA1:	F78BD467E16CF41250C6D371F2E89C0D878A8099
SHA-256:	8D8C85092C0BB45F7B97EA98C52578181A1FF0E57554EBE048564A551BCA0E4D

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\oreolazylegacy[1].js	
SHA-512:	B4D6F54F904BA726E01F3DABF4AB01EB112C0F2CCEC24586E256A53A60DB826EFDF52F36670DB1001C955627AE380B5221C5D30C11A214CF56229653C21D0C7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c1-onenote-15.cdn.office.net/o/s/161351641006_App_Scripts/oreolazylegacy.js
Preview:	/*! Copyright (C) Microsoft Corporation. All rights reserved. */.(window.webpackJsonporeo_name_=window.webpackJsonporeo_name_||[]).push([[2],{536:function(e,t,n){"use strict";n.d(t,"a",(function(){return s})),n.d(t,"b",(function(){return f}));var o=n(2),i=n(0),r=["setState","render","componentWillMount","UNSAFE_componentWillMount","componentDidMount","componentWillReceiveProps","UNSAFE_componentWillReceiveProps","shouldComponentUpdate","componentWillUpdate","getSnapshotBeforeUpdate","UNSAFE_componentWillUpdate","componentDidUpdate","componentWillUnmount"];var s,a=function(e){function t(t){var n=e.call(this,t)||this;return n._updateComposedComponentRef=n._updateComposedComponentRef.bind(n),n}return Object(o.c)(t,e),t.prototype._updateComposedComponentRef=function(e){var t;this._composedComponentInstance=e,e?this._hoisted=function(e,t,n){void 0===n&&(n=r);var o=[],i=function(i){"function"!=typeof t[i]||void 0!==e[i]||n&&-1!==n.indexOf(i)||(o.push(i),e[i]=function(){for(var e=[],n=0;n<arg

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\oreonavpanelegacy[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):	491772
Entropy (8bit):	5.5347401914048735
Encrypted:	false
SSDEEP:	6144:TaM6xCS8y5W/kGSwKaOjwExmry399GAc+Gg2CsaGemiyfvml2V:uoy3PQJ3
MD5:	1A33CE7DDA18C77C5ABA1F3E20406593
SHA1:	008BDC2BF336160E03C9F7636557582774514EFB
SHA-256:	ECFC668DC189B7329E6A253C57FEF7E648457F41141D3235978D4DAE9F719F29
SHA-512:	189465ADA9680EDA37DD8152F8565D0B452717E5A598A79B3006E8A9A86733FD89B479E678DF2BFEC9C82413FC88934D0CE25BDE04ADDCA5C129F8D693ADBB3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c1-onenote-15.cdn.office.net/o/s/161351641006_App_Scripts/oreonavpanelegacy.js
Preview:	/*! Copyright (C) Microsoft Corporation. All rights reserved. */.(window.webpackJsonporeo_name_=window.webpackJsonporeo_name_||[]).push([[3],{532:function(e,t,n){"use strict";n.d(t,"a",(function(){return s}));var o=n(86),r=n(541),i=new o.a("Oreo.Navpane."),a={AddNotebookButtonText:"Add notebook",AriaNewNotebookButtonLabel:"New notebook",AriaNotebookLabel:"Click to view other notebooks.",AriaNavOptionsLabel:"Navigation pane settings. Select to choose navigation pane view settings.",AriaShowAllLabel:"Show Navigation Panes. Select this option to show the navigation panes",AriaShowSectionsAndPagesLabel:"Show Sections and Pages. Select this option to show Sections and Pages",AriaShowOnlyPagesLabel:"Show only pages. Select this option to only show pages",AriaHideAllLabel:"Hide Navigation Panes. Select this option to hide the navigation panes",NavOptionsTooltip:"Navigation Pane view options",NewNotebookButtonText:"Notebook",NewNotebookDialogTitle:"Create New Notebook",NewNotebookTextFieldLabe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\osfruntime_strings[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):	9113
Entropy (8bit):	4.967273648043953
Encrypted:	false
SSDEEP:	192:cHGdGchIoF8yj9fsUbZ3pNiRjoasminAfzGAlVMsIHbLi+Jzpiiih2ZHWzAHDLAa:Ftlp3AQfLcph2Z2m4RhYhvKufLmnJxi3
MD5:	45912587E1C40C6266F492158AE5DAAF
SHA1:	FA7DD43C3A5D2AC29C83D5ED0D63DF6A39838919
SHA-256:	C589CEAEF21B8959E1344D41E227A8AB105CA859035003D145DEFF0CE7A2CB01
SHA-512:	6E298FCBAA60935503B4E9F2E98A1C738537E772E54A6B5252C239DD1C464EBCCDC0171ECF5F8CFA7AAA739A1C698D336EAA4CF1BC0094E6C005D5FF02711C3E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c1-onenote-15.cdn.office.net/o/s/161351641006_App_Scripts/1033/osfruntime_strings.js
Preview:	Type.registerNamespace("Strings");Strings.OsfRuntime=function(){};Strings.OsfRuntime.registerClass("Strings.OsfRuntime");Strings.OsfRuntime.L_AgaveLicenseNotAquired_ERR='Click "Buy" to purchase this add-in.';Strings.OsfRuntime.L_SignInButton_TXT="Sign in";Strings.OsfRuntime.L_AppsDisabled_WRN="Office Add-ins are disabled";Strings.OsfRuntime.L_EnableAppsButton_TXT_FirstParty="Enable this feature";Strings.OsfRuntime.L_AgaveServerConnectionFailed_ERR_FirstParty="We couldn't connect to the catalog server for this feature.";Strings.OsfRuntime.L_AgaveWarningTitle_TXT="Add-in Warning";Strings.OsfRuntime.L_TrustButton_TXT="Trust this add-in";Strings.OsfRuntime.L_AgaveManifestRetrieve_ERR_FirstParty="We couldn't get the information needed to start this feature.";Strings.OsfRuntime.L_InfobarIconSecInfoAccessibleName_TXT="Security information";Strings.OsfRuntime.L_AgaveManifestError_ERR_FirstParty="Sorry, but we can't start this feature because it isn't set up properly.";Strings.OsfRuntime.L_Agav

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\otelFull.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	112776
Entropy (8bit):	5.361705652707183
Encrypted:	false
SSDEEP:	1536:d64Vo7kCXxzKh0AUU1LYvt7VQ2IHJ29ng4CE/RZcZT2+hAVHoh:PVo7/xzKhuV7SBHmjR1+hDh

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\otelFull.min[1].js	
MD5:	64C23FFEB1719AB23400701261147F0B
SHA1:	A7F6CE80A5AEE6B2E0702C6FF93442F5D05EED7E
SHA-256:	D842880879BCE1934CA91B4E6AF5350A07A25CFA702D9A48A4B3DD719CF26933
SHA-512:	D72F4A73D07B9678B7231AB06457B782822047FB81C875AF7F7B3F738D9D98B9FED637C8839FCFFA008F0C369164A480039DAD394BF01D930D189CB7F9E791DE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c1-onenote-15.cdn.office.net/o/s/161351641006_App_Scripts/otelFull.min.js
Preview:	var otelFull=function(e){var t={};function n(r){if(t[r])return t[r].exports;var i=t[r]={i:r,l:!1,exports:{}};return e[r].call(i.exports,i,i.exports,n),i.l=!0,i.exports}return 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 i in e)n.d(r,i,function(t){return e[t]}.bind(null,i));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="",n(n.s=9)}([,,,function(e,t){var n="undefined"!=typeof crypto&&crypto.getRandomVa

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\oteljs_agave[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):	73678
Entropy (8bit):	5.345301149748092
Encrypted:	false
SSDEEP:	768:2mEAABhINqfFi3U+BBZ9rbov8krznXSCaMIRF+b+hNH8IBYLd9+yerrHg6ksYcI0:sBhPfQ3pBBZ9nTHQB4XjUQeoSGfUk
MD5:	7DA5297CA907FBC4FE756D57F406BBDA
SHA1:	74498EB25106A81615CDC1F20A6425B4A369025C
SHA-256:	008E5AB80D0E3BB08A630824E563FF973F31926F7301743AC95A16CAC9A1E5B2
SHA-512:	B8B6982340FE4E239F4D95176FF6D1ED69089410695533BCF77EA28256BA7501D31F301AC97C5D58349018879C2D08C4435D526F47080C964F0AFB40CF53661B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://appsforoffice.microsoft.com/lib/1.1/hosted/telemetry/oteljs_agave.js
Preview:	var oteljs_agave=function(e){var t={};function n(i){if(t[i])return t[i].exports;var r=t[i]={i:i,l:!1,exports:{}};return e[i].call(r.exports,r,r.exports,n),r.l=!0,r.exports}return n.m=e,n.c=t,n.d=function(e,t,i){n.o(e,t)||Object.defineProperty(e,t,{enumerable:!0,get:i})},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 i=Object.create(null);if(n.r(i),Object.defineProperty(i,"default",{enumerable:!0,value:e}),2&t&&"string"!=typeof e)for(var r in e)n.d(i,r,function(t){return e[t]}.bind(null,r));return i},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="",n(n.s=31)}([function(e,t,n){"use strict";Object.defineProperty(t,"__esModule

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\ping[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	4
Entropy (8bit):	1.5
Encrypted:	false
SSDEEP:	3:N:N
MD5:	72054D9A6FBDCC7DF012E19F32345B65
SHA1:	52DD4C74C813DB3790179C4F236CEADACA3467A8
SHA-256:	C48B5B1A9776C84602DE2306D7903A7241158A5077E7A8519AF75C33441B8334
SHA-512:	5305BACDFD7C9BB525FF6C40D3FFA23C3F82EB5268CE3037DC353FA1A043AE31B239EED46DB0FB043D61C55D57B97C5F00C308F92456C51C44069F23FDA4037
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://browser.events.data.microsoft.com/ping
Preview:	"ok"

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\require-a19851d1[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):	23828
Entropy (8bit):	5.204345384621181
Encrypted:	false
SSDEEP:	384:m2uyhTTumu7iOYY0QPepWDqFZWo/tSGt8EDVvHlei1gNuXIcHGyNMdgYYxD:pu4siPvQPepWDqFZWo/tSBEDZFEuzHGa
MD5:	DF4E0D1890C3BF6CCD06ADDF5FDD3F9A
SHA1:	2466FF461C68832CD78D82FA79435B8896845D83
SHA-256:	903FEC3EEE9FF3FB95C52B94AE0E0579A471B9E4795C4C3238F8FD8D5B36DC21

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\require-a19851d1[1].js	
SHA-512:	9AB0416E984E36BFC7B7160B1E65D51ABA5B40239B90B36E371445F3D3EB80BF25F70AEC6CDA6D8C6973C35A586F9685F603FD196E30EAE4B3BBEB69872B6E0
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://spoprod-a.akamaihd.net/files/odsp-next-prod_2018-11-02-sts_20181108.001/require-a19851d1.js
Preview:	!function(e,t){"object"==typeof exports&&"undefined"!=typeof module?module.exports=t():"function"==typeof define&&define.amd?define(t):e.ES6Promise=t()}(this,function(){"use strict";function c(e){return"function"==typeof e}function t(){var e=setTimeout;return function(){return e(r,1)}}function r(){for(var e=0;e<w;e+=2){(0,j[e])(j[e+1]),j[e]=void 0,j[e+1]=void 0}w=0}function a(e,t){var r=this,i=new this.constructor(s);void 0===i[T]&&b(i);var n=r._state;if(n){var o=arguments[n-1];_(function(){return v(n,i,o,r._result)})}else m(r,i,e,t);return i}function u(e){if(e&&"object"==typeof e&&e.constructor===this)return e;var t=new this(s);return p(t,e),t}function s(){}function f(e){try{return e.then}catch(e){return N.error=e,N}}function l(e,t,r){t.constructor===e.constructor&&r===a&&t.constructor.resolve===u?(o=e,(s=t)._state===C?d(o,s._result):s._state===D?h(o,s._result):m(s,void 0,function(e){return p(o,e)},function(e){return h(o,e)})):r===N?(h(e,N.error),N.error=null):void 0===r?d(e,t):c(r)?(

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\require[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	17672
Entropy (8bit):	5.233316811547578
Encrypted:	false
SSDEEP:	384:lpLsOooX8uvFBiRh+HnEDuvvy1pqvuvDX/0ohHK9mm+tMHvVOPoQeOMmuI:QnoX8uNB2YHnEDsvy1pqvub/0iq4NMHM
MD5:	6EFDDF589864D2E146A55C01C6764A35
SHA1:	EFA8BBA46CB97877EEC5430C43F0AC32585B6B2F
SHA-256:	2D92F0CE8491D2F9A27EA16D261A15089C4A9BE879D1EEDCB6F4A3859E7F1999
SHA-512:	1AFC735660AAE010C04EF89C732D08EBA1B87BE6048164F273BEAEBECA3F30062812B4CD141DDF0291A6AB54F730875D597678A3564C0EED2AAC11E5400F951A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.sharepointonline.com/bld/_layouts/15/16.0.8231.1219/require.js
Preview:	/** vim: et:ts=4:sw=4:sts=4. * @license RequireJS 2.1.22 Copyright (c) 2010-2015, The Dojo Foundation All Rights Reserved.. * Available via the MIT or new BSD license.. * see: http://github.com/jrburke/requirejs for details. */.var requirejs,require,define;!function(global){function isFunction(e){return"[object Function]"===ostring.call(e)}function isArray(e){return"[object Array]"===ostring.call(e)}function each(e,t){if(e){var r;for(r=0;r<e.length&&(!e[r]||!t(e[r],r,e));r+=1);}}function eachReverse(e,t){if(e){var r;for(r=e.length-1;r>-1&&(!e[r]||!t(e[r],r,e));r-=1);}}function hasProp(e,t){return hasOwn.call(e,t)}function getOwn(e,t){return hasProp(e,t)&&e[t]}function eachProp(e,t){var r;for(r in e)if(hasProp(e,r)&&t(e[r],r))break}function mixin(e,t,r,i){return t&&eachProp(t,function(t,n){(r||!hasProp(e,n))&&(!i||"object"!=typeof t||!t||isArray(t)||isFunction(t)||t instanceof RegExp?e[n]=t:(e[n]||(e[n]={}),mixin(e[n],t,r,i))})},e}function bind(e,t){return function(){return t.apply(e,ar

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\spoguestaccess-f1ac83f1[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	113639
Entropy (8bit):	5.3336312735682485
Encrypted:	false
SSDEEP:	1536:bXGxg/LiufTH206/VT43jt/Vq3RZBDhuDaCYLs5xkhMaK3ArS0q:rG0LnrGxaasNX
MD5:	F1AC83F1407CFDF6C25C1F5556C00BC7
SHA1:	77EF032D27E6D02A75152993E463D073469148A8
SHA-256:	3ED3DCF13D073B36625EFCCEC1AB6E960E5A187F43945475C0972F7FDB82290A
SHA-512:	45CA2F9FDB41FF28953EF1F18027447B0C14819864AC061B56CFC712093F24DB0EBFD040560A529C46112D30A54CC282EEC796980773108FA286C8A8CE57605E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://spoprod-a.akamaihd.net/files/odsp-next-prod_2018-11-02-sts_20181108.001/spoguestaccess-f1ac83f1.js
Preview:	define("odsp-next/roots/SPOGuestAccess",["require","exports","@uifabric/file-type-icons/lib/initializeFileTypeIcons","@uifabric/file-type-icons/lib/getFileTypeIconProps","@uifabric/styling/lib/utilities/icons"],function(e,t){"use strict";Object.defineProperty(t,"__esModule",{value:!0})});define("@uifabric/file-type-icons/lib/initializeFileTypeIcons",["require","exports","react","@uifabric/styling","./FileTypeIconMap"],function(e,t,o,s,a){"use strict";Object.defineProperty(t,"__esModule",{value:!0});var l="_png",u="_svg",r=[16,20,32,40,48,64,96],c="?refresh1";t.initializeFileTypeIcons=function(t,n){void 0===t&&(t="https://spoprod-a.akamaihd.net/files/fabric/assets/item-types/");r.forEach(function(e){!function(t,n,e){var r=Object.keys(a.FileTypeIconMap),i={};r.forEach(function(e){i[e+n+l]=o.createElement("img",{src:t+n+"/"+e+".png"+c});i[e+n+u]=o.createElement("img",{src:t+n+"/"+e+".svg"+c});if(20!==n){i[e+n+"_1.5x"+l]=o.createElement("img",{src:t+n+"_1.5x/"+e+".png"+c,height:"100%",widt

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\wac0-82320d2a[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):	15653
Entropy (8bit):	5.384833486091678
Encrypted:	false
SSDEEP:	384:ZfWQ2UX5rZt5rL/qL7CVXRhexQ4NPLD4zlaAPizNrs82:kEPeS9PEDwlaAP2Nro
MD5:	82320D2AF741B525DF0C7498E0C5EE1C
SHA1:	375C8F4FA54C41DAA06A1F76D4A1A4EE2C4B208E

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\wac0-82320d2a[1].js	
SHA-256:	F63E4709CAFC3D0CD899FA68337DD796247B2A43861C0763047C4B6E16961C44
SHA-512:	37D021B175860DE7F54EA9DADBBEB6A6BF467AF5EB56F4FFA84B51C502323DB704BE0EC9BF20A993DA1FB03798F353F4D8B211A02E9CA247BE46DC15A9DAF4D5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://spoprod-a.akamaihd.net/files/onedrive-website-release-prod_master_20200814.002/wac0-82320d2a.js
Preview:	define("debug",[],function(){}),define("lightobject",[],function(){!function(){var w=window,_object=w.Object,_array=w.Array,_jsonDefined="undefined"!=typeof JSON;if(_object.create||(_object.create=function(e){function t(){}return t.prototype=e,new t}),_object.keys||(_object.keys=function(e){var t=[];for(var n in e)_object.prototype.hasOwnProperty.call(e,n)&&t.push(n);return t}),_object.isString||(_object.isString=function(e){return"string"==typeof e||e&&e.constructor===String}),_object.isArray||(_object.isArray=function(e){return e&&"[object Array]"===Object.prototype.toString.call(e)}),_array.isArray||(_array.isArray=function(e){return e&&"[object Array]"===Object.prototype.toString.call(e)}),_object.isFunction||(_object.isFunction=function(e){return"function"==typeof e}),_object.isObject||(_object.isObject=function(e){return e&&"object"==typeof e}),_object.isBoolean||(_object.isBoolean=function(e){return"boolean"==typeof e||e&&e.constructor===Boolean}),_object.isNumber||(_object.isNu

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\wac1-cdc297b4[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	47711
Entropy (8bit):	5.198357151474762
Encrypted:	false
SSDEEP:	768:SKJSTPFQF5Fflaid1Hp7p3M6OsodVrse7VWz45yMAdoyekllgwr3Bp9Ej70L2fGR:juPq7Vlaw1Hp7p39OsodVH7Vg4QMAdo0
MD5:	CDC297B451DBB9E8EEA693C529C28ECB
SHA1:	B651A9DAF2393832A834B0C33B2F910C38DC27B0
SHA-256:	B323D86681653D7E2E92716F79F18A324B1337DD9AD3D456644CA9FB7493FFA3
SHA-512:	4248EF437B7E4099796E79E4CB99E6D5D1C4642A8E16A7415ED7D79C93B9526D7963CF1EEDD498F50E03491A2A4F9EFDF02E1F5FC4D21E14414EF23700777402
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://spoprod-a.akamaihd.net/files/onedrive-website-release-prod_master_20200814.002/wac1-cdc297b4.js
Preview:	define("defineutilities",[],function(){!function(){function e(e,t,n){if(e[t]){var i=e.__appendedFunctions=e.__appendedFunctions||{};if(i[t])i[t].push(n);else{i[t]=[];i[t].push(e[t]),i[t].push(n),e[t]=function(){for(var e=this.__appendedFunctions[t],n=0;n<e.length;n++)e[n].apply(this,arguments)}}}else e[t]=n}function t(n,i,r){for(var a in i)i.hasOwnProperty(a)&&("initialize"!==a&&"dispose"!==a||r?r&&n[a]?t(n[a],i[a],r):n[a]=i[a]:e(n,a,i[a]));return n}function n(e){var t={};for(var n in e)if(e.hasOwnProperty(n)){var i=e[n];i&&"[object Array]"===Object.prototype.toString.call(i)?t[n]=i.slice(0):t[n]=i}return t}var i=1;t(window,{getId:function(e){var t;return e?(e.__id||(e.__id=String(i++)),t=e.__id):t=String(i++),t},getKey:function(e){var t;return e&&(e.key||(e.key=getId(e)),t=e.key),t},defineNamespace:function(e,n,i,r){for(var a=e.split("."),s=i||window,o=0;o<a.length-1;o++)s=s[a[o]]=s[a[o]]||{};var l=a[a.length-1];return s[l]?t(s[l],n,r):s[l]=n,l},defineClass:function(e,n,i,r){var a=n.p

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\wac2-34e3e925[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):	318185
Entropy (8bit):	5.479652130179025
Encrypted:	false
SSDEEP:	6144:0mzOnKQHhpesR7txGH6HvvU4rm+ae40ADwBUZZb:0EOnKUvvU/+ae40ywg1
MD5:	34E3E9258C00F66C4C342416287C76B6
SHA1:	4F4DB5EE3E22F1BC0D98BE29464D0AE984C0DE52
SHA-256:	2351DD8BFCD6CDD2B5C106E48A086C19167EC3241222F3900A5BCD3D397B1C0B
SHA-512:	535D6C46D5B9D58F6B3C8CF08B42090FAB456DE0E7F7E869646670995C8D3B8D9661879A2B011E152EBFEC43CA0337967E167B9A083EC5ED3B55278AFB9488D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://spoprod-a.akamaihd.net/files/onedrive-website-release-prod_master_20200814.002/wac2-34e3e925.js
Preview:	define("registernamespace",[],function(){!function(){function e(e){for(var n=0,r=arguments.length;r>n;n++)for(var i=this,o=arguments[n].split("."),a=0,s=o.length;s>a;a++){var c=o[a],l=i[c];l||(l=i[c]={}),i.__namespace||(0===a&&"Sys"!==arguments[n]&&(t.Sys.__rootNamespaces[Sys.__rootNamespaces.length]=l),l.__namespace=!0,l.__typeName=o.slice(0,a+1).join("."),l.getName=function(){return this.__typeName}),i=l}return i}var t=window;t.registerNamespace=e,e("Sys"),t.Sys.__rootNamespaces||(t.Sys.__rootNamespaces=[t.Sys])}()}),define("dependancies",["jquery-1.7.2","debug","validateconfig"],function(){!function(e){var t,n=window;n.Debug;t=n.wLive?n.wLive:n.wLive={},t.Core={},t.Controls={};var r=n.$Config;if(r.handlerBaseUrl=r.handlerBaseUrl||"",!r.sd){var i=document.domain,o=i.split(".");r.sd=1===o.length?"":"."+o[o.length-2]+".com"}r.mkt=r.mkt||"na",r.prop=r.prop||"X","undefined"!=typeof window.SymRealWinOpen&&(window.open=window.SymRealWinOpen)}(window.originaljQuery||jQuery)}),define("trunca

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\36796050726[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	TrueType Font data, 19 tables, 1st "GDEF", 50 names, Unicode, \251 2018 Microsoft Corporation. All Rights Reserved.
Category:	downloaded
Size (bytes):	1364920
Entropy (8bit):	6.583606734987835
Encrypted:	false
SSDEEP:	24576:rbiTlANREKFCTRElRNa/GzH61ZI5U8cB2YLUFG6nI75P:ywBheZI5/YLgnII
MD5:	CCAE5A3CBE37C4F3CFBC3F98E0B93F36

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\36796050726[1]	
SHA1:	6E6B66DC5C85BFC387D3DA5F4ED4FB84D6CC4876
SHA-256:	5802737795E427EDEF6224D56CF32F9641F938ADF6C919DC829CE4F748D9AFAB
SHA-512:	CAFC382B050EBFE92CD8A3D5EFB44137690BADF2EB4A1444F08B09DFF646FCB9B0F7AD882CBAB658B6AF46BE14137CEE0355CDFDDB7A0EF6BCA726C68FD5 5D6E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fs.microsoft.com/fs/4.9/rawguids/36796050726
Preview:	.....0GDEF.'.....GPOSn.):.....tGSUB..''...D..6.OS/2._5.....`cmaph1A...l(..3.cvt ?.P.....fpgmp..}.....gasp.#.#.....glyfb.....].head...1...<...6hhea...3...t...$hmt xJ.....j.kernt]pW..t...0.loca.....l..j.maxp...N..... meta..O...X...`name..+I.....2.post...h..... prep..I1.....5.2&..._.<.....p.....x.....x.....% ...../.f.....).,.....3.....3.....*...${.....MS .....& ....(...(...(...(...(...(...(...(...(.....H...H.k.H.k.H.k.H.k.H.k.H.k.....!...!.....H .....J...L...o...d.....e...e...e...e...e.....>.).....B...)...3...$...Q...H...x.....,t.....Z...Z...Z...m. .M.....<.n.<.n.<.n.<.n.<.n.<.n.<.n.<.n.<.n. <.n...n.....T.n.B...B...B.F.B.....L...L.....L...L.....o.(

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\44327025345[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	TrueType Font data, 21 tables, 1st "EBDT", name offset 0x108c90
Category:	downloaded
Size (bytes):	1564532
Entropy (8bit):	6.750207541248198
Encrypted:	false
SSDEEP:	24576:zQCOg+DmUVv0XPSP7ZhtoFN8PFt/nq3JPj481BlS7GM5ShhAoG:J+/vbP7ZhtAkY48HlS7GQShha
MD5:	B83DB46379A90931DBCEC27E30D37C0D
SHA1:	5B0730CDEE0410861CFCF52B08DEE774CBDE25A4
SHA-256:	1522F5C0F14D035C42540D84AD4D00D92B72240E91784C15C59E12921A1F0D79
SHA-512:	B2999BD4BA88D69827F58A5D322BBF8F4A055834477011577E204E1E38A30F2AD2CE846295F03CC64309B79100EE20C4EDDD847B19135B4D2D8D9907EA471B1E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fs.microsoft.com/fs/4.9/rawguids/44327025345
Preview:	.....PEBDT19.....8..O.EBLC|5o.....GDEF...T..#.....GPOS..A...*.....GSUB.4.8.....).OS/2..6.....`cmapph.K..j...3.cvt .p.5.....fpgm~..7.....+gasp...#...(....glyf.d....>.....hea d.....\...6hhea...5.....$hmtxv.N....8..hjkern7..Q.....q.loca...r...X..hpmaxp-..... meta..O.....`name.....1xpost..... prep.g".....$.....5.%._.<.....|.....z.....6... .....:...../.....6.5.....+.....3.....3.....*...${.....MS .@.....& ....#...#...#...#...#...#...#...#...#...#..... ..Z...D.a.D.a.D.a.D.a.D.a.D.a.....E.....F...F...c..._.....[...[...[...[...[.....@. .....J...(...9...1...P...O...{.....'.....(...(...]...]...b...]...p...^.....*...*...*...*...*...*... ....L.c.L.c.L.c.L.c.L.c.L.c.L.c.L.c.O.c.O.c...c."..."...b.c.X...X...X.S.X.....G...G.....G...G....."..."...".."..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\OneNote[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	2864113
Entropy (8bit):	5.614825309946695
Encrypted:	false
SSDEEP:	49152:lu+o+ZKu8ajNtP8/Z455jICNr5qRCCHnnewGyEJDH5WU39/CCVMzIQqaMeoYuJPQ:rWdR93CHnner/1y
MD5:	0986CD5AB5EB7637B4F401221A4C65B0
SHA1:	D057DCB8FB965ABD599E99F568FE9A39EFC95807
SHA-256:	1ABA417A40483E75506625AFAF94120BA78F25292E975B1E5065AC714054A80A
SHA-512:	206A7E1434855306526CF1451BE9D8DDA50FE67CC629F3338344AB6ADAAC01FA9858EC62D69E8A34208247A0DB89A9E4A2F56E549C20D913C279A45CD7197F3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c1-onenote-15.cdn.office.net/o/s/161351641006_App_Scripts/OneNote.js
Preview:	var wac_aaa=[];function wac_a(a){return function(){return wac_aaa[a].apply(this,arguments)}}"undefined"==typeof IEnumerable&&(IEnumerable=function(){},IEnumerab le.registerInterface("IEnumerable"));"undefined"==typeof IEnumerator&&(IEnumerator=function(){},IEnumerator.registerInterface("IEnumerator"));"undefined"==typeof Sys&&Type.registerNamespace("Sys");"undefined"==typeof Sys.Is&&(Sys.Is=function(){},Sys.Is.registerInterface("Sys.IEnumerable$1"));."undefined"==typeof Sys.nx&& (Sys.nx=function(){},Sys.nx.registerInterface("Sys.IEnumerator$1"));Type.registerNamespace("Diag");var wac_aa=window.Diag||{};function wac_baa(){}wac_baa.regi sterInterface("Diag.IUlsHost");wac_aa.vdb=function(){};wac_aa.vdb.prototype={};wac_aa.vdb.registerEnum("Diag.ULSTraceLevel",!1);function wac_ba(a,b,c,d,e,f,g,h) {this.idb=a;this.bJa=b;this.cB=c;this.zo=d;this.ur=e||"";this.kMa=f;this.q9a=g;this.Pp=h}wac_ba.prototype={idb:0,bJa:0,cB:0,zo:0,ur:null,kMa:0,q9a:!1,Pp:null};.function w ac_ca(a){wac_ca.initializeBase

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\OreoSlice1[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):	886985
Entropy (8bit):	5.437715647774208
Encrypted:	false
SSDEEP:	12288:rfG5BtLFTEBwfFlzcqnm1m47AGBqgDhnxgn8g:rOcIO73BqePg
MD5:	8206026EAB007B295AD91E4E116F8B93

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\OreoSlice1[1].js	
SHA1:	07AC2A66561D51431F69E49A7C014758E8627B89
SHA-256:	E8F405F1946D68D8648833D5916FBE0FC6ED1188019070424909F4912C0C045C
SHA-512:	655D267E182F6A79352B855C25D4531164D44D346956AA9B5C3F97BCD76E2EF1B96A004F7CACE1395334F7FB4858C1ABEB0D5E75206302EF389259CE1372E75F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c1-onenote-15.cdn.office.net/o/s/161351641006_App_Scripts/OreoSlice1.js
Preview:	/*! Copyright (C) Microsoft Corporation. All rights reserved. */.window.oreo_slice1=function(e){function t(t){for(var n,i,o=t[0],a=t[1],s=0,c=[];s<o.length;s++)i=o[s],Obj ect.prototype.hasOwnProperty.call(r,i)&&r[i]&&c.push(r[i][0]),r[i]=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={6:0};function i(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,i),r.l=!0,r.exports}i.e=function(e){var t=[],n=r[e];if(0!==n)if(n)t.pu sh(n[2]);else{var o=new Promise((function(t,i){n=r[e]=[t,i]}));t.push(n[2]=o);var a,s=document.createElement("script");s.charset="utf-8",s.timeout=120,i.nc&&s.setAttribut e("nonce",i.nc),s.src=function(e){return i.p+""+({0:"onenoteloadingspinner",1:"oreofab",2:"oreolazy",3:"oreonavpane",4:"oreonotebookpane",5:"oreosearchpane"}[e] ||e)+"legacy.js"}(e);var l=new Error;a=function(t){s.onerror=s.onload=null,clearTimeout(c);var n=r[e];if(0!==n){if(n){var i=t&&("l

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\Plt[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	downloaded
Size (bytes):	42
Entropy (8bit):	3.0241026136709444
Encrypted:	false
SSDEEP:	3:CUmExltxlNXE:JQ
MD5:	B4682377DDFBE4E7DABFDDB2E543E842
SHA1:	328E472721A93345801ED5533240EAC2D1F8498C
SHA-256:	6D8BA81D1B60A18707722A1F2B62DAD48A6ACCED95A1933F49A68B5016620B93
SHA-512:	202612457D9042FE853DAAB3DDCC1F0F960C5FFDBE8462FA435713E4D1D85FF0C3F197DAF8DBA15BDA9F5266D7E1F9ECAEEE045CBC156A4892D2F931FE6FA BB
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://onedrive.live.com/Handlers/Plt.mvc?bicild=&v=0.0.0
Preview:	GIF89a.....!.....,.....2.;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\ScriptResource[1].axd	
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):	26954
Entropy (8bit):	4.516288580103467
Encrypted:	false
SSDEEP:	384:EMgviMjM4if38GmhXeC1QRwweTkBE9wbOY4Jf/JhRZ5h+73hNVt8oC4veONhLYVi:ZLEiJSdo11vIYHqb5Klo8v
MD5:	3DBD97A205B8CE59D755AB94F8C42964
SHA1:	B0520226342BBA131160A510BA3B57A1E8B7B80C
SHA-256:	36F7B9FE80A026A5D933855DE494AC6B7A4D01A93C26CE8A8737EED0C79367F4
SHA-512:	82BE6F1015CC346811EB736BD78F4949C855E49F8B4CC8493B22AE0F8D329EFA34205599E1138E57D33302B8A7B76F085DED053530B0F79D0DC71E257C99D80D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://wonderwaterbeads.com/Stephanie/Drive/asd/ScriptResource.axd?d=P9Sp2kK_d4BNWXJEemNdILK9AkaZTG86MaHXVWE9ulLLVoOV2_uW1v0US-bX7dmgAnCfaQZZr5Xs_PMb2qlY_PZzJWUXIvFhdqwbDETknzEmfBkVtnOHt2UrW1fhYKSvnNu6LRTwvwsd5-_je6Walguw52MlxQXzYUZD9J954ItjszBMdOwHNUoRr-iIqIr00&t=545ba255
Preview:	.var Page_ValidationVer = "125";..var Page_IsValid = true;..var Page_BlockSubmit = false;..var Page_InvalidControlToBeFocused = null;..var Page_TextTypes = /^(t ext|password|file|search|tel|url|email|number|range|color|datetime|date|month|week|time|datetime-local)$/i;..function ValidatorUpdateDisplay(val) {.. if (typeof(val.display) == "string") {.. if (val.display == "None") {.. return;.. }.. if (val.display == "Dynamic") {.. val.style.display = val.isvalid ? "none" : "inline";.. return;.. }.. }.. if ((navigator.userAgent.indexOf("Mac") > -1) &&.. (navigator.userAgent.indexOf("MSIE") > -1)) {.. val.style.display = "inline";.. }.. va l.style.visibility = val.isvalid ? "hidden" : "visible";..}..function ValidatorUpdateIsValid() {.. Page_IsValid = AllValidatorsValid(Page_Validators);..}..function AllValidators Valid(validators) {.. if ((typeof(validators) != "undefined") && (validators != null)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\WebResource[1].axd	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	23063
Entropy (8bit):	4.7535440881548165
Encrypted:	false
SSDEEP:	384:GvUzYI+Vi4g1V5it1ONhA6w+Kv8i/4CYzLKL4DrLU0iTxZTAzIzrwDlTWMClQip9:bkON69kClQq8hDRJHp2tWU25Zt/gREVG
MD5:	90EA7274F19755002360945D54C2A0D7
SHA1:	647B5D8BF7D119A2C97895363A07A0C6EB8CD284
SHA-256:	40732E9DCFA704CF615E4691BB07AECFD1CC5E063220A46E4A7FF6560C77F5DB

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\WebResource[1].axd	
SHA-512:	7474667800FF52A0031029CC338F81E1586F237EB07A49183008C8EC44A8F67B37E5E896573F089A50283DF96A1C8F185E53D667741331B647894532669E2C07
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://wonderwaterbeads.com/Stephanie/Drive/asd/WebResource.axd?d=Vseh0_O29CS6SASZGjJ5B50eCxofIEK9mDd5NZNa5k8KtiJMrh6DL1CqUgbSMvuYp9XMuEXY1onzPRs6Z1nFvYLL4ESa9mSIGj7DzvVHhP41&t=636686402738678653
Preview:	function WebForm_PostBackOptions(eventTarget, eventArgument, validation, validationGroup, actionUrl, trackFocus, clientSubmit) {.. this.eventTarget = eventTarget;.. this.eventArgument = eventArgument;.. this.validation = validation;.. this.validationGroup = validationGroup;.. this.actionUrl = actionUrl;.. this.trackFocus = trackFocus;.. this.clientSubmit = clientSubmit;..}..function WebForm_DoPostBackWithOptions(options) {.. var validationResult = true;.. if (options.validation) {.. if (typeof(Page_ClientValidate) == 'function') {.. validationResult = Page_ClientValidate(options.validationGroup);.. }.. }.. if (validationResult) {.. if ((typeof(options.actionUrl) != "undefined") && (options.actionUrl != null) && (options.actionUrl.length > 0)) {.. theForm.action = options.actionUrl;.. }.. if (options.trackFocus) {.. var lastFocus = theForm.elements["__LASTFOCUS"];.. if ((typeo

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\agavedefaulticon96x96[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 96 x 96, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	1115
Entropy (8bit):	7.474905425501729
Encrypted:	false
SSDEEP:	24:OQkGe2gKOcQO9S80Axzhkzc7iFTZkqeNblj5ILlN0EFgFahPKN7FqP8:OQkRrTCbxzwSiZLCN52TFgM5KN7Fp
MD5:	084E7612635DFCF69A16255B41E70CAA
SHA1:	0D9721AA70B01487D3340B864C0BD49FB1D95206
SHA-256:	7B3897478186358CA6FE76F5E3226EDA36AF53D8F27526796BC975EBD440A395
SHA-512:	A0104DBB40429BCA5F54061CE6D36A695283D883CE1B732CA87A30743234D29BEBA07A0100DE0DE0B274A70C8C7C289574F6343DF16C3E4C7B6453F60E8737B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c1-onenote-15.cdn.office.net/o/s/1613516410006_resources/1033/agavedefaulticon96x96.png
Preview:	.PNG.....IHDR...`...`.....w8....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^.k.A.....@ .6.* ..H...R....V....l.! X..Z..Z..... X... .. .{.^fw...{.fv..70.~..|..... .. ..3.8.1q....(.&.....B.o.."w..Y.....]......~0N0....]..z....|.n.*....._..O...9..8@..K./..%..[..LQ.rm:.H.>...-..;,...9.G.n....`.{..-.F...'.?...y..]H..o{y..#.....]..x|...K.(x|p~.....r..R..~\.2.Y...f.Q..i...o...r.....Gc..Bp.Ol..\(...~.T..,....j.O.(e.....j(e. ...Z....Rf.....j(e. ...Z....Rf.....j(e.....D.,Y.....~..n.[.....PA....]....0.mK...sE.....J~}z[.!n...RV|.#.....7s.....)B.e;j2.....tX..k.....o.V....j.k3*A.....9..?R....Z....5t..j....f.Z.....E.L....J..7.}Uk.....H..i.Z...1...x$....]<l.....#ixw..h.h.h.a.4....9.&.v.....2i..D..l...'.-.+.._...eLZ...M..x..1%.g....'A..X.....jkK.^W.}.m...T....|...._^.[..~u'...mco.8...nT....d.m.l.b..M.4...s.U.;Yu...k.1|..93a..(M..2..U.....B..S..O.....c.....?)....iz.D...T.D!....R

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\appChrome.min[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):	617581
Entropy (8bit):	5.32993437203588
Encrypted:	false
SSDEEP:	6144:e1383NvnNd0oC35Bu32vRPGOcUh9tYkTYhWx2p+T4ZeUXVaU4U7x:e1389eBtN9tp0UxUR3VahI
MD5:	70D6EDF7611851F09BE24C8086FE570B
SHA1:	C49B93E709D447B25D1215105AE289C36457E186
SHA-256:	355589F1002202C42AB731D1EBBA719F6C0067A93E3F455415BEFBC93EA7E990
SHA-512:	6B0C44221FFD31F1E74B9BEF3FF697B71FABFD6BD931CB1E04D0F04B2E70609A3A4DDAF6E4A891B71C344C8059FCCA0C58496EAD4B57FA29FFAC06B562206052
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c1-onenote-15.cdn.office.net/o/s/1613516410006_App_Scripts/appChrome.min.js
Preview:	var appChrome=function(e){function t(t){for(var n,a,l=t[0],c=t[1],u=t[2],d=0,p=[];d<l.length;d++)a=l[d],r[a]&&p.push(r[a][0]),r[a]=0;for(n in c)Object.prototype.hasOwnProperty.call(c,n)&&(e[n]=c[n]);for(s&&s(t);p.length;)p.shift()();return i.push.apply(i,u||[]),o()}function o(){for(var e,t=0;t<i.length;t++){for(var o=i[t],n=!0,l=1;l<o.length;l++){var c=o[l];0!==r[c]&&(n=!1)}n&&(i.splice(t--,1),e=a(a.s=o[0]))}return e}var n={},r={4:0},i=[];function a(t){if(n[t])return n[t].exports;var o=n[t]={i:t,l:!1,exports:{}};return e[t].call(o.exports,o,o.exports,a),o.l=!0,o.exports}a.e=function(e){var t=[],o=r[e];if(0!==o)if(o)t.push(o[2]);else{var n=new Promise((function(t,n){o=r[e]=[t,n]}));t.push(o[2]=n);var i,l=document.createElement("script");l.charset="utf-8",l.timeout=120,a.nc&&l.setAttribute("nonce",a.nc),l.src=function(e){return a.p+""+({1:"common50",5:"appChromeLazy",6:"appIconsLazy",19:"uiFabricLazy",20:"uiSlice20"}[e]||e)+".min.js"}(e),0!==l.src.indexOf(window.location.origin+"/")&&(l.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\app[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF, LF line terminators
Category:	downloaded
Size (bytes):	262641
Entropy (8bit):	4.9463902181496096
Encrypted:	false
SSDEEP:	3072:u+Vd0pBbqPLYoyjFkxD2hAYwJb8ILm731Ss:u+Vd0DePLYoyjFkxD2hAYwJbZLM31Ss
MD5:	7C593B06759DB6D01614729D206738D6
SHA1:	0D4F76D10944933B8DDECFFE9691081439A77A3C

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\app[1].css	
SHA-256:	F7D9FB0479DE843CF3FB0B78FC56BBB9E30BF0A238C6F79D9209FA8B22EFB574
SHA-512:	EF91B610CF17A17AAFB48984B4403EF175EB86096E3F12E23AE8D4C7C96EF60ED14DA3F69721E095CD2ACE3F0A06190186D000992823814BB906F7FB3576C2C1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.onestore.ms/cdnfiles/external/oneui/oneui1.16.2/dist/css/app.css
Preview:	@font-face {. font-family: "wf_segoe-ui_normal";. src: url("//i.s-microsoft.com/fonts/segoe-ui/west-european/normal/latest.eot");. src: url("//i.s-microsoft.com/fonts/segoe-ui/west-european/normal/latest.eot?#iefix") format("embedded-opentype"), url("//i.s-microsoft.com/fonts/segoe-ui/west-european/normal/latest.woff") format("woff"), url("//i.s-microsoft.com/fonts/segoe-ui/west-european/normal/latest.ttf") format("truetype"), url("//i.s-microsoft.com/fonts/segoe-ui/west-european/normal/latest.svg#web") format("svg");. font-weight: normal;. font-style: normal; }..@font-face {. font-family: "wf_segoe-ui_light";. src: url("//i.s-microsoft.com/fonts/segoe-ui/west-european/light/latest.eot");. src: url("//i.s-microsoft.com/fonts/segoe-ui/west-european/light/latest.eot?#iefix") format("embedded-opentype"), url("//i.s-microsoft.com/fonts/segoe-ui/west-european/light/latest.woff") format("woff"), url("//i.s-microsoft.com/fonts/segoe-ui/west-european/light/latest.ttf") format("truetype

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\box42[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 222 x 204, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	6336
Entropy (8bit):	7.887073484659419
Encrypted:	false
SSDEEP:	192:wx46x27I7L8lRcTx3HCHBDA3B6VHj6V+Jcj:Ktv8lROx34ZA3B6VH+kO
MD5:	5D71229F6CA9EBFF5F7972F01B547C7C
SHA1:	4D71B33506E6F0EBA1C783DE37E36480F2E392BE
SHA-256:	ABC0FA95B72F082CF4FBB18267CDBD282F2909B65B1B479D7F339DB41769946E
SHA-512:	31915EB859D432D714CAA2DFF74B7E760DFFE3A672CD872EB8CF07EDDC3B544578640C315CD47802B34F4BF06B31D290C9CBEAB228BC1FA64BDAF36DC52323A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c1-onenote-15.cdn.office.net/o/s/161351641006_resources/1033/m2/box42.png
Preview:	.PNG.....IHDR.....y.'....IDATx^.....y.....)...5..MT....6./..f.m,@*.....W.A...o&..$.Q."7..... 0k.VdI..VL.`...w.k\|;...u....=.sf.~....s.9g/w..9.<.93..".H$]]..ttt..*....7g.ys.0}zg..3u....E.$C...G....\|'N...jk.f.....i..X0....X8....C...^;v..:..:.a.m....rz.x<..c..q..>..S...t.s....<...o..Cw.y.....<x...*....6e.....3..._..9H.f..}.._.....m.F.#.Wd...(.J.....\|yB....\|...+."O+.B.=..^.6-cK...\|./.t..m .f._...F.E.oum\..>.7l..l.<.f..[.Hm.ZFiC...-_..#....[.d..{.....Z.~dd.....t.../`S.^.z.....-....Gm...n....m..2...#n!%..Ci.j..t....7..M.....8t.....^..h..d..]a.....K....L.....x6\|6xM.s.M.../.]...=.....<4..l.....e.....>J1.....D.;w.\|..fY...x.....m....W.+...9.Q>S.l..J.U.f0..._Z..Y....._s.O..!.2....u&..zo.z.-..>S..p..... .....x=u..2.M.jGb..G9.V.<;d."x@...@.....c.f.p....5....ZQ..8].<^.)c..f(.W....[...^.....gCW&.$i...l.&x.0.~8..!.x.t../>.c..:.(..cN..]XD..-...gk{.gCW9....<.'.l... ..v.....<.....).

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\filescss1-11eb1969[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	86703
Entropy (8bit):	5.269017817764116
Encrypted:	false
SSDEEP:	1536:JYS6qxvJbU8zPImHvZtohtDq2ACa209sgqWboBdiyMUWC8ErpH/TVTDrwCG0mJn:P6qxfSy
MD5:	11EB1969D9AC9F1EFC77D65620A7ECC1
SHA1:	1A6A2E37E37086BDE5FBD0F415F27BA7E424323C
SHA-256:	BD88D1E741693AB877B020059B46BE7CF4EF62B46017B2489A8CD1BF9CE5B9FC
SHA-512:	0B4C9A46BB69FEC33B76C58BAF971018A21DEBE4B4EC3620BCA8BF63231EF656DE4CFFE84786352CAF8E1598E24E703ADA38FEE0E1DBE369B204A55353A10403
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://spoprod-a.akamaihd.net/files/onedrive-website-release-prod_master_20200814.002//filescss1-11eb1969.css
Preview:	.c_if img{visibility:hidden;-ms-interpolation-mode:bicubic}.is_c{vertical-align:middle}.IE_M7 .is_c,.IE_M8 .is_c{vertical-align:text-top;padding-top:0}.is_o{position:relative;display:inline-block;vertical-align:text-bottom}.IE_M6 .is_hc *{visibility:inherit}.IE_M6 .is_o{vertical-align:middle}.is_i{display:block;overflow:hidden;position:absolute;left:0;top:0}.IE_M6 .is_i{position:relative}.is_i img{position:absolute!important;display:block;vertical-align:baseline}.is_p{display:none}.FF_M2 .is_o{position:absolute;display:inline}.FF_M2 .is_p{margin-top:3px;visibility:hidden;display:inline}.wl_bubble{width:0;height:0}.wl_bub_content{position:absolute;z-index:200;top:0;left:0;margin:0;width:300px;overflow-x:hidden;min-height:50px;height:auto;border:2px solid #1A1A1A;background-color:#FCFCFC;word-wrap:break-word}.wl_bub_content p{margin:0}.wl_bub_bk_outline{position:absolute;border:10px solid;width:0;height:0}.wl_bub_bk_cover{position:absolute;border:8px solid;width:0;height:0}.wl_bub_html{p

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\filescss2-7859787f[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	173416
Entropy (8bit):	5.241907392452272
Encrypted:	false
SSDEEP:	3072:5Yug51Mu3QgnsU2k7acc4WRmT9V+d1rTrWDrwLrgIr/rbrHrhg+4ly:5Yug51Mu3QgsNa+d1rTrWDrwLrgIr/r7
MD5:	7859787F547559F309A1C3BAC15B1484
SHA1:	AF58B37C40546F0D73410E3169D83D9E797E51F4

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\filescss2-7859787f[1].css	
SHA-256:	85B57EAEE8F090113CA4EB0584C8E22F1E1A891EFBAC13B9251676EA5E968449
SHA-512:	2D1D9530A249D05C91515B234106273E3289B85B36E678680E20654904F037A1409B1FF95EE29304C52C94D8093A3D1BCD95EB0BFB6B664BCE5B9944CC4FDF1F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://spoprod-a.akamaihd.net/files/onedrive-website-release-prod_master_20200814.002//filescss2-7859787f.css
Preview:	div.cc2_main div.cc2_main_bk{z-index:10;position:relative;top:0;left:0;margin-left:8px}.rtl.IE div.cc2_main div.cc2_main_bk{zoom:1}div.cc2_main h3.cc2_hdr{padding-bottom:2px}div.cc2_main div.cc2_refc img,div.cc2_main span.cc2_addngext img{vertical-align:middle}div.cc2_main span.cc2_addngext{margin-left:4px;color:#000}div.cc2_main div.cc2_refc{margin-left:4px;margin-top:6px;margin-bottom:6px}div.cc2_main div.cc2_refc span.cc2_nmco{color:#666}div.cc2_main div.cc2_main_bk img{z-index:10;vertical-align:bottom}body.IE_M6 div.cc2_main div.cc2_main_bk{display:none}div.cc2_main div.cc2_main_cntn{background-color:#e8eff9;border:1px solid #c1defb;padding:4px;margin-top:-1px}body.IE_M6 div.cc2_main div.cc2_main_cntn{margin-top:-3px}div.cc2_main div.cc2_main_cntn div.cc2_cmt{padding:5px}div.cc2_main div.cc2_main_cntn div.cc2_txt{font-size:100%;color:#555;word-wrap:break-word;padding-top:3px}div.cc2_main div.cc2_main_cntn span.cc2_tsmain{color:#666;font-size:86%}div.cc2_main div.cc2_main_cntn div.c

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\icons[1].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), icons family
Category:	downloaded
Size (bytes):	4388
Entropy (8bit):	5.568378803379191
Encrypted:	false
SSDEEP:	96:2WZx42qACoApC6do8MPOGiN4mER38GTDfO/fv:1x42qAHAo6VMPi6mcTy
MD5:	77E1987DF3A0274C5A51E3C55CEE7C98
SHA1:	9B0FE96AF141AB09183F386F65BC627B8C396460
SHA-256:	EF04649D4D068673CF0FA47EF4C45C8BE291E703F4EC5FC0E507F17839120AA2
SHA-512:	B1E0CFB515FF2298799BA54574899D27B1FC043F66CC4E9591C504F88273B98697B99ED25955DB84986B39ED9F51864611833DC88064B14C29ADC020FBF6E295
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.onestore.ms/cdnfiles/external/oneui/oneui1.16.2/dist/fonts/icons/icons.eot?
Preview:	$.....LP.....G.....i.c.o.n.s.....R.e.g.u.l.a.r.....V.e.r.s.i.o.n. .1...0.....i.c.o.n.s..... OS/2@.Mn...(...Vcmap.1.....Jglyf.....dhead.9.....6hhea.$.....$hmtx@.....loca". h...L...Bmaxp.3.`..... name.....post{NK..... .....G..._.<.....|.....|..... .T.....D.I...H.D.I.....PfEd.@.....D.....(.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\jquery-1.7.2-39eeb07e[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):	94124
Entropy (8bit):	5.308749614691286
Encrypted:	false
SSDEEP:	1536:5IE3Hz9WAJ0A7W+pR5YghP4Crd+uhGJ0jxM+1AZx5g6yWf9qOmRaliJl1m9Yjq+H:t5Ygh4YGn+0m3qIX8kbP3V1v
MD5:	39EEB07E6802E2B57F5E10A9AD9BCA24
SHA1:	CD952A05FD3DA2945C372F5B9701F0145BF3C82F
SHA-256:	D6C15974B6181A68E9B74E4F38FBAC81D640569EF0FBBAA3381CC59683A9763F
SHA-512:	A40D9FCE6E49C4E3135395010BC86DF8CCB0A762512B6B315A60CFA8866DCF0A4E7237DDEA3B55880B2DFE69156AC4F4B1617AB74730B418F47130437ACE0F0 2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://spoprod-a.akamaihd.net/files/onedrive-website-release-prod_master_20200814.002/jquery-1.7.2-39eeb07e.js
Preview:	!function(e,t){function n(e){var t,n,r=O[e]={};for(e=e.split(/\s+/),t=0,n=e.length;n>t;t++)r[e[t]]=!0;return r}function r(e,n,r){if(r===t&&1===e.nodeType){var i="data-"+n.replace(q,"-$1").toLowerCase();if(r=e.getAttribute(i),"string"==typeof r){try{r="true"===r?!0:"false"===r?!1:"null"===r?null:H.isNumeric(r)?+r:P.test(r)?H.parseJSON(r):r}catch(o){}H.data(e,n,r)}else r=t}return r}function i(e){for(var t in e)if(("data"!==t||!H.isEmptyObject(e[t]))&&"toJSON"!==t)return!1;return!0}function o(e,t,n){var r=t+"defer",i=t+"queue",o=t+"mark",a=H._data(e,r);!a||"queue"!==n&&H._data(e,i)||"mark"!==n&&H._data(e,o)||setTimeout(function(){H._data(e,i)||H._data(e,o)||(H.removeData(e,r,!0),a.fire())},0)}function a(){return!1}function s(){return!0}function l(e){return!e||!e.parentNode||11===e.parentNode.nodeType}function u(e,t,n){if(t=t||0,H.isFunction(t))return H.grep(e,function(e,r){var i=!!t.call(e,r,e);return i===n});if(t.nodeType)return H.grep(e,function(e,r){return e===t===n});if("string"==type

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\latest[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 35900, version 0.0
Category:	downloaded
Size (bytes):	35900
Entropy (8bit):	7.989413276112553
Encrypted:	false
SSDEEP:	768:d1DM2UJJ9OKKukRdfijklR4f0Ki9NkmeWkujUkTl68TEG4sI:LD7RKKukRdfukKiDq3ITEl
MD5:	70C1D43A35B7A48D088D830EA07FCF77
SHA1:	025E0E281139C70C5538E09BFA7927141AF0CC0B

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\latest[1].woff	
SHA-256:	942E5DD2012006745O6B0DF50C1AFEF021FFF6D5BD7BB7F600DED8617DBCB386
SHA-512:	E40B2CEAA1F672891BFF21F7C22A8B473DCF998FDC0A74B3DD1999190BA281C330C871D4BC82F89561E2AD7D97FE3169F33748AD368184BD1B4850941822D92
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://i.s-microsoft.com/fonts/segoe-ui/west-european/semibold/latest.woff
Preview:	wOFF.....<.....OS/2...D...W...`K..rcmap.....<.cvt .....y....c.e0fpgm...,.....5.KV.gasp.....glyf.....sH.....$head...0...6...6....hhea...h...!...$...Jhmtx.. .....loca...L.....z.@maxp...H... ... .N.?name...h.....!MG$post...X..... .Q.wprep...l.....[...x.c`fie.``e.`..j...(.../2.1.q.2q.3..!.s...2.....+(.)..X/..d..X.....ca`.....1..e .x.e.}L.U..?..''e.\4.4..(8_R.#....MM.Z[[.%*....(& .Q...:G.ZF..2..{....i^n.ee..Vx...1...=...vv>....D.....:..'...t.z.....k....MP...S..|-.RU.VuNog..3.)r.;+.:.C.s.....w....'h.M..e.k2M..e. C.nz...n...Mq{.i.`w....g..8.....}..!..Gir5HC5B#.H..I=..U.rU.xR;..t.-....MO.j.7&.3..n.I.<.u...x......_&V..$..b3...o.....l...b...M...]..^=xv.^.7(....z...e..tT.&.1.:R..E.K....k!..UY.4.....P}. :8g..m?.....JT.;.....5....T.oS...z....&t[..M.y..~x..b.&.....d..J.d..j.u.f^.8.U.V..OZ....)N..3..z...|>.4.s..|.U.h....=fq.:..+.f6..+.P...1.bJ.1.R.1.....E,.g.y.%,.....eTY./.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\maincss-3d633429[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	139723
Entropy (8bit):	5.270500603578539
Encrypted:	false
SSDEEP:	1536:JYS6qxvJbU8zPImHvZtohtDq2ACa20eboBdiyMUWC8ErpH/TVTDrwCG0mJlkssg8:P6qxfB+
MD5:	3D633429D8E6291C54FF4705E0ABFF53
SHA1:	DB065DEB77642EBB6C282A65E9407DCFFF456500
SHA-256:	63AEF72D236CDE38C258F82E8797D13CB24CD903F01E83732EEDE839AA5CF2C5
SHA-512:	12E6126515C92F4C7644BDC77E64B147116DB04EAF7847E705E524FB537A10EC2246D1F6D5DC8D8D3A3EC94E31EC4DDC2400CDED13830C8871D5AAF8FF43D5B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://spoprod-a.akamaihd.net/files/onedrive-website-release-prod_master_20200814.002//maincss-3d633429.css
Preview:	.c_if img{visibility:hidden;-ms-interpolation-mode:bicubic}.is_c{vertical-align:middle}.IE_M7 .is_c,.IE_M8 .is_c{vertical-align:text-top;padding-top:0}.is_o{position:relative;display:inline-block;vertical-align:text-bottom}.IE_M6 .is_hc *{visibility:inherit}.IE_M6 .is_o{vertical-align:middle}.is_i{display:block;overflow:hidden;position:absolute;left:0;top:0}.IE_M6 .is_i{position:relative}.is_i img{position:absolute!important;display:block;vertical-align:baseline}.is_p{display:none}.FF_M2 .is_o{position:absolute;display:inline}.FF_M2 .is_p{margin-top:3px;visibility:hidden;display:inline}.wl_bubble{width:0;height:0}.wl_bub_content{position:absolute;z-index:200;top:0;left:0;margin:0;width:300px;overflow-x:hidden;min-height:50px;height:auto;border:2px solid #1A1A1A;background-color:#FCFCFC;word-wrap:break-word}.wl_bub_content p{margin:0}.wl_bub_bk_outline{position:absolute;border:10px solid;width:0;height:0}.wl_bub_bk_cover{position:absolute;border:8px solid;width:0;height:0}.wl_bub_html{p

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\microsoft-logo[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 226 x 48, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	3331
Entropy (8bit):	7.927896166439245
Encrypted:	false
SSDEEP:	96:zHjOKn3csE3x5liVsCo4GcPIZpV6x5cge8oo9:zDOK3zE3x5TCwcP4LQNeq
MD5:	EF884BDEDEF280DF97A4C5604058D8DB
SHA1:	6F04244B51AD2409659E267D308B97E09CE9062B
SHA-256:	825DE044D5AC6442A094FF95099F9F67E9249A8110A2FBD57128285776632ADB
SHA-512:	A083381C53070B65B3B8A7A7293D5D2674D2F6EC69C0E19748823D3FDD6F527E8D3D31D311CCEF8E26FC531770F101CDAF95F23ECC990DB405B5EF48B0C91B2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://wonderwaterbeads.com/Stephanie/Drive/images/microsoft-logo.png
Preview:	.PNG.....IHDR.....0.....sRGB.....IDATx..=w....G.z..L.4fN.k\dS..._`.....r...~.F..e._.RZ.0.K.\..CB...1.{qq/..^|.G..o.....?....Or.....y~....]..V.a.mM...M.\k*H..@B`s.$"n ...)!.@"b#4. !.9...7.u...hD ....T.....:EJ.4"..X.....<\|.pgkk+....>~.....pju1i"b.J.&!.!...=T....k..D7.....O.<.?}...../..(.`0..!.C..'.?..e..~.....l6...._.x1rmR...$|E...l.WKDH...f..... ...Y.0R... .>...{...-..o.....,...E../....._....eM.Q....@Q...w sp5.9..l.W)...Pq... .]..B..).../M.G.g....].V...5$<.....Eb.9.....>LYAk.Z.k..b..]N%>}4a....4!S...t..d..<.8AH+.../r...._...!qt.:q..fR.:.. KW._....T...5..>.0!.hq.rbND\...XR.,2.uX..Q.b...wQ.....g..X...F...~.....ikZE...UA....V.I!..]..Mm..R.....~k.VC.n..V.*B#W...\..yI.3.....2.....6c....2J....,g..5O1.s.4V2.....f..K..Obf\....;.w ...\.F>F>6_z..P.dU<.wVV.....?.q.?&.....O.>....l.S.upp....59.C_.....fJ.M.={v,.....]Y_....n.?UF....v<.$..AD...p.....:$r =p...C.k.3....n.v..~.TGd!...l.W...s..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\moe_status_icons[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 82 x 258, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	6140
Entropy (8bit):	7.86318803852975
Encrypted:	false
SSDEEP:	96:JCXCuvaxrUZXtOVVLMtSqdyZ7x5rY4gby5cR+YBaB7W+Nf9XF5Qfhl4/t5K:MMr7AtaZ7fY4f5l/qRf9V6hSl5K
MD5:	2443F04DFD8CE58264835F7CD477799C
SHA1:	E798EF676A42AA8F723246C95FA6A918010223B2

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\moe_status_icons[1].png	
SHA-256:	77DD1463FE34BE51528C6535C5AAF5590EE90BBD3B76AE8E362657C45E9F90FD
SHA-512:	2668E7EEFF653ECDEF04058FDC43328A80F297EE601839737F35A860737DAD438B03298C1A452E83DAED31DDDA540F7F065FE8F22FB05FC150A9FEAB08FFC91D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c1-onenote-15.cdn.office.net/o/s/161351641006_resources/1033/moe_status_icons.png
Preview:	.PNG.....IHDR...R.....m.....tEXtSoftware.Adobe ImageReadyq.e<...fiTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.0-c061 64.140949, 2010/12/07-10:57:01 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpMM:OriginalDocumentID="xmp.did:C714FB70438BE1119DF2F8ED1CCAF400" xmpMM:DocumentID="xmp.did:98155F5CD83911E1ACDEFDB8BE9BCEAA" xmpMM:InstanceID="xmp.iid:98155F5BD83911E1ACDEFDB8BE9BCEAA" xmp:CreatorTool="Adobe Photoshop CS5.1 Windows"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:09F73A8D39D8E111AE39EC2BD256A3F2" stRef:documentID="xmp.did:C714FB70438BE1119DF2F8ED1CCAF400"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>Y.[...,IDATx.....{....a.... .<c.....3.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\moeerrorux[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	10290
Entropy (8bit):	4.837717444305284
Encrypted:	false
SSDEEP:	192:iAY/Yye00RR2WxnYkSSWmcrKnmuV2UmHPRmCHpoRqiKaUVIv4DLhBA:w0RR2WxnYk5Wmw8ipo0Hu
MD5:	4DF9B0011F8AE623E26116BC635CFB36
SHA1:	0D68BBCB58D190F6E2803043A1823A3826325F33
SHA-256:	47D6DBDB766BD7EA675F68A5CE5A22654554001EFC7007A0B8C484069D9E2638
SHA-512:	3BD8C4FDCC43199DB8D4EA1E668495837AF3931EAD7EA4AC16D775D3FBDF3BC35833CF2DF86BE8492EDC82090A1ED2B79A4DC3233BC3FD064F7C46424B40345
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c1-onenote-15.cdn.office.net/o/s/161351641006_resources/1033/moeerrorux.css
Preview:	.moe-infobar-body {.. background-color:#FCF7B6;.. border:1px solid #D9D98B;.. position:relative;.. max-height:110px;.. overflow:hidden;.. white-space: normal;..}.....moe-infobar-body:hover {.. background-color:#FEF294;..}.....moe-hovered {.. background-color:#FEF294;..}.....moe-infobar-infotable {.. width:100%;.. height:100%;.. max-height:110px;..}.....moe-infobar-top-left-cell {.. width:30px;.. min-width:30px;.. max-width:30px;.. vertical-align:top;.. padding:1px; ..}.....moe-infobar-message-cell {.. padding:7px 7px 3px 0px;.. vertical-align:top;..}.....moe-infobar-top-right-cell {.. width:20px;.. min-width:20px;.. max-width:20px;.. vertical-align:top;..}.....moe-infobar-button-cell {.. padding:0px 10px 6px 0px;..}.....moe-status-warning-icon{.. position:absolute;.. clip:rect(0px 42px 41px 0px);.. top:0px;.. left:0px;.. .. ..}.....moe-status-warning-icon_ie{.. position:ab

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\officebrowserfeedback[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	17814
Entropy (8bit):	5.150364783549352
Encrypted:	false
SSDEEP:	192:FoUYg5vedZLnecWqBg57UBXmF6SDxKOkOFy37mwWmCOFmZYIqb:FyaC0cvS57UTSDx1kOFy37mwWmCZqb
MD5:	B7BB7EC93CFD3B25F2E2ADBBE38D346E
SHA1:	3638001DC2A15D7A98D0EDB8ABD7084C6ED896A6
SHA-256:	A4864530E8C21F08364BF52157AD1E3C297BF12EA7DA8E443E08F31AA55B03F5
SHA-512:	DE0553C5729844FEEE10383135403A6D0B6882BDEA6A1D77FB718BE858D5AB01079A787CC58BEFB8F972AC1C3363D8D97A3AC3A58E2029E72E28B91FEA2F08EA
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c1-officeapps-15.cdn.office.net/o/s/161351641006_App_Scripts/Feedback/latest/officebrowserfeedback.css
Preview:	.obf-ChoiceGroup{margin-bottom:8px}.obf-ChoiceGroup fieldset{margin:0;border:none;padding:0}.obf-ChoiceGroup legend{max-width:100%}.obf-ChoiceGroup input{position:absolute;opacity:0}.obf-ChoiceGroup input+label{display:block;display:grid;grid-template-columns:20px auto;cursor:pointer;margin:8px 6px 8px 6px}.obf-ChoiceGroup input:focus+label{outline:1px dashed black}.obf-ChoiceGroup input+label>.obf-ChoiceGroupLabel{display:inline-block;vertical-align:middle;margin:0px 0px 0px 10px}.obf-ChoiceGroup input[type=radio]+label>.obf-ChoiceGroupIcon{display:inline-block;content:'';border:1px solid #a6a6a6;width:20px;height:20px;border-radius:10px;vertical-align:middle;box-sizing:border-box;-webkit-transition-property:border-color;-moz-transition-property:border-color;-o-transition-property:border-color;transition-property:border-color;-webkit-transition-duration:.2s;-moz-transition-duration:.2s;-o-transition-duration:.2s;transition-duration:.2s;-webkit-transition-timing-function:cubic-bezier(0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\onenote-intl-mlr.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	109072
Entropy (8bit):	4.779766581298964
Encrypted:	false
SSDEEP:	768:XeGlNYKVK2HstacI+GAUa4ZHVxTujE7JwujFbiKBbklPfeZrC7tSGlxXX9Xa+7+H:XHDamsojDbvbklPkWty+7+4MS1m+E1

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\onenote-intl-mlr.min[1].js	
MD5:	D6B6D6D34531619C6695EA29312BA247
SHA1:	709F8154683D3655199D32325021B5D64418CE89
SHA-256:	05369EF9C6DE0110EA9C66476905C09E9BDD619DE14E1D55DE5EF87793410C78
SHA-512:	028906F8D259EF5DB50097386D56F8E2978D49D6523C1BEDB05E6F097ABD788CB9048F884F0A4A938D38E66901E80C9BAED4772353A38907C646CE2DC07C8D3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c1-onenote-15.cdn.office.net/o/s/161351641006_App_Scripts/1033/onenote-intl-mlr.min.js
Preview:	var OnenoteRibbonStrings={About:"About",AboutKeytip:"D",Accessibility:"Accessibility",AddInsKeytipPrefix:"Y",AdditionalControls:"Additional Controls",AlignLeft:"Align Left",AlignLeftKeytip:"AL",AlignRight:"Align Right",AlignRightKeytip:"AR",AudioTabTitle:"Record & Playback",AutoCorrectOptions:"AutoCorrect Options...",AutoCorrectOptionsKeytip:"AC",Automatic:"Automatic",AutomaticKeytip:"A",Back15Seconds:"Back 15 Seconds",Back15SecondsKeytip:"B",Bold:"Bold",BoldKeytip:"1",BrowseVersions:"Page Versions",BrowseVersionsKeytip:"V",BulletLibraryTitle:"Bullet Library",BulletStyle1:"Solid",BulletStyle1Keytip:"S",BulletStyle2:"Hollow",BulletStyle2Keytip:"H",BulletStyle3:"Square",BulletStyle3Keytip:"B",ButtonOfficeAddins:"Office Add-ins",CentimeterUnitPlaceholder:"{0} cm",ClearFormatting:"Clear Formatting",ClearFormattingKeytip:"E",ClearStyleFormattingKeytip:"C",Clipboard:"Clipboard",ClipboardKeytip:"C",Close:"Close",CloseMenu:"Close Menu",ContactSupport:"Contact Support",ContactSupportKeytip:"C",

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\onenote-ribbon-intl.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	168783
Entropy (8bit):	4.984168973294062
Encrypted:	false
SSDEEP:	3072:XjamBSnEfydIEw8GBsDvZZ5/b/zRuLqTw82BshXM1XM3ZxHAl:zJRyLZjZxgl
MD5:	F68DE4D318892D4B9400318665A457F3
SHA1:	445955AC03A79ACBD07CD5F9F9B28293C0F655DC
SHA-256:	391B335861E5C636843C7514BEF9A3D929D34A6C65371C6D5E5A71A2BE672FB6
SHA-512:	BBFD715E14A178CABD6974E504D3E1260FD4453EED5A543A10A41D286C0A597FC8E79B8AD6D8542A8E422DA3123D307F604BA17C45B4719A2A671CF42322820
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c1-onenote-15.cdn.office.net/o/s/161351641006_App_Scripts/1033/onenote-ribbon-intl.min.js
Preview:	var OnenoteRibbonStrings={About:"About",AboutKeytip:"D",Accessibility:"Accessibility",AddInsKeytipPrefix:"Y",AdditionalControls:"Additional Controls",AlignLeft:"Align Left",AlignLeftKeytip:"AL",AlignRight:"Align Right",AlignRightKeytip:"AR",AudioTabTitle:"Record & Playback",AutoCorrectOptions:"AutoCorrect Options...",AutoCorrectOptionsKeytip:"AC",Automatic:"Automatic",AutomaticKeytip:"A",Back15Seconds:"Back 15 Seconds",Back15SecondsKeytip:"B",Bold:"Bold",BoldKeytip:"1",BrowseVersions:"Page Versions",BrowseVersionsKeytip:"V",BulletLibraryTitle:"Bullet Library",BulletStyle1:"Solid",BulletStyle1Keytip:"S",BulletStyle2:"Hollow",BulletStyle2Keytip:"H",BulletStyle3:"Square",BulletStyle3Keytip:"B",ButtonOfficeAddins:"Office Add-ins",CentimeterUnitPlaceholder:"{0} cm",ClearFormatting:"Clear Formatting",ClearFormattingKeytip:"E",ClearStyleFormattingKeytip:"C",Clipboard:"Clipboard",ClipboardKeytip:"C",Close:"Close",CloseMenu:"Close Menu",ContactSupport:"Contact Support",ContactSupportKeytip:"C",

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\ppq8mv6lfjzaqwrntj9kw0pl[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):	39144
Entropy (8bit):	5.688320667561668
Encrypted:	false
SSDEEP:	768:8Ggg2GBKEXZDRAjcD0kQcPvKm6+Xsgc0Di2JHrsh1Ac8KWb:lgg1wjUvKm6+7VJHrK1AZKWb
MD5:	73DBC18E4084AF996284725C4F99DD73
SHA1:	A0B89369723295374CFC64AA5FEEB8D557992960
SHA-256:	227951C518660BBEDBF7B91FA2D8B9BB77089BD7056430E5F24D7058B1859B4F
SHA-512:	2304D5AF0E26BD9B9B63F4EA926CD17E6182835CFF860F7DE6459C0F03758F998E90243DE4E0101A5FF37947ED7545225C937C0582CE8D5C7EF18B9342FA1870
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_10, Description: Yara detected HtmlPhish_10, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\ppq8mv6lfjzaqwrntj9kw0pl[1].htm, Author: Joe Security
Reputation:	low
IE Cache URL:	http://https://wonderwaterbeads.com/Stephanie/Drive/ppq8mv6lfjzaqwrntj9kw0pl.php?8i6Hi81606398059128f968ba1612ccb0168b841d07c4251128f968ba1612ccb0168b841d07c4251128f968ba1612ccb0168b841d07c4251128f968ba1612ccb0168b841d07c41128f968ba1612ccb0168b841d07c4251&email=&error=
Preview:	.<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">.<html xmlns:o="urn:schemas-microsoft-com:office:office" lang="en-us" dir="ltr">.<head><meta name="GENERATOR" content="Microsoft SharePoint" /><meta http-equiv="Content-Type" content="text/html; charset=utf-8" /><meta http-equiv="Expires" content="0" /><meta name="Robots" content="NOHTMLINDEX" /><meta charset="UTF-8" /><meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1" /><meta http-equiv="X-UA-Compatible" content="IE=edge" /><link id="favicon" rel="shortcut icon" href="images/favicon.ico?rev=45" type="image/vnd.microsoft.icon" /><title>..Sharing Link Validation.</title>..<style type="text/css" media="screen, print, projection">...html{line-height:1.15;-ms-text-size-adjust:100%;-webkit-text-size-adjust:100%}body{margin:0}article,aside,footer,header,nav,section{display:block}h1{font-size:2em;margin:.67em 0}figcaption,figure,main{display:block}fig

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\progress[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 24 x 24

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\progress[1].gif	
Category:	downloaded
Size (bytes):	695
Entropy (8bit):	5.696679956038459
Encrypted:	false
SSDEEP:	12:HarRMs0pTestEsVEsl3Est3EshEsZ9NMzrI3TjEEofVcQ72TVkI3TjE:Har2nTeUEME23E+3EoEQ9NFj6kbjE
MD5:	648AD2F7EEA95A9B5491DCD2203B2F54
SHA1:	5FFA99938410AEBAB10B32308F242437B9432B53
SHA-256:	A3596C17DAD9A003D0BFBE0B7BA6765F51391B5C3943660316F01C8E77B323DB
SHA-512:	F7984FFEAEC122EFCBE36218979BB4C35E27007CC091BA5A8829BA5088999A3F9F7A7D5E11D90A05904D58644EC0B4E5EE1D57C68DD5270B7F456A762D8D699A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c1-onenote-15.cdn.office.net/o/s/161351641006_resources/1033/progress.gif
Preview:	GIF89a.....!..NETSCAPE2.0.....!.....,.....0.+.....H.....V..!.....,.....`..Q.!.....,.....`..Q.!.....,.....`..Q.!.....,.....`..Q.!.....,.....`..Q.!.....,.....`..Q.!.....,.....z...cr...!.....,.....dp.,.....H.....;..!.....,.....2.....dp.,...QP.Td.....F.[...v..?y....".....!.....,.....0.....dp.,...QP.Td.....gO:.....Q..!.....,.....*.....dp.,...QP.Td.....g.[.}.)..!.....,.....&.....dp.,...QP.Td.....>..!.....,.....#.....dp.,...QP.Td.....L.6V..!.....,.....dp.,.....H....;..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\redir[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	6938
Entropy (8bit):	5.591906799722691
Encrypted:	false
SSDEEP:	96:LyLqn3ziYf6l5nrcjoINElz1liGPt/bmPlty0FlO1++umUKLm:lvoBrcjoIoyGPtjmN0WmUKLm
MD5:	4D00C21DC31433601035F81D88D4741F
SHA1:	4749632CB0353D29B5613243406651899B1AA4F3
SHA-256:	8F6582AE926A504D292E3555D12E40FB49E30418284A168026E6AC8C37C0C62B
SHA-512:	44F4C46FAA8A266AD70B5760C377A89F3D12A8C0E47FFB2CD6E304425404CF66DCB520A4F2B7A0843865E305E35D4F1BBF8EDE85096F300F2257D52850BA85F2
Malicious:	false
Reputation:	low
Preview:	..<html>.. <head>.. <title>Microsoft OneDrive - Access files anywhere. Create docs with free Office Online.</title><meta name="title" content="Microsoft OneDrive - Access files anywhere. Create docs with free Office Online."/><meta name="description" content="Store photos and docs online. Access them from any PC, Mac or phone. Create and work together on Word, Excel or PowerPoint documents."/><meta property="og:title" content="Churches Fire Security Ltd"/><meta property="og:image" content="https://p.sfx.ms/icons/v2/Large/One.png"/><meta property="og:image:width" content="96"/><meta property="og:image:height" content="96"/><meta property="og:url" content="https://onedrive.live.com/redir?resid=E18A4FB0F2CDF48D!1033&authkey=!Akhvvv4zEZ5hGII&ithint=onenote%2c&page=view&e=94ZeN_PuoUemTbfJGTBFqw&at=9"/><meta property="og:description" content="Microsoft OneNote Notebook"/><meta property="twitter:site" content="@

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\shell.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	82190
Entropy (8bit):	5.036904170769404
Encrypted:	false
SSDEEP:	1536:tJzwN0CbUTqI34/9w6/Qua+1IGEbjBko230WBYT:vyA
MD5:	1F9995AB937AC429A73364B4390FF6E8
SHA1:	81998DCC6407CEB5CEF236AD52B9F2A3A9528D3B
SHA-256:	49E5166F40D8586714F86E08AB76A977199DF979357147A0E81980A804151C2A
SHA-512:	6669AE352FF46DB734BB8F973D1C0527C3A5EC4119D534AAE4C33F29EFF970168ED5FE200A05D4E1B6A2EC0E090E2207549B926317D489DC7664B0D9C208546
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.onestore.ms/cdnfiles/onestorerolling-1510-19009/shell/v3/scss/shell.min.css
Preview:	@charset "UTF-8";@font-face{font-family:'wf_segoe-ui_normal';src:local("Segoe UI");src:url("//i.s-microsoft.com/fonts/segoe-ui/west-european/normal/latest.eot");src:url("//i.s-microsoft.com/fonts/segoe-ui/west-european/normal/latest.eot?#iefix") format("embedded-opentype"),url("//i.s-microsoft.com/fonts/segoe-ui/west-european/normal/latest.woff") format("woff"),url("//i.s-microsoft.com/fonts/segoe-ui/west-european/normal/latest.ttf") format("truetype"),url("//i.s-microsoft.com/fonts/segoe-ui/west-european/normal/latest.svg#web") format("svg");font-weight:normal;font-style:normal}@font-face{font-family:'wf_segoe-ui_semilight';src:url("//i.s-microsoft.com/fonts/segoe-ui/west-european/semilight/latest.eot");src:url("//i.s-microsoft.com/fonts/segoe-ui/west-european/semilight/latest.eot?#iefix") format("embedded-opentype"),url("//i.s-microsoft.com/fonts/segoe-ui/west-european/semilight/latest.woff") format("woff"),url("//i.s-microsoft.com/fonts/segoe-ui/west-european/semilight/latest.ttf")

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\view[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	94237

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\view[1].htm	
Entropy (8bit):	5.521746961054254
Encrypted:	false
SSDEEP:	1536:44qtmf2LEGY8rGhM1P0GGLmHFu2b2l/nDSVUvDl+trBtZkhrwRPv1tP:4PIeGJ9L0yUvDYt6rwRPv1tP
MD5:	137CF1B67FE2CA53330069DD7C4B998F
SHA1:	29302254A00EC308E06296937F223166EB44E59A
SHA-256:	607A2364B614181EC0DA75C9317A295152D2318D92D240184685F552EC55676B
SHA-512:	D19A70FF71E02C36C7EC8EC3528F52412237D6B2937CD78FC52F0F6C1A4E579BC0D41357D46E2AE8B4043FC101126F29496C8741D1D977D7F127CCB1B77D691
Malicious:	false
Reputation:	low
Preview:	..<!DOCTYPE html>..<html lang="en" dir="ltr" xml:lang="en" xmlns="http://www.w3.org/1999/xhtml" class=" responsive sdx_html" style="">.. <head>.. <meta http-equiv="Content-Type" content="text/html;charset=utf-8"/><meta name="title" content="Churches Fire Security Ltd"/><meta name="description" content=""/><meta name="msapplication-tap-highlight" content="no"/><meta name="referrer" content="origin-when-cross-origin"/><meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, minimum-scale=1.0, user-scalable=no"/><meta name="format-detection" content="telephone=no"/><script type="text/javascript">function Css_Start(b,a){return {apiId:b,propertyId:a,startTime:(new Date).getTime()}}function Css_Load(e,c){var d=window,b=e.styleSheet,a;try{if(b&&!b.rules.length&&!b.cssText)a=1}catch(f){a=1}a&&(c.errorCode="DownloadFailure");if(d.$Static)d.$Static.logQos(c)}function Css_Error(b,a){a.errorCode="DownloadFailure";window.$Static&&

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\wac_s_office-2f03ce8e[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):	339628
Entropy (8bit):	5.406244560516871
Encrypted:	false
SSDEEP:	3072:/S+24ymQFofXUBtLmsxa6zLz+jtKpyaIsJPa9mlI7jHsZNp4HcI6t1tWRK5eQPPX:KFxH+jtEfOmlI7jHsZNp4HcVt+MFPP
MD5:	2F03CE8E2561DB41ECA65A39114C14B7
SHA1:	81F6CD529C184C7BE90381C8C202788F3C3E057D
SHA-256:	886CEDD621C1B8394ECB1B9C4EEF82F622F3485C302750B117907B9A41908589
SHA-512:	54867500187210B3A23D046840896B7683350CBFCC83211F46619BEB3C9F929D45CFEF6107C5F74F337BC93C7ED1C6636D15D0C804DDB3AE8C9E944C5FEFAF2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://spoprod-a.akamaihd.net/files/onedrive-website-release-prod_master_20200814.002/wac_s_office-2f03ce8e.js
Preview:	define("popover",["jquery-1.7.2","registernamespace"],function(){!function(e){registerNamespace("$UI"),window.$UI.Dialog=function(t,i,n,r,o,a){function s(){if(f){var e=f.style,t=$B.IE&&7==$B.V?p.offsetLeft/100:1;0==t&&(t=1),$Debug.trace("zoomAmount: ",t),$Debug.trace("scrollLeft: ",S.scrollLeft),$B.IE&&6==$B.V&&(e.width=S.scrollWidth-3+"px",e.pixelTop=Math.max(0,S.scrollTop/t)),e.pixelHeight=C.clientHeight/t,e.pixelWidth=C.clientWidth/t}}function l(e){var t;t=e.target==m?$UI.Dialog.findFocusableElement(D,g,!1):$UI.Dialog.findFocusableElement(D,m,!0),t&&setTimeout(function(){try{t.focus()}catch(e){}},0)}function d(){e(window).bind({"resize.ext":c,"scroll.ext":c})}function c(t){e(window).unbind(".ext",c),_.recalc(!1),d()}function u(){if($B.IE&&$B.V<7){v=w.getElementsByTagName("select");for(var e=D.getElementsByTagName("select"),t=0;t<v.length;t++){for(var i=!1,n=0;n<e.length;n++)if(v[t]==e[n]){i=!0;break}i||(v[t].wlppHide=v[t].style.visibility,v[t].style.visibility="hidden")}}}var h=wind

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\wapsw[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 448 x 336, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	5884
Entropy (8bit):	7.656622988312936
Encrypted:	false
SSDEEP:	96:Zs4BodBmk+ZXNCtOmBZADWtjKOuTRBwVhiI2CQwks/uZ1my5QkWi8WE9eSFs2xVM:y0odXg2jA/TUVhe2CzjuZAKvE9LFC/
MD5:	93A322C8B54119CFE9B2CEA455E9204E
SHA1:	42578D63A9340A1788B9319CA819CE0A2074C33D
SHA-256:	390577D35C959FFE7DD2AF4519C04410A04FDC4A433B151E27B049FC4A1AB3E9
SHA-512:	0F1D4D70C129C26349752D5A871A55D2936BCE084B74206AA547C17C5823C9DDA8F28EFC7DDF795D9FF5AC4EF1441ABC02E5F521AE77E4C0BA45B9BFA1FC4C6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c1-officeapps-15.cdn.office.net/o/s/161351641006_resources/1033/wapsw.png?b=1601351641006
Preview:	.PNG........IHDR.....P.....(C.0....IDATx^..}.}y]....J.FKD-#,.A1..."7.....Q*...| ...h...)T..Knt..(....k...?..(I.....6Y.fN..g...}8...{f.....8;w..>{.=.....899yn.[...?....._V..SS...Eq.5.....kQ....}.1...?.z.Xn..gQ.....a.(.q{...|..H....8j.5..n.tQ..-.fo.^~.h.8..,.7>}a...O.tt..UA.R..<p...Z...!3...h..F.=p..v.@.R....&>}V..l.$.%..T.p..M.t..H.}...=Q..=...Z..e....e.E)d.....8..{..I...~v.....b..R....x.....4B..Z.A...Xt7K.....wF.Z..g.....[.../.....V..EP.Tu..-.....x.....S.../.88 ....,.S..... .i.x.E}(.....z.6.....G..{W...i.&....].^....[Rs....|H.....`@.....+.e..f. -Fb.....5._,.....U...6.8.....p...98.:.....(..Q.u?|[..".h.[..Au..b}/.p.TqA...T...g.3[w..|h.....Y.u..j.w...!8I.e!.X.w..r..!^wY..NM...i.=.....:..g.%..O..7..r.bMo'..0.....S.....4..?s..&W..[/..?.`z!..l..kD)...7}...`.TKCgF..]~*i3.....w.(...F..B...8.....S.y..\.....+.g..^.....4..ga:.`....\.K....?..C".wF.Z.<(....`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\webauth.implicit.msal.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	266561
Entropy (8bit):	5.235117380630118

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\webauth.implicit.msal.min[1].js	
Encrypted:	false
SSDEEP:	6144:VGOINtnUuPaz4rnn2B3TPPVaVA300ZRB2uF9mOGUINmlhi+PalK1nO2HYTrPVspd:VGBWe/VA300MOGcl0LqpQMh55Pn
MD5:	447DEE3C2BA49194C19CEB120F44F9D4
SHA1:	BEEBE9CB49DC9800846191ADB144548C8F60BE3E
SHA-256:	8EAD034934F66F8898AECA85D5CB82AE45E4C78BC721477209C6B8692D9AEDAE
SHA-512:	C0AD039C8F87ECB34ADCAC5E2BB05F82D803576233DA0D714CE82AA3655513D10B2B75FF9B5E11923F1C439969B3B43AF1823BF43660514D5B5E6110FD6E7A4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c1-onenote-15.cdn.office.net/o/s/161351641006_App_Scripts/webauth.implicit.msal.min.js
Preview:	!function(e,t){"object"==typeof exports&&"object"==typeof module?module.exports=t():"function"==typeof define&&define.amd?define("Implicit",[],t):"object"==typeof exports?exports.Implicit=t():e.Implicit=t()}(window,function(){return function(e){var t={};function r(o){if(t[o])return t[o].exports;var n=t[o]={i:o,l:!1,exports:{}};return e[o].call(n.exports,n,n.exports,r),n.l=!0,n.exports}return r.m=e,r.c=t,r.d=function(e,t,o){r.o(e,t)||Object.defineProperty(e,t,{enumerable:!0,get:o})},r.r=function(e){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(e,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(e,"__esModule",{value:!0})},r.t=function(e,t){if(1&t&&(e=r(e)),8&t)return e;if(4&t&&"object"==typeof e&&e&&e.__esModule)return e;var o=Object.create(null);if(r.r(o),Object.defineProperty(o,"default",{enumerable:!0,value:e}),2&t&&"string"!=typeof e)for(var n in e)r.d(o,n,function(t){return e[t]}.bind(null,n));return o},r.n=function(e){var t=e&&e.__esModule?function

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\Box4Intl[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):	73197
Entropy (8bit):	5.065102304001194
Encrypted:	false
SSDEEP:	768:+1Cm1r0AOKbnbhCWm6MlO0zBZNumn047hNXcb7GLLWZWxW86ssTbxLh:+1CkdxYWmGhKNXcb7GLLCmcssfxF
MD5:	F806F54E73D9D2A73472CA970CF895D5
SHA1:	8D8FC0B1A219CE2F234BAC09AF5A564A14957C06
SHA-256:	FED03FC1176B327B0CC496FA8BB886A2CDEDD7AD26C063BBCA252F6ECB38A29E
SHA-512:	9D945DC3CBBD9FA1408BDD866D9FD1CE9D50B8BB923A77B64E4CD24D2C9557050B2E8232EC36C48FA794970F3BF4FABBA292795157CB5F18F9EEEC5BB478A68
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c1-onenote-15.cdn.office.net/o/s/161351641006_App_Scripts/1033/Box4Intl.js
Preview:	Type.registerNamespace("Box4Intl");Box4Intl.Box4Strings=function(){};Box4Intl.Box4Strings.registerClass("Box4Intl.Box4Strings");Box4Intl.Box4Strings.l_OutlineResizeAlt="Resize the Outline";Box4Intl.Box4Strings.l_NavigationPaneContentsLabel="Notebook Contents";Box4Intl.Box4Strings.l_UntitledPageText="Untitled Page";Box4Intl.Box4Strings.l_UntitledSection="Untitled Section";Box4Intl.Box4Strings.l_NotebookPagesSection="General Pages";Box4Intl.Box4Strings.l_ProtoButtonText="New Page";Box4Intl.Box4Strings.l_SectionGroupAltText="Section Group";Box4Intl.Box4Strings.l_SectionGroupArrowAltText="Navigate Up";Box4Intl.Box4Strings.l_DefaultUserName="Unknown User";Box4Intl.Box4Strings.l_UserInitialsDelimeter="; ";Box4Intl.Box4Strings.l_PageLoadingText="Loading...";Box4Intl.Box4Strings.l_OreoSpinnerText="Loading Page...";Box4Intl.Box4Strings.l_ConflictPage="Conflict Page";Box4Intl.Box4Strings.l_PageAccessibilityContext="Page {0}";Box4Intl.Box4Strings.l_PageWithSearchResultsAccessibilityContext="Page

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\BrowserUls[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):	1922
Entropy (8bit):	5.006174566262526
Encrypted:	false
SSDEEP:	48:yThd/YIWeETNQuFNJMgBVAGzeFWOUutFRVoZjskBWs:U0IWYuPuG3yov
MD5:	3E3CD75B07B521BC61C01450E2C7873A
SHA1:	57D7881E0E878CABE74B1021CF86126148928DE7
SHA-256:	2882BF4B22D0AD63E6F8877EB5C22353921E8C87B197911462933B7D1A7A44B8
SHA-512:	3B1D53CB1F49B2CF8648CEF8EDEB526B924430F2FC622421DF6AB3F61E49449CD5EB8BCCC7E6A019575A4843B0D3C50A69C4B0BF1D1133F960E92969CAC37BE7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn.onenote.net/officeaddins/161351940458_Scripts/BrowserUls.js
Preview:	function InitializeUls(){TheUlsHost=new Diag.ConsoleUlsHost;Diag.ULS.setUlsHost(TheUlsHost)}function FlushBrowserUls(){TheUlsHost&&TheUlsHost.dispose();InitializeUls()}var __extends=this.__extends||function(n,t){function r(){this.constructor=n}for(var i in t)t.hasOwnProperty(i)&&(n[i]=t[i]);r.prototype=t.prototype;n.prototype=new r},Diag,TheUlsHost;(function(n){var t=function(){function n(){}return n.prototype.isEnabled=function(){var n=!1;try{typeof Storage!="undefined"&&(n=localStorage.getItem("EnableConsoleLogging")==="true")}catch(t){}return n&&window.console&&window.console.log},n.prototype.error=function(n){window.console.error(n)},n.prototype.warning=function(n){window.console.warn(n)},n.prototype.info=function(n){window.console.info(n)},n.prototype.log=function(n){window.console.log(n)},n}(),i=function(i){function r(r,u){r===void 0&&(r=new t);i.call(this,SessionId,BrowserUlsUploadPath,new n.UlsUploadConfiguration(null,null,null,null,null,null,!0));this._console=r;this._suppress

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\CommonDiagnostics[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\CommonDiagnostics[1].js	
Size (bytes):	31865
Entropy (8bit):	5.533745604382844
Encrypted:	false
SSDEEP:	384:S/Td4EWwl29vxBX/ETqR3fSQSJaJSQS3wYRgWUQgkplcnQLzaL1UaR4yEZ8VouWW:k9vb8TqRYlLpjfDcn9XXg8VoGd
MD5:	93717ED93BE946CF903364FCE8172285
SHA1:	A83ACB90EC19602330EBD383501A45A978B5241C
SHA-256:	D5A79479A3041502198CC8DD2E72C7F0281BFC8A5820AF15AC6D9C9D6FA3F376
SHA-512:	2297980F50111D147ACD6596BDE78ED8AA51F7B97078D799A4F0981223E5134A2727A808C08A197F80928269CD44E95AB5D033A845A0D68477EC79594136987F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn.onenote.net/officeaddins/161351940458_Scripts/CommonDiagnostics.js
Preview:	/*! Version=16.0.0.0 */.if(!window)this.window=this;var Type=Function;Array.$H=function(a,b){a.push(b)};Array.$1m=function(d,b){for(var a=0;a<b.length;a++){var c=b[a];d.push(c)}};Array.clear=function(a){a.length=0};Array.$1U=function(a,b){return Array.$1c(a,b)>=0};Array.$1c=function(c,e,a){if(c.indexOf)return c.indexOf(e,a);a=a;if(isNaN(a))a=0;var d=c.length;if(isFinite(a))a=a\|0;if(a<0)a=Math.max(0,d+a);for(var b=a;b<d;b++)if(c[b]===e)return b;return-1};Array.dequeue=function(a){return a.shift()};Array.enqueue=function(a,b){Array.$H(a,b)};Array.__typeName="Array";Array.$1K=true;Boolean.__typeName="Boolean";Boolean.$1K=true;Function.$2Q=function(a,b){return function(){return b.apply(a,arguments)}};Function.__typeName="Function";Function.$1K=true;Date.__typeName="Date";Date.$1K=true;Error.$1t=function(e,f){var a=new Error(e);a.message=e;if(f){var b=f;for(var c in b){var d={key:c,value:b[c]};a[d.key]=d.value}}a.$19();return a};Error.$1S=function(a,b){return Error.$1V("Sys.ArgumentExceptio

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\EditSurface[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	26092
Entropy (8bit):	5.539038486683526
Encrypted:	false
SSDEEP:	384:ne7LRwe03wCS8V012RwlKzXicngHlI4xIZD333qYSzK1/0:ne756VnzZUIRDnqYWd
MD5:	509E198E7333B66A19165385831BB218
SHA1:	3D00C52D011E476154057427137373 60C0F85066
SHA-256:	F5381B300327898B4D31B583D273EBFD168FC3469BE685F3F7477EDC649115ED
SHA-512:	AB62C39AB5A3E47DFF578522B2F09E0AB3FD833D8E621F015900A9B81FF177A582B5FB4B68A51D02949B5A2D4803529AABF1C8FC0D201CAAF794EE5FD67B3731
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c1-onenote-15.cdn.office.net/o/s/161351641006_resources/1033/EditSurface.css
Preview:	FocusedContentControl*{margin:0;padding:0;}.EditingSurfaceBody{background-color:transparent;border:none;outline:none;}.EditingSurfaceBody,.EditingSurfaceBody *{-ms-touch-select:none;-webkit-user-select:text;-khtml-user-select:text;-moz-user-select:text;-ms-user-select:text;}.EditMode span.SpellingError,.EditingSurfaceBody span.SpellingError{background-image:url('');border-bottom:solid 1px transparent;}.EditMode span.DictationCorrection,.EditingSurfaceBody span.DictationCorrection{background-image:url("data:image/svg+xml;utf8,<svg xmlns='http://www.w3.org/2000/svg' width='3' height='4'><path d='M 0 0 L 5 5' stroke='gray' stroke-width='1px'/></svg>");border-bottom:solid 1px transparent;}.EditMode span.ContextualSpellingAndGrammarError,.EditingSurfaceBody span.ContextualSpellingAndGrammarError{background-image:url('

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\Instrumentation[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):	3263
Entropy (8bit):	5.202198382150091
Encrypted:	false
SSDEEP:	48:G6E6oKn0FmM8LOCvlocJYSq0JMlL+49W0lwlQSoIQ90ESf4TmlSYmYBo:9yDWocGSPWg4IbOQS/CahlcYW
MD5:	03674DB75782BFB0CB3C6B1AFB84C6AA
SHA1:	D609684F3423CC185834DA28396A6E1DEE7142A0
SHA-256:	5D5B6A8449DF6BADA967EE227F79A9A8E8E1DCEBF3367EB23292971E6E822EBA
SHA-512:	9F9174D1C0668BBD151607D0DAE2EB99DF18AC6BE772B5A8DBE1B37B8C615FE312FD8FA9FC93D98C706BEEBBF1C8262CDE9B812C685C075C776926052D37A06
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn.onenote.net/officeaddins/161351940458_Scripts/Instrumentation.js
Preview:	function GetInstrumentationCategory(){return instrumentationCategory?instrumentationCategory:InstrumentationCategoryString?instrumentationCategory=Diag.ULSCat[InstrumentationCategoryString]:null}function InstrumentLinks(n){for(var t,r=0,i=0;i<n.length;i++)t=n[i],t.id||(t.id="un_"+r,r++),t.onclick=GenerateInstrumentationLink(t.id,t.onclick),t.ondragstart=GenerateDragInstrumentationLink(t.id,t.ondrag),t.oncontextmenu=GenerateContextMenuInstrumentationLink(t.id,t.oncontextmenu)}function LogUserViewPortInfo(){var t=$(window).width(),n=$(window).height(),i=screen.width,r=screen.height,u=$(document).height(),f=n/u*100;Diag.ULS.sendTraceTag(6436628,GetInstrumentationCategory(),Diag.ULSTraceLevel.info,"User ViewPort Info;windowWidth={0};windowHeight={1};screenWidth={2};screenHeight={3};percentageOfPageVisible={4};",t,n,i,r,f.toFixed(3))}function UpdateFurthestScrollDepth(){var t=$(window).scrollTop(),i=$(window).height(),r=t+i,u=$(document).height(),n=r/u*100;n>furthestScrollDepthPercentage&&(

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\LearningTools[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):	19705
Entropy (8bit):	5.376005492661156
Encrypted:	false
SSDEEP:	384:1Wt1CTbGLeulh4MQOCS9AKBINrXNlQihhST3iqd0XaVfPdZ3:41GTuli2gKBkrPqCqFdZ3
MD5:	A583A3BEBEDE2070D1F7108512F2FC8A
SHA1:	516EA1C9F095669E004C382A82E65D224260B210
SHA-256:	B9667EBBD8CB1C9F5AC673B2A7988597E810D79C5BF07B717307A8403204107E
SHA-512:	5F9132C450EC4AD431DCB43001BD174428E700E6D280BB79B60189EF5AEB9F8186A98C1F7896876448 74CB9A5DCD3ED44D6933EABB2E27F35F1CAD75E900EA 1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn.onenote.net/officeaddins/161351940458_Scripts/LearningTools/LearningTools.js
Preview:	function getLanguageParameter(n){for(var t,f=window.location.search.substr(1),r=f.split("&"),u="",i=0;i<r.length;i++)if(t=r[i].split("=",2),t.length==2&&t[0]=="ui"){u=""+ n+"="+t[1];break}return u}function getEdgeMajorVersion(){var t=navigator.userAgent,n=t.match(/Edge\/([0-9]+)/i);return n&&n.length>=2?parseInt(n[1]):-1}function getQueryParameter(n){var u,r,t,i;if(window.location.search&&window.location.search.length>1)for(u=window.location.search.substring(1),r=u.split("&"),t=0;t<r.length;t++)i f(i=r[t].split("="),decodeURIComponent(i[0])==n)return i.length>1?decodeURIComponent(i[1]):"";return null}function now(){return(new Date).getTime()}function gen erateGuid(){return"xxxxxxxx-xxxx-4xxx-yxxx-xxxxxxxxxxxx".replace(/[xy]/g,function(n){var t=Math.random()*16|0,i=n==="x"?t:t&3|8;return i.toString(16)})}function createSim pleHtml(n,t,i){i===void 0&&(i=null);var r=document.createElement(n);return r.innerText=t||"",i&&r.setAttribute("lang",i),r.outerHTML}function loadTableAsync(n,t,i,r){var

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\OfficeExtension.WacRuntime[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	164949
Entropy (8bit):	4.207150502607244
Encrypted:	false
SSDEEP:	1536:0hUYBUBvBrBXBWBIBXBXBwBIBQBbBnBeBRBbB3BjBTBDBvBHBPBPBdBBBHBmB7Bq:uRYAQL
MD5:	BD127BDDA40BC67C26C030F3E78C8652
SHA1:	B61028A4A7F18B306C95F6EC57C49939AFA84370
SHA-256:	50170845A660D2259F8E7B495D1B26E85951A6537A472224851D93ED3E046D9F
SHA-512:	D3AA0A8602378A966BC1A7E527906A8E652BFA34E629BBF43679869FAD5EAC5E8037BE129DD1144BD9F6CA77161F42C7B963123A8689C6625E168DD592DC78A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c1-onenote-15.cdn.office.net/o/s/161351641006_App_Scripts/OfficeExtension.WacRuntime.js
Preview:	var __extends = (this && this.__extends) || (function () {.. var extendStatics = function (d, b) {.. extendStatics = Object.setPrototypeOf ||.. ({ __proto__: [] } instanceof Array && function (d, b) { d.__proto__ = b; }) ||.. function (d, b) { for (var p in b) if (b.hasOwnProperty(p)) d[p] = b[p]; };.. return extendStatics(d, b);.. };.. return function (d, b) {.. extendStatics(d, b);.. function __() { this.constructor = d; }.. d.prototype = b === null ? Object.create(b) : (__.prototype = b .prototype, new __());.. };..})();..var OfficeExtension;..(function (OfficeExtension) {.. var WacRuntime;.. (function (WacRuntime) {.. var Constants = (function () {.. function Constants() {.. }.. Constants.httpMethodGet = "GET";.. Constants.httpMethodPost = "POST";.. Constants.httpMethodPatch = "P ATCH";.. Constants.httpMethodDelete = "DELETE";..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\OneNote.Refresh[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	419191
Entropy (8bit):	5.309898171819597
Encrypted:	false
SSDEEP:	6144:YaAMX8gWd5eL5Ac4nb+9xVpO0KSZ+968S37v5or:pAMX8guc4nb+9xVpO0KSZ+968S37v5or
MD5:	B30128679A7DB62C74ADD0097A060693
SHA1:	CE6A273276E3CB529506EA4D6102ADE7B0E1C6CE
SHA-256:	C31C126CB3298904AB3CC79BEB6E62197C8E05AD2F6D5B2E9C213A0226654B09
SHA-512:	98F85B5577CC38340D8289C3BC13105F61026CB0F0290D784019DCE4AFEE6740505CFB3B0F31C9225051390A782EDE35BDDE1C600BC9527F89E79ED6F025754F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c1-onenote-15.cdn.office.net/o/s/161351641006_resources/1033/OneNote.Refresh.css
Preview:	.headBrand{cursor:default;line-height:48px;font-size:22px;margin-left:20px;margin-right:20px;font-family:'SegoeUI-SemiLight-final','Segoe UI SemiLight','Segoe UI WPC Semilight','Segoe UI',Segoe,Tahoma,Helvetica,Arial,sans-serif;}.cui-topBar1-transistionalHeaderUI .headBrand{width:auto !important;height:24px !important;line-heigh t:normal !important;padding-bottom:12px;padding-top:12px;display:inline-block;font-size:17px;font-family:inherit;margin-left:17px;margin-right:17px;font-family:'Segoe UI' ,'Segoe UI Web',Arial,Verdana,sans-serif;}.cui-topBar1-transitionalReactHeaderUI .headBrand{width:auto !important;line-height:48px !important;padding:0 6px;disp lay:inline-block;font-size:16px;font-weight:600;font-family:"Segoe UI","Segoe UI Web (West European)","Segoe UI",-apple-system,BlinkMacSystemFont,Roboto,"Helvetica Neue",sans-serif;}@font-face{font-family:"Segoe UI Web Light";font-style:normal;font-weight:normal;src:local("Segoe UI Light"),url('./segoeuil.woff') format('woff'),url('./sego

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\OneNoteSimplified.Wac.TellMeModel[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):	210420
Entropy (8bit):	5.648752403576843
Encrypted:	false
SSDEEP:	3072:Bw7NKvX3WhiX1z3LtTOd3wYLMUJdmRPiWmqtmzAZWTEM0BR1zGoEmVWvSnxU:GZKvXr1z3m37MjcWmqdWTEhBRBGoVBn2
MD5:	966B9F9897C113C2E2BA63D7E2E5289B
SHA1:	D88ECB07061BE84679AF27DCE0D29E5F6158451E
SHA-256:	C2F603FAF7C04768811C4DC08B7ECB4B6F39018FC5742EA735C94DEBD3902418
SHA-512:	A3C2E373BFA699D18CF60BF1F79742E223F7A3AB18305558FCFDDC93411D2C5CCFE84AD8C919BC29CB18DDD7DECD9D91D352501D0BEE3C088C4116AAC8E9 984
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c1-onenote-15.cdn.office.net/o/s/161351641006_App_Scripts/1033/OneNoteSimplified.Wac.TellMeModel.js
Preview:	var TellMeModel={"m":{"":76},"t":[0,7,7,7,7,7,7,7,7,7,7,7,5,5,5,5,5,5,5,5,5,5,5,5,5,5,5,5,5,5,5,5,5,5,5,5,5,5,5,5,5,5,5,5,5,5,5,5,5,5,5,5,5,5,5,5,6,6,6,6,6,6, 6,7,2,10,10,10,7,4,4,4,4,4,4,4,4,4,4,7,7,7,7,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1 ,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1 ,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,7,7,7],"n":[306,393,396,399,402,405,408,412,415,418,421,4 24,427,430,451,480,489,498,507,520,533,542,551,560,569,582,595,608,621,634,647,656,669,682,695,704,717,730,743,756,769,782,795,811,829,853,877,898,927 ,948,961,974,994,1015,1025,1035,1056,1065,1075,1084,1094,1104,1125,1159,1164,1169,1176,1205,1228,1249,1251,1253,1254,1255,1256,1258,1271,1273,16533,16

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\OneNoteSimplified.Wac.TellMeSuggestionModel[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	127321
Entropy (8bit):	3.8975903207588436
Encrypted:	false
SSDEEP:	3072:afDyAXsHQxmPHmLZyb92FcFxSYJVBp0HoU:fA8HQxaG0AExSYJVGN
MD5:	57471BC6CC30C96D25D74B24DD6602C1
SHA1:	9DD004D4B1AAADC316A506A182A4CBCEED140E12
SHA-256:	24CDC3A8BED362E1EFA94BFEE82E9100E4ED9A034A229F9D0069D981CBDD75F7
SHA-512:	2188FDC12265DBF7DBC9B693734BD798EA8F64663F6BE2AC5FD1DF6012EDD8A9008117B5409D283DD5B522811F2184A0442A7DABBD1430BFEAC60980A2D731 1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c1-onenote-15.cdn.office.net/o/s/161351641006_App_Scripts/OneNoteSimplified.Wac.TellMeSuggestionModel.js
Preview:	var CoefficientModelIdMap= {50:'AlignLeft',123:'floatiefseaOutdent',151:'DeleteTable',69:'EditInApp',188:'InsertInTableMenu',2:'MenuOpen',175:'NT18',124:'EnterI nkingHighlighterMode',89:'btnFileSharing',53:'NT1',5:'Share',166:'SelectRow',149:'InsertCameraPicture',91:'NT14',86:'btnOpenInClient',59:'floatiebtnImageCropDia log',184:'StartAudioRecording',67:'mnuNoteTagMarkLauncher',126:'NT2',58:'InsertAbove',122:'MoreSymbols',41:'EnterMarqueeSelectMode',20:'ShowAccChecker Pane',48:'MenuClose',119:'SelectTable',131:'floatiebtnImageShrink',75:'NT11',43:'floatieidTableInsert',172:'LineSpacingOptions',153:'DeleteColumn',81:'floatiesbBullets',1 76:'MenuCellShading',146:'StopAudioRecording',44:'Print',148:'Cut',34:'ApplyStyleGallery',145:'TextDirRTL',115:'PictureCropDialog',88:'btnImmersiveMode',83:'Pic tureAbsoluteHeight',111:'Copy',14:'faShare',144:'NT23',68:'InsertSymbolGallery',179:'NT16',112:'ShowSectionsAndPagesCommand',37:'SetProofingLanguage',6:'HideAll NavCommand',185:'Table',35:'DecreaseInde

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\OsfRuntimeOneNoteWAC[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	544674
Entropy (8bit):	5.341820635481777
Encrypted:	false
SSDEEP:	6144:FUdpr55afI8FdMyaTpEIDm9STsGVaN1y3xOzwje2X2xdKoC9l5eNgiKqQWYsg3o/:wtEIDlSSOzwI
MD5:	663AB7F5AFB769D9ABA2E9AD99A25903
SHA1:	240EFDBA5CB93E942A9121FD063C5FAA37B813F4
SHA-256:	B6AA2E8A1F6170807A412C5088C08A1327DD839F735CEF18C3B415E994FCDC6A
SHA-512:	717B0715363A4C6E2BDA3B889A4FE579E5C37F5638D7F01E158CA76D62C7CE0DDCAE59C929D021FEE8AAF39FD83696272E15CC7B96DEEBCC5FDD450196E8D 73
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c1-onenote-15.cdn.office.net/o/s/161351641006_App_Scripts/OsfRuntimeOneNoteWAC.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\OsfRuntimeOneNoteWAC[1].js	
Preview:	/* Office runtime JavaScript library */..../*...Copyright (c) Microsoft Corporation. All rights reserved...*/...../*.. Your use of this file is governed by the Microsoft Services Agreement http://go.microsoft.com/fwlink/?LinkId=266419..... This file also contains the following Promise implementation (with a few small modifications):.. * @overview es6-promise - a tiny implementation of Promises/A+... * @copyright Copyright (c) 2014 Yehuda Katz, Tom Dale, Stefan Penner and contributors (Conversion to ES6 API by Jake Archibald).. * @license Licensed under MIT license.. * See https://raw.githubusercontent.com/jakearchibald/es6-promise/master/LICENSE.. * @version 2.3.0..*/..var OfficeExt;(function(b){var a=function(){var a=true;function b(){}b.prototype.isMsAjaxLoaded=function(){var b="function",c="undefined";if(typeof Sys!==c&&typeof Type!==c&&Sys.StringBuilder&&typeof Sys.StringBuilder===b&&Type.registerNamespace&&typeof Type.regis

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\aria-web-telemetry-2.9.0.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	53853
Entropy (8bit):	5.500009921962495
Encrypted:	false
SSDEEP:	768:WFBlHId5vh+HExEP0HLVwU+megaBJpLGgVI3g6BifcqJMBSWDv6:WpHId5W0HLEagVIw6QXb
MD5:	5A8ED3646A340A247CD48F5732BAEA69
SHA1:	8A961A2C1461EB5CD8A9009911970824602F8B79
SHA-256:	C459EC1608D98A847AB4C83723E1C4B2DC6E58A7006D5566C529A93113C2EE62
SHA-512:	5421BC6C0EA27EE75F7B5633AA5757C62EE16C84E94099D301EEA9944131F8A26CE941711ACE5EFB66AD62FBD16460B31403A2B016E8CF72D1F025868CA838D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn.onenote.net/officeaddins/161351940458_Scripts/aria-web-telemetry-2.9.0.min.js
Preview:	var clienttelemetry_build;!function(e){e.version="2.9.0"}(clienttelemetry_build||(clienttelemetry_build={}));var Microsoft;!function(e){var t;!function(e){var t;!function(e){e[e.BT_STOP=0]="BT_STOP",e[e.BT_STOP_BASE=1]="BT_STOP_BASE",e[e.BT_BOOL=2]="BT_BOOL",e[e.BT_UINT8=3]="BT_UINT8",e[e.BT_UINT16=4]="BT_UINT16",e[e.BT_UINT32=5]="BT_UINT32",e[e.BT_UINT64=6]="BT_UINT64",e[e.BT_FLOAT=7]="BT_FLOAT",e[e.BT_DOUBLE=8]="BT_DOUBLE",e[e.BT_STRING=9]="BT_STRING",e[e.BT_STRUCT=10]="BT_STRUCT",e[e.BT_LIST=11]="BT_LIST",e[e.BT_SET=12]="BT_SET",e[e.BT_MAP=13]="BT_MAP",e[e.BT_INT8=14]="BT_INT8",e[e.BT_INT16=15]="BT_INT16",e[e.BT_INT32=16]="BT_INT32",e[e.BT_INT64=17]="BT_INT64",e[e.BT_WSTRING=18]="BT_WSTRING",e[e.BT_UNAVAILABLE=127]="BT_UNAVAILABLE"}(t=e.BondDataType||(e.BondDataType={}));var n;!function(e){e[e.MARSHALED_PROTOCOL=0]="MARSHALED_PROTOCOL",e[e.MAFIA_PROTOCOL=17997]="MAFIA_PROTOCOL",e[e.COMPACT_PROTOCOL=16963]="COMPACT_PROTOCOL",e[e.JSON_PROTOCOL=21322]="JSON_PROTOCOL",e[e.PRETTY_JSON_PR

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\clientstring[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):	93118
Entropy (8bit):	5.08887724148592
Encrypted:	false
SSDEEP:	1536:9f/hyu1HHOx43CJvE28pcmehNsFVP4DN3urga/xBC:9Ryu1nR3CJBNmehNsvP4UjJQ
MD5:	7EEB13B7F9DBAF66183A71E9B25C5278
SHA1:	AD62E7C182E1D907211135820BDF8226661B91DA
SHA-256:	E8E938DA89D10BA70A329D976228BA69D67C2D370A7F11826A0E0571E9488045
SHA-512:	FEDD99104C4C21D2654E8DE351E2C259C266EC811D0489EBE48DA5858D634A726E372C104BD80149A5CC1C39C24A6CC885E2C22E7197AF1A106F06A44A48D36
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://onedrive.live.com/handlers/clientstring.mvc?mkt=en-US&group=Office&v=19.419.0221.2001&useRequiresJs=False
Preview:	(function () {window.GetString = function(s){var rootObject = this, parts = s.toLowerCase( ).split('.'), iCount = parts.length;for (var i = 0; i < iCount; i++){var currentPart = parts[i];rootObject = rootObject[currentPart];if (rootObject == null){return '';}}return typeof (rootObject) == "object" ? rootObject.___str : rootObject.toString();};.var BaVq = window.live=window.live||{};var UIsu=BaVq.shared=BaVq.shared||{};var IDCS=UIsu.skydrive=UIsu.skydrive||{};var iXDx=IDCS.pc=IDCS.pc||{};var LGkx=iXDx.da=iXDx.da||{};LGkx["error10001_2"]="{0}Fetching files on a PC running Windows 8.1 isn't supported. If you upgraded a PC to Windows 8.1, or no longer use the OneDrive desktop app on a PC, you can remove the PC from the list. {1}";var oYkr=iXDx.tagfiltermenu=iXDx.tagfiltermenu||{};oYkr["fast_food"]="Fast food";oYkr["group_photo"]="Group photo";oYkr["hand_bag"]="Hand bag";oYkr["meeting_room"]="Meeting room";oYkr["mobile_phone"]="Mobile phone";oYkr["stained_glass"]="Stained glass";oYkr["steeri

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\common50.min[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):	713440
Entropy (8bit):	5.4707108333799646
Encrypted:	false
SSDEEP:	6144:Uaa3vykxvXj1mzhuzoD6ywR8yx01CS8y5W/kGSwKahl+P2MjBwijPbyIysrAkO:vlfWTSHFwiO
MD5:	E154C6ECA03078945C5A187DB6F8A543
SHA1:	9632A14695BB512606818ECADA5EAE6ABB4B9B58
SHA-256:	ED8359D4338300E76AEDCC40CD5E1449456A1B654069AC0995618CDCCD93DBCA
SHA-512:	466D061B0438ADC552A09E7F9C9B4CDEE94FD8BA55008A89C8831125E382357FE11C80BE206D51A451AF90081C8FB97A04242ABAA5BBD5CE05676D020194999
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\common50.min[1].js	
Reputation:	low
IE Cache URL:	http://https://c1-onenote-15.cdn.office.net/o/s/161351641006_App_Scripts/common50.min.js
Preview:	(window.webpackJsonp_name_=window.webpackJsonp_name_||[]).push([[1],[,,,,,,,,,,,,,function(e,t,n){"use strict";n.r(t);n(709);var o=n(141);n.d(t,"assign",(function(){return o.D})),n.d(t,"filteredAssign",(function(){return o.ab})),n.d(t,"mapEnumByName",(function(){return o.ic})),n.d(t,"shallowCompare",(function(){return o.Qc})),n.d(t,"values",(function(){return o.cd})),n.d(t,"omit",(function(){return o.tc})),n.d(t,"setFocusVisibility",(function(){return o.Ic})),n.d(t,"IsFocusVisibleClassName",(function(){return o.n})),n.d(t,"setSSR",(function(){return o.Nc})),n.d(t,"createMergedRef",(function(){return o.Q})),n.d(t,"Async",(function(){return o.a})),n.d(t,"AutoScroll",(function(){return o.b})),n.d(t,"BaseComponent",(function(){return o.c})),n.d(t,"nullRender",(function(){return o.rc})),n.d(t,"DelayedRender",(function(){return o.i})),n.d(t,"EventGroup",(function(){return o.j})),n.d(t,"FabricPerformance",(function(){return o.k})),n.d(t,"GlobalSettings",(function(){return o.m})),n.d(t,"KeyCo

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\jquery-2.1.3.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	84320
Entropy (8bit):	5.370493917084567
Encrypted:	false
SSDEEP:	1536:AP1vk7i6GUHdXXeyQazBu+4HhiO2wd0uJO1z6/A4fGAub0i4ULgGiyz4npa98Hrb:z4UdWJiz6UAIJ8pa98Hrb
MD5:	32015DD42E9582A80A84736F5D9A44D7
SHA1:	41B4BFBAA96BE6D1440DB6E78004ADE1C134E276
SHA-256:	8AF93BD675E1CFD9ECC850E862819FDAC6E3AD1F5D761F970E409C7D9C63BDC3
SHA-512:	EDA31B5C7D371D4B3ACCED51FA92F27A417515317CF437AAE09A47C3ACC8A36BDBB5A5E70F0FBFD82D3725EDF45850DDE8CA52C20F9A2D6E038B8EAACEE3CF1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ajax.aspnetcdn.com/ajax/jQuery/jquery-2.1.3.min.js
Preview:	/*! jQuery v2.1.3 | (c) 2005, 2014 jQuery Foundation, Inc. | jquery.org/license */.!function(a,b){"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a document");return b(a)}:b(a)}("undefined"!=typeof window?window:this,function(a,b){var c=[],d=c.slice,e=c.concat,f=c.push,g=c.indexOf,h={},i=h.toString,j=h.hasOwnProperty,k={},l=a.document,m="2.1.3",n=function(a,b){return new n.fn.init(a,b)},o=/^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g,p=/^-ms-/,q=/-([\da-z])/gi,r=function(a,b){return b.toUpperCase()};n.fn=n.prototype={jquery:m,constructor:n,selector:"",length:0,toArray:function(){return d.call(this)},get:function(a){return null!=a?0>a?this[a+this.length]:this[a]:d.call(this)},pushStack:function(a){var b=n.merge(this.constructor(),a);return b.prevObject=this,b.context=this.context,b},each:function(a,b){return n.each(this,a,b)},map:function(a){return this.pushStack(n.map(this,functi

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\js-cookie[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	3831
Entropy (8bit):	5.120639874211328
Encrypted:	false
SSDEEP:	96:itGurLtJwqfjH6CluRxs0gPhtxq+jLqXnvZQQ2:itGu3t+yb6CBUHN
MD5:	72D9A825554620C51BF0018A457E7F2E
SHA1:	23400E26C69A1F8A47236FFAD4BC80FC80BA773E
SHA-256:	365009220D893F07B356C7F253CECD5A9F7E06D6207A3DD7A148FC73812B4FE6
SHA-512:	9212035EFC74AD61A74FA806229E4A97BB9FB50698B0B15BD7296AD53B6A2C9A43D0A3E2082286F4AC60167E129E07CB511638A103C510DB3B5ADA6A383165A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn.onenote.net/officeaddins/161351940458_Scripts/ExternalResources/js-cookie.js
Preview:	/*!.. * JavaScript Cookie v2.1.3.. * https://github.com/js-cookie/js-cookie.. *.. * Copyright 2006, 2015 Klaus Hartl & Fagner Brack.. * Released under the MIT license.. */..; (function (factory) {...var registeredInModuleLoader = false;...if (typeof define === 'function' && define.amd) {....define(factory);....registeredInModuleLoader = true;...}...if (typeof exports === 'object') {....module.exports = factory();....registeredInModuleLoader = true;...}...if (!registeredInModuleLoader) {....var OldCookies = window.Cookies;....var api = window.Cookies = factory();....api.noConflict = function () {.....window.Cookies = OldCookies;.....return api;....};...}..}(function () {...function extend () {....var i = 0;....var result = {};....for (; i < arguments.length; i++) {.....var attributes = arguments[i];.....for (var key in attributes) {......result[key] = attributes[key];.....}....}....return result;...}.....function init (converter) {....function api (key, value, attributes) {.....var res

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\latest[1].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), Segoe UI family
Category:	downloaded
Size (bytes):	35047
Entropy (8bit):	7.975792390307888
Encrypted:	false
SSDEEP:	768:I6ibzTDpOGuAJ63YB9eSzDtQEspfAzyNyuBmOfAJYCM:/iPMYJ4GEAZoTyglcM
MD5:	CAD76E4816AF6890C9BFD02A6D1EA899
SHA1:	9EDC91541C31034FCE0D83AABBAAD4C314CD3D33
SHA-256:	D5794223D1A062E5DBE6C34C1994C8CE3792B24AFD5218D0644CB1F53DA4BE58
SHA-512:	24983A5856C2B4D8CBE2A4BD233A93B266A03D4218942E1D1733B33B65AB7A504AF0AC31DE2F1E69F6FF8CCD7A169CD4555539D34FFF8DE4CB8C98DB2DB2C63

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\latest[1].eot	
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://i.s-microsoft.com/fonts/segoe-ui/west-european/normal/latest.eot?
Preview:	...=.....LP#...B..... .....S.e.g.o.e. .U.I.....R.e.g.u.l.a.r.....V.e.r.s.i.o.n. .5...3.2.....S.e.g.o.e. .U.I.....RV.z..;~.....U.D.-..iu...N4P\..GLFM .Y.?.;..-...~~....Ox.M..".$.._.....g..sC*2..4W.....9AGc.[a..*.rCl,..@..U_..L...e..Ru.J.-.f..3.....S`.A.....K<;...n.Y...rli.....([...W...5k.....^K.G...U.@....2H..B.)N0w.....C..9..... ....#.l2,4..6y.3$b....K.wx...l.$E..?3.8.c...,x..t.wa.O....4.c...!..+.<EM...2T.>\..]4.A.H.;..G.....W.:.?...Z".....e....8....84.L,.)0..y.Xdd.Pa.@.&.o(.I.q.yF...[.y.m(D...(....T.....,A.;q.... .w.$..C..a.. .Y.O?{..0...'1.;C.,.....W..Q-..'.5tD@9..U...E4e.&_...S.Y...\)b.s.rIR.....%..R..KU O..{.0(.....^Q\^!.et...Kf%..K...}.1...S.{.....3p..]...|Y...w..|JeS$..k.....>(8 .ZlV..N.). c...Z.K.\..q.....'S.j.....9...._.E.#s*'#.....[.....DJ^.L7../1...+U.qG.....-..MM..q....L..c...^...:e....<h...:.`.jz..fb.Ha.....k.....e\)g..\."..M

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\latest[2].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), Segoe UI Light family
Category:	downloaded
Size (bytes):	28315
Entropy (8bit):	7.9724193003797
Encrypted:	false
SSDEEP:	384:+R0Z7+bHAtrQ1yBFbgqLct7rJhhPLLkHsrvSzaJu4mI3n5o+MmKCxDg6iT7jdVye:+uNUAtE3phPLLFTiMu+pxCjHyGEQ9zL
MD5:	17DFE73CB9C64527F7248B0A24DB317D
SHA1:	345198B9239FCDAF038FB2D3A919E4724037DBAA
SHA-256:	AD75FB92B2EBCE6C37640F03E1AB96A752F388BCE60C877ADE4780B13839E8C4
SHA-512:	421B56D93E9BD5E4B4449DD0FCDEE8D531087FD484C91530AAF0A67EDEA33D5AC2F14A7F4966C528C0F130F17F26629FCAB9F8AB47E950CEB5B9F1A827EA07 28
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://i.s-microsoft.com/fonts/segoe-ui/west-european/light/latest.eot?
Preview:	.n...m.....LP#...B..... .....S.e.g.o.e. .U.I. .L.i.g.h.t.....R.e.g.u.l.a.r.....V.e.r.s.i.o.n. .5...3.2.....S.e.g.o.e. .U.I. .L.i.g.h.t.....K..e..66.....U.D.-.. iu...4P\..GLFM..C?.;..-...~|...P..\.(..)RI....>.>..CE..SsV.jPR...H.....].R..&.n.hT.....x.....q .....wA[....F.....c."....Zed..>.?...`..3...B..W....R....F.j....v..'?.5.k^.....+..a...).. _].x.#QSi.....|<t....k.;..Hv1.G...L$.9....5.t.:...V.Y.....|.@....B.....P`..2.Z.0....2`.FR.MF8.x....GP0..$:.....PYm.22..."S."1.*j[=.=.mR.*.....j....&.4...k..].1@..y$....."y..C..g7..k.B*. ..V..F\...G.m.jK ...O....b.Qlo...!.N.V....t.[..p.N..~@1d...YX.."....R_i.4.$j.P..U....u9...<..6..4%.....9`.....S...N.Y..L..B$2\.E.vhe...n..h..5..Z..K?.H..S...2..=R..x....EX.2.....$."..... It8..z.+.h ..$.2*T....}Z../....p..b0ae.qq.(-v1..E.!.!".a..p.).;..8t..7..^..W...4A.D\eOb$.....b.NI.Pe.#$.O38....,...g..&|...B{...].....9..u.8..~Y...3.X..ff,,.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\latest[3].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), Segoe UI Semibold family
Category:	downloaded
Size (bytes):	30643
Entropy (8bit):	7.976822258863597
Encrypted:	false
SSDEEP:	768:UOtV1asJ9G0dAdnVrKX/HkVJRPvkgxYZ4Zoe:bLasJ9G0u0fk/RnkgxGof
MD5:	E812BA8B7E2A657F2B70CFACE93C7682
SHA1:	2F02CDDBB483F9B11BBBE74C3CA917A4C345FBAD
SHA-256:	3330C1DEAC468874238DD0C6BF902179A8731EDA8A208C7D01DAC0AB1EAE1BC9
SHA-512:	354B2DB12BC1D67F26F94352B0B663DAD64C46C107454FC19CFEA01C54BB09340BC26C06DE1B96FF826F5287CE246A6317722BAE41B72B63BA86FDAF844BA94 E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://i.s-microsoft.com/fonts/segoe-ui/west-european/semibold/latest.eot?
Preview:	.w...v.....X.....LP#...B..... .....".S.e.g.o.e. .U.I. .S.e.m.i.b.o.l.d.....R.e.g.u.l.a.r.....V.e.r.s.i.o.n. .5...3.2...".S.e.g.o.e. .U.I. .S.e.m.i.b.o.l.d.....H .P..lb.7^.....U.D.-..iu...:4P\..GLFM.Y.#?.;..-...~}_).z{.rmD.1".$.....{.t.....=...!cK...%.~.....g.....j.9S....6. ..n..V.]pz...e.....#X...=,.p.F..6&.VR...k$~J..n....7.....K.8..T.....x..J.....#.J .XaQ.Q%_{3..xr.... 0Dm...k..Ep.....>..?Pk!KB..C...Q.q..1=6<,.S.F.&B..J.....ya2b."S.....6.2.....H.....*..09A...Tb/.&.d..#.E.:.E.(..I5.M..444d.1.....K..l...l.O..VBb...:..:b..Mh.'= 4.d/..o.k.mMm.....bx..!..S.@E.....>@:..k.JCas..7."..uG3hR.h..w..8W>.4.....pX....J..a....}.Y.....(>H^=.`=.mg*.!.....w'...J.<.ob..3A .../.....5%.'....XS0a.....l.Ia....a...=..g..... {V1+..")7$2 O..!bb.=..|.s.1..2qm..#.O.....+E(I..1....EgQ.....E)R.m.?.8.q...J.G.@!f..n.F.r#..(..2p.?.9.8..?.d]..s..0.9.f..A...r.iq....x.g.aO....S.....R0i..BT.yl.".<k...:&Ja.\.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\listAll[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	199361
Entropy (8bit):	4.952858754150251
Encrypted:	false
SSDEEP:	768:trGONW5SpM6JSmm/W2UntbvZPPe+LwgaoK109i6eR9QNJTBARPOin6UubpQF:tiaVm/WtBvM+LwVoK1yk9EJdA9TibpQF
MD5:	DA0BD83A887299F6A4A2B5ACF6C88AF1
SHA1:	A4E5450A42DD41173F0B63A7A24D47152BC0C99E
SHA-256:	4339EF6FC484D48533E9DA01AB8016B060F3C378C63ED58EE5FFD869121FC362
SHA-512:	42C97DB3393A02BFC0120D563D690E7ACBB49D29C7FE9DF683AA2D5CF019A2050A91AA3DB741B3B140EA8BC663468A101844B75353D67B04950D1772BFB854D E

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\listAll[1].json	
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fs.microsoft.com/fs/4.9/listAll.json
Preview:	{"MajorVersion":4,"MinorVersion":9,"Expiration":14,"Fonts":[{"a":[4294967167],"f":"Abadi","fam":[],"sf":[{"c":[1,0],"dn":"Abadi","fs":32696,"ful":[{"lcp":983040,"lsc":"Latn","ltx":"Abadi"}],"gn":"Abadi","id":"23643452060","p":[2,11,6,4,2,1,4,2,2,4],"sub":[],"t":"ttf","u":[2147483651,0,0,0],"v":197263,"w":26215680},{"c":[1,0],"dn":"Abadi Extra Light","fs":22180,"ful":[{"lcp":983041,"lsc":"Latn","ltx":"Abadi Extra Light"}],"gn":"Abadi Extra Light","id":"17656736728","p":[2,11,2,4,2,1,4,2,2,4],"sub":[],"t":"ttf","u":[2147483651,0,0,0],"v":197263,"w":13108480}]},{"a":[4294967167],"f":"Agency FB","fam":[],"sf":[{"c":[536870913,0],"dn":"Agency FB Bold","fs":54372,"ful":[{"lcp":983042,"lsc":"Latn","ltx":"Agency FB"}],"gn":"Agency FB","id":"31150835240","p":[2,11,8,4,2,2,2,2,2,4],"sub":[],"t":"ttf","u":[3,0,0,0],"v":67502,"w":45875968},{"c":[536870913,0],"dn":"Agency FB","fs":52680,"ful":[{"lcp":983042,"lsc":"Latn","ltx":"Agency FB"}],"gn":"Agency FB","id":"29260917085","p":[2,11,5,3,2,2,2,2,2

Static File Info

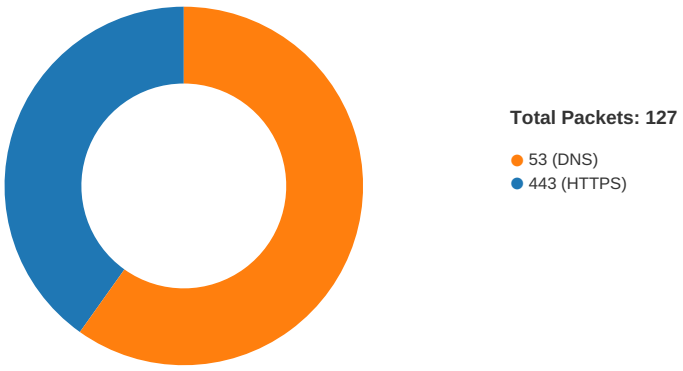
No static file info

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/26/20-14:40:33.786146	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	8.8.8.8

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 14:40:14.562782049 CET	49716	443	192.168.2.3	13.107.42.12
Nov 26, 2020 14:40:14.562849045 CET	49717	443	192.168.2.3	13.107.42.12
Nov 26, 2020 14:40:14.574285984 CET	443	49717	13.107.42.12	192.168.2.3
Nov 26, 2020 14:40:14.574301958 CET	443	49716	13.107.42.12	192.168.2.3
Nov 26, 2020 14:40:14.574462891 CET	49717	443	192.168.2.3	13.107.42.12
Nov 26, 2020 14:40:14.575246096 CET	49716	443	192.168.2.3	13.107.42.12
Nov 26, 2020 14:40:14.580178976 CET	49716	443	192.168.2.3	13.107.42.12
Nov 26, 2020 14:40:14.580182076 CET	49717	443	192.168.2.3	13.107.42.12
Nov 26, 2020 14:40:14.591893911 CET	443	49716	13.107.42.12	192.168.2.3
Nov 26, 2020 14:40:14.591921091 CET	443	49717	13.107.42.12	192.168.2.3
Nov 26, 2020 14:40:14.592797995 CET	443	49717	13.107.42.12	192.168.2.3
Nov 26, 2020 14:40:14.592837095 CET	443	49717	13.107.42.12	192.168.2.3
Nov 26, 2020 14:40:14.592871904 CET	443	49717	13.107.42.12	192.168.2.3
Nov 26, 2020 14:40:14.592905045 CET	443	49717	13.107.42.12	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 14:40:14.592938900 CET	443	49717	13.107.42.12	192.168.2.3
Nov 26, 2020 14:40:14.592966080 CET	443	49717	13.107.42.12	192.168.2.3
Nov 26, 2020 14:40:14.593008995 CET	443	49716	13.107.42.12	192.168.2.3
Nov 26, 2020 14:40:14.593028069 CET	49717	443	192.168.2.3	13.107.42.12
Nov 26, 2020 14:40:14.593046904 CET	443	49716	13.107.42.12	192.168.2.3
Nov 26, 2020 14:40:14.593070030 CET	49717	443	192.168.2.3	13.107.42.12
Nov 26, 2020 14:40:14.593075991 CET	49717	443	192.168.2.3	13.107.42.12
Nov 26, 2020 14:40:14.593080044 CET	49717	443	192.168.2.3	13.107.42.12
Nov 26, 2020 14:40:14.593080997 CET	49716	443	192.168.2.3	13.107.42.12
Nov 26, 2020 14:40:14.593106031 CET	49716	443	192.168.2.3	13.107.42.12
Nov 26, 2020 14:40:14.593122959 CET	443	49716	13.107.42.12	192.168.2.3
Nov 26, 2020 14:40:14.593158960 CET	443	49716	13.107.42.12	192.168.2.3
Nov 26, 2020 14:40:14.593182087 CET	49716	443	192.168.2.3	13.107.42.12
Nov 26, 2020 14:40:14.593216896 CET	443	49716	13.107.42.12	192.168.2.3
Nov 26, 2020 14:40:14.593233109 CET	49716	443	192.168.2.3	13.107.42.12
Nov 26, 2020 14:40:14.593265057 CET	443	49716	13.107.42.12	192.168.2.3
Nov 26, 2020 14:40:14.593274117 CET	49716	443	192.168.2.3	13.107.42.12
Nov 26, 2020 14:40:14.593308926 CET	49716	443	192.168.2.3	13.107.42.12
Nov 26, 2020 14:40:14.629062891 CET	49717	443	192.168.2.3	13.107.42.12
Nov 26, 2020 14:40:14.629170895 CET	49716	443	192.168.2.3	13.107.42.12
Nov 26, 2020 14:40:14.635673046 CET	49716	443	192.168.2.3	13.107.42.12
Nov 26, 2020 14:40:14.635871887 CET	49717	443	192.168.2.3	13.107.42.12
Nov 26, 2020 14:40:14.636102915 CET	49716	443	192.168.2.3	13.107.42.12
Nov 26, 2020 14:40:14.639966965 CET	443	49716	13.107.42.12	192.168.2.3
Nov 26, 2020 14:40:14.640153885 CET	443	49717	13.107.42.12	192.168.2.3
Nov 26, 2020 14:40:14.641673088 CET	443	49717	13.107.42.12	192.168.2.3
Nov 26, 2020 14:40:14.641736984 CET	443	49716	13.107.42.12	192.168.2.3
Nov 26, 2020 14:40:14.641798019 CET	443	49717	13.107.42.12	192.168.2.3
Nov 26, 2020 14:40:14.641834021 CET	49717	443	192.168.2.3	13.107.42.12
Nov 26, 2020 14:40:14.641881943 CET	443	49716	13.107.42.12	192.168.2.3
Nov 26, 2020 14:40:14.641963005 CET	49716	443	192.168.2.3	13.107.42.12
Nov 26, 2020 14:40:14.642031908 CET	49716	443	192.168.2.3	13.107.42.12
Nov 26, 2020 14:40:14.642035007 CET	49717	443	192.168.2.3	13.107.42.12
Nov 26, 2020 14:40:14.642669916 CET	49717	443	192.168.2.3	13.107.42.12
Nov 26, 2020 14:40:14.643204927 CET	49716	443	192.168.2.3	13.107.42.12
Nov 26, 2020 14:40:14.646493912 CET	443	49716	13.107.42.12	192.168.2.3
Nov 26, 2020 14:40:14.646708965 CET	443	49716	13.107.42.12	192.168.2.3
Nov 26, 2020 14:40:14.646755934 CET	443	49717	13.107.42.12	192.168.2.3
Nov 26, 2020 14:40:14.647072077 CET	49716	443	192.168.2.3	13.107.42.12
Nov 26, 2020 14:40:14.652606010 CET	443	49717	13.107.42.12	192.168.2.3
Nov 26, 2020 14:40:14.652771950 CET	49717	443	192.168.2.3	13.107.42.12
Nov 26, 2020 14:40:14.653274059 CET	443	49717	13.107.42.12	192.168.2.3
Nov 26, 2020 14:40:14.653884888 CET	443	49716	13.107.42.12	192.168.2.3
Nov 26, 2020 14:40:14.785336971 CET	443	49716	13.107.42.12	192.168.2.3
Nov 26, 2020 14:40:14.785465002 CET	49716	443	192.168.2.3	13.107.42.12
Nov 26, 2020 14:40:25.814388990 CET	49747	443	192.168.2.3	40.90.142.230
Nov 26, 2020 14:40:25.815265894 CET	49748	443	192.168.2.3	40.90.142.230
Nov 26, 2020 14:40:25.836992025 CET	443	49747	40.90.142.230	192.168.2.3
Nov 26, 2020 14:40:25.837243080 CET	49747	443	192.168.2.3	40.90.142.230
Nov 26, 2020 14:40:25.837589025 CET	443	49748	40.90.142.230	192.168.2.3
Nov 26, 2020 14:40:25.837883949 CET	49748	443	192.168.2.3	40.90.142.230
Nov 26, 2020 14:40:25.838010073 CET	49747	443	192.168.2.3	40.90.142.230
Nov 26, 2020 14:40:25.838449955 CET	49748	443	192.168.2.3	40.90.142.230
Nov 26, 2020 14:40:25.862399101 CET	443	49747	40.90.142.230	192.168.2.3
Nov 26, 2020 14:40:25.862432957 CET	443	49747	40.90.142.230	192.168.2.3
Nov 26, 2020 14:40:25.862454891 CET	443	49747	40.90.142.230	192.168.2.3
Nov 26, 2020 14:40:25.862478018 CET	443	49747	40.90.142.230	192.168.2.3
Nov 26, 2020 14:40:25.862499952 CET	443	49747	40.90.142.230	192.168.2.3
Nov 26, 2020 14:40:25.862515926 CET	443	49747	40.90.142.230	192.168.2.3
Nov 26, 2020 14:40:25.862535954 CET	443	49748	40.90.142.230	192.168.2.3
Nov 26, 2020 14:40:25.862543106 CET	49747	443	192.168.2.3	40.90.142.230
Nov 26, 2020 14:40:25.862556934 CET	443	49748	40.90.142.230	192.168.2.3
Nov 26, 2020 14:40:25.862580061 CET	443	49748	40.90.142.230	192.168.2.3
Nov 26, 2020 14:40:25.862585068 CET	49747	443	192.168.2.3	40.90.142.230

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 14:40:25.862607956 CET	443	49748	40.90.142.230	192.168.2.3
Nov 26, 2020 14:40:25.862632990 CET	443	49748	40.90.142.230	192.168.2.3
Nov 26, 2020 14:40:25.862648010 CET	443	49748	40.90.142.230	192.168.2.3
Nov 26, 2020 14:40:25.862648964 CET	49748	443	192.168.2.3	40.90.142.230
Nov 26, 2020 14:40:25.862653971 CET	49747	443	192.168.2.3	40.90.142.230
Nov 26, 2020 14:40:25.862668991 CET	49748	443	192.168.2.3	40.90.142.230
Nov 26, 2020 14:40:25.862670898 CET	49748	443	192.168.2.3	40.90.142.230
Nov 26, 2020 14:40:25.862689972 CET	49748	443	192.168.2.3	40.90.142.230
Nov 26, 2020 14:40:25.871768951 CET	49748	443	192.168.2.3	40.90.142.230
Nov 26, 2020 14:40:25.872400045 CET	49748	443	192.168.2.3	40.90.142.230
Nov 26, 2020 14:40:25.872858047 CET	49748	443	192.168.2.3	40.90.142.230
Nov 26, 2020 14:40:25.874049902 CET	49747	443	192.168.2.3	40.90.142.230
Nov 26, 2020 14:40:25.874528885 CET	49747	443	192.168.2.3	40.90.142.230
Nov 26, 2020 14:40:25.894567966 CET	443	49748	40.90.142.230	192.168.2.3
Nov 26, 2020 14:40:25.894593000 CET	443	49748	40.90.142.230	192.168.2.3
Nov 26, 2020 14:40:25.894695044 CET	443	49748	40.90.142.230	192.168.2.3
Nov 26, 2020 14:40:25.894763947 CET	49748	443	192.168.2.3	40.90.142.230
Nov 26, 2020 14:40:25.894895077 CET	443	49748	40.90.142.230	192.168.2.3
Nov 26, 2020 14:40:25.894948959 CET	49748	443	192.168.2.3	40.90.142.230
Nov 26, 2020 14:40:25.895869017 CET	49748	443	192.168.2.3	40.90.142.230
Nov 26, 2020 14:40:25.896575928 CET	443	49747	40.90.142.230	192.168.2.3
Nov 26, 2020 14:40:25.896696091 CET	443	49747	40.90.142.230	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 14:40:13.336667061 CET	58361	53	192.168.2.3	8.8.8.8
Nov 26, 2020 14:40:13.383284092 CET	53	58361	8.8.8.8	192.168.2.3
Nov 26, 2020 14:40:14.507101059 CET	63492	53	192.168.2.3	8.8.8.8
Nov 26, 2020 14:40:14.552639008 CET	53	63492	8.8.8.8	192.168.2.3
Nov 26, 2020 14:40:14.803109884 CET	60831	53	192.168.2.3	8.8.8.8
Nov 26, 2020 14:40:14.830144882 CET	53	60831	8.8.8.8	192.168.2.3
Nov 26, 2020 14:40:17.699899912 CET	60100	53	192.168.2.3	8.8.8.8
Nov 26, 2020 14:40:17.726972103 CET	53	60100	8.8.8.8	192.168.2.3
Nov 26, 2020 14:40:18.953036070 CET	53195	53	192.168.2.3	8.8.8.8
Nov 26, 2020 14:40:18.973664999 CET	50141	53	192.168.2.3	8.8.8.8
Nov 26, 2020 14:40:18.999811888 CET	53	53195	8.8.8.8	192.168.2.3
Nov 26, 2020 14:40:19.019496918 CET	53	50141	8.8.8.8	192.168.2.3
Nov 26, 2020 14:40:19.983191013 CET	53023	53	192.168.2.3	8.8.8.8
Nov 26, 2020 14:40:20.028734922 CET	53	53023	8.8.8.8	192.168.2.3
Nov 26, 2020 14:40:20.201457977 CET	49563	53	192.168.2.3	8.8.8.8
Nov 26, 2020 14:40:20.213255882 CET	51352	53	192.168.2.3	8.8.8.8
Nov 26, 2020 14:40:20.248091936 CET	53	49563	8.8.8.8	192.168.2.3
Nov 26, 2020 14:40:20.258860111 CET	53	51352	8.8.8.8	192.168.2.3
Nov 26, 2020 14:40:20.614006042 CET	59349	53	192.168.2.3	8.8.8.8
Nov 26, 2020 14:40:20.664223909 CET	53	59349	8.8.8.8	192.168.2.3
Nov 26, 2020 14:40:23.257147074 CET	57084	53	192.168.2.3	8.8.8.8
Nov 26, 2020 14:40:23.304420948 CET	53	57084	8.8.8.8	192.168.2.3
Nov 26, 2020 14:40:23.464809895 CET	58823	53	192.168.2.3	8.8.8.8
Nov 26, 2020 14:40:23.511647940 CET	53	58823	8.8.8.8	192.168.2.3
Nov 26, 2020 14:40:23.784887075 CET	57568	53	192.168.2.3	8.8.8.8
Nov 26, 2020 14:40:23.811955929 CET	53	57568	8.8.8.8	192.168.2.3
Nov 26, 2020 14:40:24.820908070 CET	50540	53	192.168.2.3	8.8.8.8
Nov 26, 2020 14:40:24.848159075 CET	53	50540	8.8.8.8	192.168.2.3
Nov 26, 2020 14:40:25.139378071 CET	54366	53	192.168.2.3	8.8.8.8
Nov 26, 2020 14:40:25.166757107 CET	53	54366	8.8.8.8	192.168.2.3
Nov 26, 2020 14:40:25.473872900 CET	53034	53	192.168.2.3	8.8.8.8
Nov 26, 2020 14:40:25.530191898 CET	53	53034	8.8.8.8	192.168.2.3
Nov 26, 2020 14:40:25.767246008 CET	57762	53	192.168.2.3	8.8.8.8
Nov 26, 2020 14:40:25.812499046 CET	53	57762	8.8.8.8	192.168.2.3
Nov 26, 2020 14:40:31.629445076 CET	55435	53	192.168.2.3	8.8.8.8
Nov 26, 2020 14:40:31.674916983 CET	53	55435	8.8.8.8	192.168.2.3
Nov 26, 2020 14:40:31.735263109 CET	50713	53	192.168.2.3	8.8.8.8
Nov 26, 2020 14:40:31.837295055 CET	56132	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 14:40:31.882802963 CET	53	56132	8.8.8.8	192.168.2.3
Nov 26, 2020 14:40:31.896162033 CET	58987	53	192.168.2.3	8.8.8.8
Nov 26, 2020 14:40:31.923216105 CET	53	58987	8.8.8.8	192.168.2.3
Nov 26, 2020 14:40:32.440154076 CET	56579	53	192.168.2.3	8.8.8.8
Nov 26, 2020 14:40:32.467514038 CET	53	56579	8.8.8.8	192.168.2.3
Nov 26, 2020 14:40:32.736994982 CET	50713	53	192.168.2.3	8.8.8.8
Nov 26, 2020 14:40:32.798077106 CET	53	50713	8.8.8.8	192.168.2.3
Nov 26, 2020 14:40:33.151782990 CET	60633	53	192.168.2.3	8.8.8.8
Nov 26, 2020 14:40:33.170265913 CET	61292	53	192.168.2.3	8.8.8.8
Nov 26, 2020 14:40:33.178905964 CET	53	60633	8.8.8.8	192.168.2.3
Nov 26, 2020 14:40:33.215476036 CET	53	61292	8.8.8.8	192.168.2.3
Nov 26, 2020 14:40:33.616030931 CET	63619	53	192.168.2.3	8.8.8.8
Nov 26, 2020 14:40:33.672452927 CET	53	63619	8.8.8.8	192.168.2.3
Nov 26, 2020 14:40:33.786037922 CET	53	50713	8.8.8.8	192.168.2.3
Nov 26, 2020 14:40:34.108462095 CET	64938	53	192.168.2.3	8.8.8.8
Nov 26, 2020 14:40:34.119544029 CET	61946	53	192.168.2.3	8.8.8.8
Nov 26, 2020 14:40:34.155064106 CET	53	64938	8.8.8.8	192.168.2.3
Nov 26, 2020 14:40:34.166379929 CET	53	61946	8.8.8.8	192.168.2.3
Nov 26, 2020 14:40:35.830527067 CET	64910	53	192.168.2.3	8.8.8.8
Nov 26, 2020 14:40:35.877645969 CET	53	64910	8.8.8.8	192.168.2.3
Nov 26, 2020 14:40:36.211718082 CET	52123	53	192.168.2.3	8.8.8.8
Nov 26, 2020 14:40:36.238872051 CET	53	52123	8.8.8.8	192.168.2.3
Nov 26, 2020 14:40:37.680465937 CET	56130	53	192.168.2.3	8.8.8.8
Nov 26, 2020 14:40:37.707468033 CET	53	56130	8.8.8.8	192.168.2.3
Nov 26, 2020 14:40:39.698646069 CET	56338	53	192.168.2.3	8.8.8.8
Nov 26, 2020 14:40:39.725841999 CET	53	56338	8.8.8.8	192.168.2.3
Nov 26, 2020 14:40:40.109014034 CET	59420	53	192.168.2.3	8.8.8.8
Nov 26, 2020 14:40:40.155265093 CET	53	59420	8.8.8.8	192.168.2.3
Nov 26, 2020 14:40:43.331428051 CET	58784	53	192.168.2.3	8.8.8.8
Nov 26, 2020 14:40:43.358892918 CET	53	58784	8.8.8.8	192.168.2.3
Nov 26, 2020 14:40:44.069576979 CET	63978	53	192.168.2.3	8.8.8.8
Nov 26, 2020 14:40:44.115391016 CET	53	63978	8.8.8.8	192.168.2.3
Nov 26, 2020 14:40:44.345813990 CET	58784	53	192.168.2.3	8.8.8.8
Nov 26, 2020 14:40:44.373003006 CET	53	58784	8.8.8.8	192.168.2.3
Nov 26, 2020 14:40:45.071532965 CET	63978	53	192.168.2.3	8.8.8.8
Nov 26, 2020 14:40:45.099056005 CET	53	63978	8.8.8.8	192.168.2.3
Nov 26, 2020 14:40:45.352881908 CET	58784	53	192.168.2.3	8.8.8.8
Nov 26, 2020 14:40:45.380130053 CET	53	58784	8.8.8.8	192.168.2.3
Nov 26, 2020 14:40:46.087264061 CET	63978	53	192.168.2.3	8.8.8.8
Nov 26, 2020 14:40:46.114514112 CET	53	63978	8.8.8.8	192.168.2.3
Nov 26, 2020 14:40:48.111943007 CET	63978	53	192.168.2.3	8.8.8.8
Nov 26, 2020 14:40:48.129220009 CET	58784	53	192.168.2.3	8.8.8.8
Nov 26, 2020 14:40:48.157979012 CET	53	63978	8.8.8.8	192.168.2.3
Nov 26, 2020 14:40:48.174525023 CET	53	58784	8.8.8.8	192.168.2.3
Nov 26, 2020 14:40:52.116092920 CET	63978	53	192.168.2.3	8.8.8.8
Nov 26, 2020 14:40:52.143495083 CET	53	63978	8.8.8.8	192.168.2.3
Nov 26, 2020 14:40:52.165651083 CET	58784	53	192.168.2.3	8.8.8.8
Nov 26, 2020 14:40:52.192981958 CET	53	58784	8.8.8.8	192.168.2.3
Nov 26, 2020 14:40:57.372493982 CET	62938	53	192.168.2.3	8.8.8.8
Nov 26, 2020 14:40:57.440826893 CET	53	62938	8.8.8.8	192.168.2.3
Nov 26, 2020 14:40:59.334619999 CET	55708	53	192.168.2.3	8.8.8.8
Nov 26, 2020 14:40:59.384182930 CET	53	55708	8.8.8.8	192.168.2.3
Nov 26, 2020 14:40:59.948350906 CET	56803	53	192.168.2.3	8.8.8.8
Nov 26, 2020 14:40:59.975709915 CET	53	56803	8.8.8.8	192.168.2.3
Nov 26, 2020 14:41:00.608026981 CET	57145	53	192.168.2.3	8.8.8.8
Nov 26, 2020 14:41:00.622314930 CET	55359	53	192.168.2.3	8.8.8.8
Nov 26, 2020 14:41:00.654850006 CET	53	57145	8.8.8.8	192.168.2.3
Nov 26, 2020 14:41:00.678361893 CET	53	55359	8.8.8.8	192.168.2.3
Nov 26, 2020 14:41:01.082973003 CET	58306	53	192.168.2.3	8.8.8.8
Nov 26, 2020 14:41:01.110318899 CET	53	58306	8.8.8.8	192.168.2.3
Nov 26, 2020 14:41:01.296590090 CET	64124	53	192.168.2.3	8.8.8.8
Nov 26, 2020 14:41:01.414659977 CET	53	64124	8.8.8.8	192.168.2.3
Nov 26, 2020 14:41:01.620932102 CET	49361	53	192.168.2.3	8.8.8.8
Nov 26, 2020 14:41:01.666518927 CET	53	49361	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 14:41:01.811734915 CET	63150	53	192.168.2.3	8.8.8.8
Nov 26, 2020 14:41:01.838740110 CET	53	63150	8.8.8.8	192.168.2.3
Nov 26, 2020 14:41:02.494823933 CET	53279	53	192.168.2.3	8.8.8.8
Nov 26, 2020 14:41:02.540374994 CET	53	53279	8.8.8.8	192.168.2.3
Nov 26, 2020 14:41:03.359755993 CET	56881	53	192.168.2.3	8.8.8.8
Nov 26, 2020 14:41:03.406387091 CET	53	56881	8.8.8.8	192.168.2.3
Nov 26, 2020 14:41:03.426532984 CET	53642	53	192.168.2.3	8.8.8.8
Nov 26, 2020 14:41:03.472176075 CET	53	53642	8.8.8.8	192.168.2.3
Nov 26, 2020 14:41:03.669939041 CET	55667	53	192.168.2.3	8.8.8.8
Nov 26, 2020 14:41:03.716370106 CET	53	55667	8.8.8.8	192.168.2.3
Nov 26, 2020 14:41:05.228096008 CET	54833	53	192.168.2.3	8.8.8.8
Nov 26, 2020 14:41:05.234703064 CET	62476	53	192.168.2.3	8.8.8.8
Nov 26, 2020 14:41:05.264049053 CET	61477	53	192.168.2.3	8.8.8.8
Nov 26, 2020 14:41:05.264374018 CET	49705	53	192.168.2.3	8.8.8.8
Nov 26, 2020 14:41:05.273869038 CET	53	54833	8.8.8.8	192.168.2.3
Nov 26, 2020 14:41:05.276420116 CET	61633	53	192.168.2.3	8.8.8.8
Nov 26, 2020 14:41:05.283117056 CET	53	62476	8.8.8.8	192.168.2.3
Nov 26, 2020 14:41:05.311238050 CET	53	49705	8.8.8.8	192.168.2.3
Nov 26, 2020 14:41:05.312323093 CET	53	61477	8.8.8.8	192.168.2.3
Nov 26, 2020 14:41:05.323446989 CET	53	61633	8.8.8.8	192.168.2.3
Nov 26, 2020 14:41:05.440515995 CET	55949	53	192.168.2.3	8.8.8.8
Nov 26, 2020 14:41:05.487241983 CET	53	55949	8.8.8.8	192.168.2.3
Nov 26, 2020 14:41:06.364921093 CET	57601	53	192.168.2.3	8.8.8.8
Nov 26, 2020 14:41:06.412328005 CET	53	57601	8.8.8.8	192.168.2.3
Nov 26, 2020 14:41:08.180655956 CET	49342	53	192.168.2.3	8.8.8.8
Nov 26, 2020 14:41:08.207992077 CET	53	49342	8.8.8.8	192.168.2.3
Nov 26, 2020 14:41:08.877105951 CET	56253	53	192.168.2.3	8.8.8.8
Nov 26, 2020 14:41:08.904397964 CET	53	56253	8.8.8.8	192.168.2.3
Nov 26, 2020 14:41:09.607166052 CET	49667	53	192.168.2.3	8.8.8.8
Nov 26, 2020 14:41:09.634301901 CET	53	49667	8.8.8.8	192.168.2.3
Nov 26, 2020 14:41:10.297075033 CET	55439	53	192.168.2.3	8.8.8.8
Nov 26, 2020 14:41:10.324141979 CET	53	55439	8.8.8.8	192.168.2.3
Nov 26, 2020 14:41:10.939915895 CET	57069	53	192.168.2.3	8.8.8.8
Nov 26, 2020 14:41:10.967152119 CET	53	57069	8.8.8.8	192.168.2.3
Nov 26, 2020 14:41:12.128084898 CET	57659	53	192.168.2.3	8.8.8.8
Nov 26, 2020 14:41:12.173511028 CET	53	57659	8.8.8.8	192.168.2.3
Nov 26, 2020 14:41:13.896984100 CET	54717	53	192.168.2.3	8.8.8.8
Nov 26, 2020 14:41:13.951055050 CET	53	54717	8.8.8.8	192.168.2.3
Nov 26, 2020 14:41:16.233086109 CET	63975	53	192.168.2.3	8.8.8.8
Nov 26, 2020 14:41:16.286398888 CET	53	63975	8.8.8.8	192.168.2.3
Nov 26, 2020 14:41:28.537098885 CET	56639	53	192.168.2.3	8.8.8.8
Nov 26, 2020 14:41:28.564197063 CET	53	56639	8.8.8.8	192.168.2.3
Nov 26, 2020 14:41:29.730417967 CET	56639	53	192.168.2.3	8.8.8.8
Nov 26, 2020 14:41:29.775523901 CET	53	56639	8.8.8.8	192.168.2.3
Nov 26, 2020 14:41:30.717890978 CET	56639	53	192.168.2.3	8.8.8.8
Nov 26, 2020 14:41:30.745166063 CET	53	56639	8.8.8.8	192.168.2.3
Nov 26, 2020 14:41:32.727633953 CET	56639	53	192.168.2.3	8.8.8.8
Nov 26, 2020 14:41:32.755002022 CET	53	56639	8.8.8.8	192.168.2.3
Nov 26, 2020 14:41:36.729896069 CET	56639	53	192.168.2.3	8.8.8.8
Nov 26, 2020 14:41:36.775257111 CET	53	56639	8.8.8.8	192.168.2.3

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Nov 26, 2020 14:40:33.786145926 CET	192.168.2.3	8.8.8.8	d047	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 26, 2020 14:40:14.507101059 CET	192.168.2.3	8.8.8.8	0xa89e	Standard query (0)	1drv.ms	A (IP address)	IN (0x0001)
Nov 26, 2020 14:40:14.803109884 CET	192.168.2.3	8.8.8.8	0xea97	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 26, 2020 14:40:18.953036070 CET	192.168.2.3	8.8.8.8	0x8c27	Standard query (0)	spoprod-a.akamaihd.net	A (IP address)	IN (0x0001)
Nov 26, 2020 14:40:18.973664999 CET	192.168.2.3	8.8.8.8	0x2dbd	Standard query (0)	p.sfx.ms	A (IP address)	IN (0x0001)
Nov 26, 2020 14:40:20.614006042 CET	192.168.2.3	8.8.8.8	0xd7c7	Standard query (0)	onenoteonlinesync.onenote.com	A (IP address)	IN (0x0001)
Nov 26, 2020 14:40:25.139378071 CET	192.168.2.3	8.8.8.8	0x4a63	Standard query (0)	messaging.office.com	A (IP address)	IN (0x0001)
Nov 26, 2020 14:40:25.473872900 CET	192.168.2.3	8.8.8.8	0xaddd	Standard query (0)	site-cdn.onenote.net	A (IP address)	IN (0x0001)
Nov 26, 2020 14:40:25.767246008 CET	192.168.2.3	8.8.8.8	0x8f9c	Standard query (0)	skyapi.onedrive.live.com	A (IP address)	IN (0x0001)
Nov 26, 2020 14:40:31.629445076 CET	192.168.2.3	8.8.8.8	0x2e8b	Standard query (0)	c.live.com	A (IP address)	IN (0x0001)
Nov 26, 2020 14:40:31.735263109 CET	192.168.2.3	8.8.8.8	0x9e96	Standard query (0)	ajax.aspnetcdn.com	A (IP address)	IN (0x0001)
Nov 26, 2020 14:40:32.736994982 CET	192.168.2.3	8.8.8.8	0x9e96	Standard query (0)	ajax.aspnetcdn.com	A (IP address)	IN (0x0001)
Nov 26, 2020 14:40:33.616030931 CET	192.168.2.3	8.8.8.8	0x262e	Standard query (0)	www.onenote.com	A (IP address)	IN (0x0001)
Nov 26, 2020 14:40:34.108462095 CET	192.168.2.3	8.8.8.8	0x36b9	Standard query (0)	cdn.onenote.net	A (IP address)	IN (0x0001)
Nov 26, 2020 14:40:59.334619999 CET	192.168.2.3	8.8.8.8	0x94cc	Standard query (0)	wonderwaterbeads.com	A (IP address)	IN (0x0001)
Nov 26, 2020 14:41:00.608026981 CET	192.168.2.3	8.8.8.8	0x14a2	Standard query (0)	static.sharepointonline.com	A (IP address)	IN (0x0001)
Nov 26, 2020 14:41:00.622314930 CET	192.168.2.3	8.8.8.8	0xdde0	Standard query (0)	spoprod-a.akamaihd.net	A (IP address)	IN (0x0001)
Nov 26, 2020 14:41:01.296590090 CET	192.168.2.3	8.8.8.8	0x8378	Standard query (0)	vikinggenetics-my.sharepoint.com	A (IP address)	IN (0x0001)
Nov 26, 2020 14:41:01.620932102 CET	192.168.2.3	8.8.8.8	0x3f01	Standard query (0)	wonderwaterbeads.com	A (IP address)	IN (0x0001)
Nov 26, 2020 14:41:05.228096008 CET	192.168.2.3	8.8.8.8	0xcf36	Standard query (0)	ajax.aspnetcdn.com	A (IP address)	IN (0x0001)
Nov 26, 2020 14:41:05.276420116 CET	192.168.2.3	8.8.8.8	0x5ceb	Standard query (0)	assets.onestore.ms	A (IP address)	IN (0x0001)
Nov 26, 2020 14:41:16.233086109 CET	192.168.2.3	8.8.8.8	0x7fe6	Standard query (0)	g.msn.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 26, 2020 14:40:14.552639008 CET	8.8.8.8	192.168.2.3	0xa89e	No error (0)	1drv.ms		13.107.42.12	A (IP address)	IN (0x0001)
Nov 26, 2020 14:40:14.830144882 CET	8.8.8.8	192.168.2.3	0xea97	No error (0)	onedrive.live.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 14:40:18.999811888 CET	8.8.8.8	192.168.2.3	0x8c27	No error (0)	spoprod-a.akamaihd.net	spoprod-a.akamaihd.net.edgesuite.net		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 14:40:19.019496918 CET	8.8.8.8	192.168.2.3	0x2dbd	No error (0)	p.sfx.ms	odwebp.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 14:40:20.664223909 CET	8.8.8.8	192.168.2.3	0xd7c7	No error (0)	onenoteonlinesync.onenote.com	prod.onenoteonlinesync-onenote.com.akadns.net		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 14:40:25.166757107 CET	8.8.8.8	192.168.2.3	0x4a63	No error (0)	messaging.office.com	omexmessaging.osi.office.net		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 14:40:25.530191898 CET	8.8.8.8	192.168.2.3	0xaddd	No error (0)	site-cdn.onenote.net	site-cdn.onenote.net.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 14:40:25.812499046 CET	8.8.8.8	192.168.2.3	0x8f9c	No error (0)	skyapi.onedrive.live.com	common-geo.ha.1drv.com		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 14:40:25.812499046 CET	8.8.8.8	192.168.2.3	0x8f9c	No error (0)	common-geo.ha.1drv.com	common-geo.onedrive.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 14:40:25.812499046 CET	8.8.8.8	192.168.2.3	0x8f9c	No error (0)	am3pcor001-com.be.1drv.com	i-am3p-cor001.api.p001.1drv.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 26, 2020 14:40:25.812499046 CET	8.8.8.8	192.168.2.3	0x8f9c	No error (0)	i-am3p-cor001.api.p001.1drv.com		40.90.142.230	A (IP address)	IN (0x0001)
Nov 26, 2020 14:40:31.674916983 CET	8.8.8.8	192.168.2.3	0x2e8b	No error (0)	c.live.com	c.msn.com		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 14:40:31.674916983 CET	8.8.8.8	192.168.2.3	0x2e8b	No error (0)	c.msn.com	c-msn-com-nsatc.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 14:40:32.798077106 CET	8.8.8.8	192.168.2.3	0x9e96	No error (0)	ajax.aspnetcdn.com	mscomajax.vo.msecnd.net		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 14:40:33.672452927 CET	8.8.8.8	192.168.2.3	0x262e	No error (0)	www.onenote.com	prod.reverseproxy-onenote.com.akadns.net		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 14:40:33.786037922 CET	8.8.8.8	192.168.2.3	0x9e96	No error (0)	ajax.aspnetcdn.com	mscomajax.vo.msecnd.net		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 14:40:34.155064106 CET	8.8.8.8	192.168.2.3	0x36b9	No error (0)	cdn.onenote.net	cdn.onenote.net.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 14:40:59.384182930 CET	8.8.8.8	192.168.2.3	0x94cc	No error (0)	wonderwaterbeads.com		162.241.117.173	A (IP address)	IN (0x0001)
Nov 26, 2020 14:41:00.654850006 CET	8.8.8.8	192.168.2.3	0x14a2	No error (0)	static.sharepointonline.com	static.sharepointonline.com-c.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 14:41:00.678361893 CET	8.8.8.8	192.168.2.3	0xdde0	No error (0)	spoprod-a.akamaihd.net	spoprod-a.akamaihd.net.edgesuite.net		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 14:41:01.414659977 CET	8.8.8.8	192.168.2.3	0x8378	No error (0)	vikinggenetics-my.sharepoint.com	vikinggenetics.sharepoint.com		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 14:41:01.414659977 CET	8.8.8.8	192.168.2.3	0x8378	No error (0)	vikinggenetics.sharepoint.com	614-ipv4e.clump.prod.aa-rt.sharepoint.com		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 14:41:01.414659977 CET	8.8.8.8	192.168.2.3	0x8378	No error (0)	614-ipv4e.clump.prod.aa-rt.sharepoint.com	17825-ipv4e.farm.prod.aa-rt.sharepoint.com		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 14:41:01.414659977 CET	8.8.8.8	192.168.2.3	0x8378	No error (0)	17825-ipv4e.farm.prod.aa-rt.sharepoint.com	17825-ipv4e.farm.prod.sharepointonline.com.akadns.net		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 14:41:01.666518927 CET	8.8.8.8	192.168.2.3	0x3f01	No error (0)	wonderwaterbeads.com		162.241.117.173	A (IP address)	IN (0x0001)
Nov 26, 2020 14:41:05.273869038 CET	8.8.8.8	192.168.2.3	0xcf36	No error (0)	ajax.aspnetcdn.com	mscomajax.vo.msecnd.net		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 14:41:05.323446989 CET	8.8.8.8	192.168.2.3	0x5ceb	No error (0)	assets.onestore.ms	assets.onestore.ms.akadns.net		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 14:41:16.286398888 CET	8.8.8.8	192.168.2.3	0x7fe6	No error (0)	g.msn.com	g-msn-com-nsatc.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Nov 26, 2020 14:40:59.819556952 CET	162.241.117.173	443	192.168.2.3	49779	CN=wonderwaterbeads.com CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon Nov 23 01:00:00 CET 2020 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Mon Feb 22 00:59:59 CET 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
Nov 26, 2020 14:40:59.819797993 CET	162.241.117.173	443	192.168.2.3	49780	CN=wonderwaterbeads.com CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon Nov 23 01:00:00 CET 2020 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Mon Feb 22 00:59:59 CET 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
Nov 26, 2020 14:41:01.940943003 CET	162.241.117.173	443	192.168.2.3	49793	CN=wonderwaterbeads.com CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon Nov 23 01:00:00 CET 2020 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Mon Feb 22 00:59:59 CET 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 5908 Parent PID: 792

General

Start time:	14:40:12
Start date:	26/11/2020
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff7f4640000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: iexplore.exe PID: 1200 Parent PID: 5908

General

Start time:	14:40:13
Start date:	26/11/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5908 CREDAT:17410 /prefetch:2
Imagebase:	0xa40000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: dllhost.exe PID: 1240 Parent PID: 792

General

Start time:	14:40:35
Start date:	26/11/2020
Path:	C:\Windows\System32\dllhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\DllHost.exe /Processid:{49F171DD-B51A-40D3-9A6C-52D674CC729D}
Imagebase:	0x7ff7bc440000
File size:	20888 bytes
MD5 hash:	2528137C6745C4EADD87817A1909677E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: explorer.exe PID: 3388 Parent PID: 1240

General

Start time:	14:40:37
Start date:	26/11/2020
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff714890000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 6896 Parent PID: 5908

General

Start time:	14:40:57
Start date:	26/11/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5908 CREDAT:82960 /prefetch:2
Imagebase:	0xa40000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis