



ID: 321201
Cookbook: browseurl.jbs
Time: 15:39:52
Date: 20/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

Table of Contents 2

Analysis Report https://eagleeyeproduce-my.sharepoint.com/:o:/p/mckrayp/EtopxtQDn3pOqhvY4g_gG3ABKX9ornSoGNhGOLlXyaU89Q?e=Ee0wW2 4

- Overview 4
  - General Information 4
  - Detection 4
  - Signatures 4
  - Classification 4
- Startup 4
- Malware Configuration 4
- Yara Overview 4
  - Dropped Files 4
- Sigma Overview 4
- Signature Overview 5
  - AV Detection: 5
  - Phishing: 5
- Mitre Att&ck Matrix 5
- Behavior Graph 5
- Screenshots 6
  - Thumbnails 6
- Antivirus, Machine Learning and Genetic Malware Detection 7
  - Initial Sample 7
  - Dropped Files 7
  - Unpacked PE Files 7
  - Domains 7
  - URLs 8
- Domains and IPs 9
  - Contacted Domains 9
  - Contacted URLs 10
  - URLs from Memory and Binaries 10
  - Contacted IPs 16
  - Public 17
- General Information 17
- Simulations 19
  - Behavior and APIs 19
- Joe Sandbox View / Context 19
  - IPs 19
  - Domains 19
  - ASN 19
  - JA3 Fingerprints 19
  - Dropped Files 19
- Created / dropped Files 19
- Static File Info 52
  - No static file info 52
- Network Behavior 52
  - Network Port Distribution 53
  - TCP Packets 53
  - UDP Packets 54
  - DNS Queries 56
  - DNS Answers 57
  - HTTPS Packets 57
- Code Manipulations 59
- Statistics 59
  - Behavior 59
- System Behavior 60
  - Analysis Process: iexplore.exe PID: 6716 Parent PID: 792 60
    - General 60
    - File Activities 60
    - Registry Activities 60
  - Analysis Process: iexplore.exe PID: 6764 Parent PID: 6716 60
    - General 60
    - File Activities 61
    - Registry Activities 61
  - Analysis Process: dllhost.exe PID: 5212 Parent PID: 792 61
    - General 61
    - File Activities 61
  - Analysis Process: explorer.exe PID: 3440 Parent PID: 5212 61
    - General 61
    - File Activities 61

Analysis Process: iexplore.exe PID: 5912 Parent PID: 6716 62
General 62
File Activities 62
Disassembly 62
Code Analysis 62

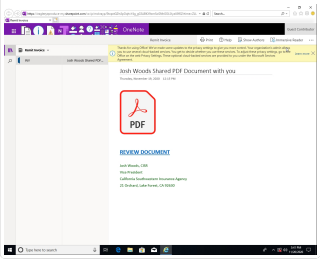
Analysis Report https://eagleeyeproduce-my.sharepoint…

Overview

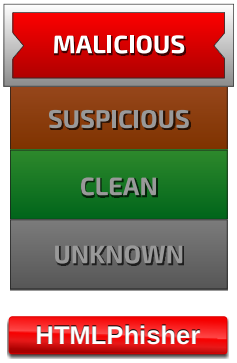
General Information

Sample URL:	http://https://eagleeyeproduce-my.sharepoint.com/:o:/p/mckrayp/EtopxtQDn3pOqhvY4g_gG3ABKX9ornSoGNhGOLlXyaU89Q?e=Ee0wW2
Analysis ID:	321201

Most interesting Screenshot:



Detection

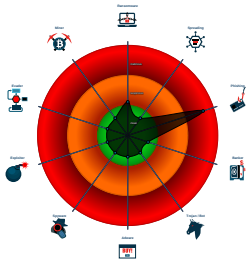


Score:	80
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for URL or domain
- Yara detected HtmlPhish_7
- Yara detected obfuscated html page
- Phishing site detected (based on im…
- Phishing site detected (based on log…
- HTML body contains low number of …
- HTML title does not match URL
- Invalid T&C link found
- Yara detected Encrypted html page …

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 6716 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6764 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6716 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 5912 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6716 CREDAT:17432 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- dllhost.exe (PID: 5212 cmdline: C:\Windows\system32\DllHost.exe /Processid:{49F171DD-B51A-40D3-9A6C-52D674CC729D} MD5: 2528137C6745C4EADD87817A1909677E)
  - explorer.exe (PID: 3440 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Dropped Files

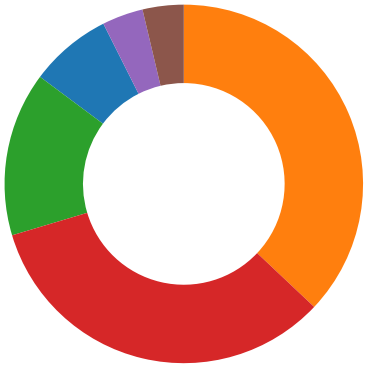
Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\OM9u8[1].htm	JoeSecurity_Obshtml	Yara detected obfuscated html page	Joe Security	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\OM9u8[1].htm	JoeSecurity_Encryptedhtml	Yara detected Encrypted html page by third party sevices	Joe Security	

Sigma Overview

No Sigma rule has matched

Copyright null 2020

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 / Scanner detection for submitted sample

Antivirus detection for URL or domain

Phishing:



Yara detected HtmlPhish_7

Yara detected obfuscated html page

Phishing site detected (based on image similarity)

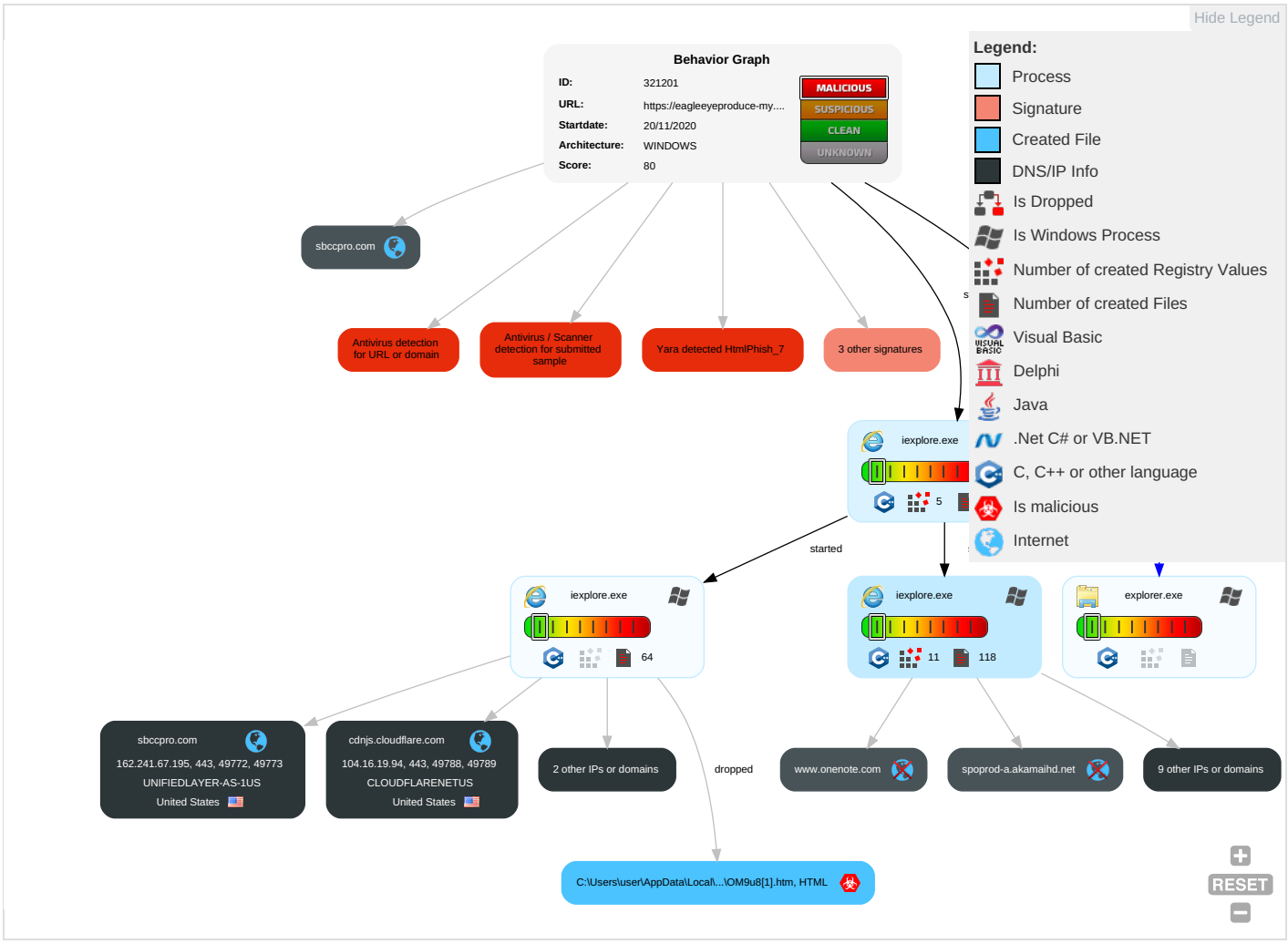
Phishing site detected (based on logo template match)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impac
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 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	Modif Syste 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	Devic Lockc
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	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	Delet Devic Data

Behavior Graph

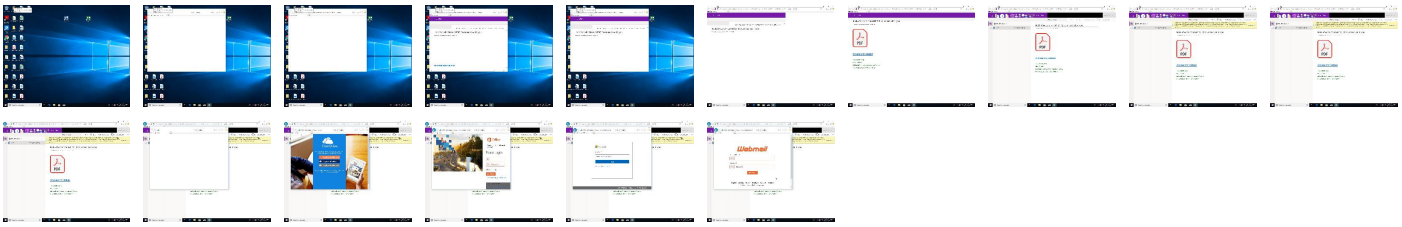
Copyright null 2020

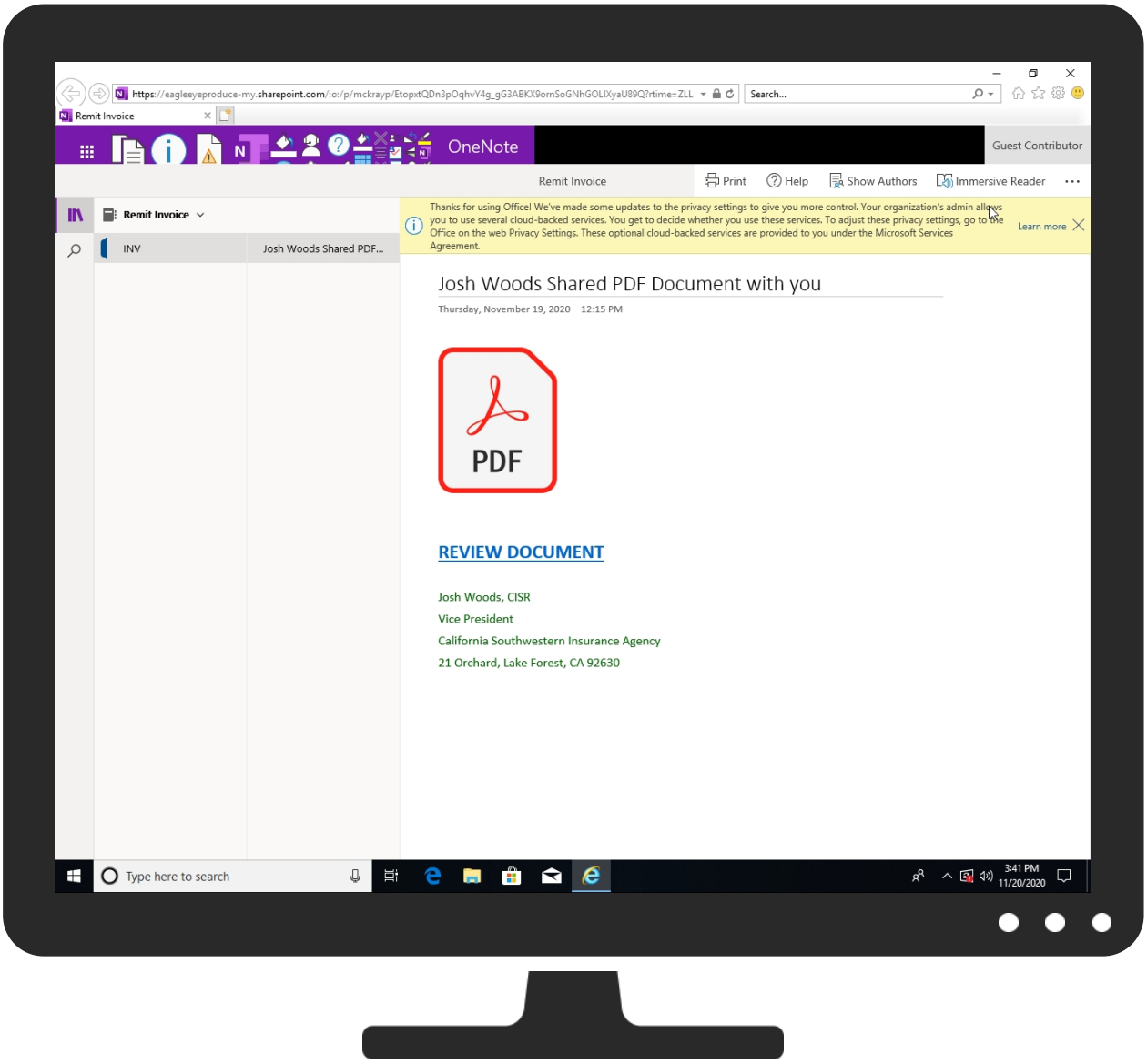


Screenshots

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://eagleeyeproduce-my.sharepoint.com/:o:/p/mckrayp/EtopxtQDn3pOqhvY4g_gG3ABKX9ornSoGNhGOLlXyaU89Q?e=Ee0wW2	5%	Virustotal		Browse
http://https://eagleeyeproduce-my.sharepoint.com/:o:/p/mckrayp/EtopxtQDn3pOqhvY4g_gG3ABKX9ornSoGNhGOLlXyaU89Q?e=Ee0wW2	0%	Avira URL Cloud	safe	
http://https://eagleeyeproduce-my.sharepoint.com/:o:/p/mckrayp/EtopxtQDn3pOqhvY4g_gG3ABKX9ornSoGNhGOLlXyaU89Q?e=Ee0wW2	100%	SlashNext	Fake Login Page type: Phishing & Social usering	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
eagleeyeproduce-my.sharepoint.com	0%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
site-cdn.onenote.net	0%	Virustotal		Browse
cdn.onenote.net	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://eagleeyeproduce-my.sharepoint.com/personal/mckrayp_eagleeyeproduce_com/_layouts/15/Doc.aspx?sourcedoc={d4c629da-9f03-4e7a-aa1b-d8e20fe01b70}&action=view&wd=target%28INV.one%7C599a019e-a35f-45c7-9412-5dae347e7e53%2FJosh%20Woods%C2%A0Shared%20PDF%20Document%20with%20you%7C442b4d04-5062-47cb-8554-05bc78fc39be%2F%29	100%	SlashNext	Fake Login Page type: Phishing & Social usering	
http://https://sbccpro.com/OMMOM/OM9u8/Othermail.php	100%	SlashNext	Fake Login Page type: Phishing & Social usering	
http://https://sbccpro.com/OMMOM/OM9u8	100%	SlashNext	Fake Login Page type: Phishing & Social usering	
http://https://sbccpro.com/OMMOM/OM9u8/Office365.php	100%	SlashNext	Fake Login Page type: Phishing & Social usering	
http://https://sbccpro.com/OMMOM/OM9u8	100%	UrlScan	phishing brand: onedrive	Browse
http://https://sbccpro.com/OMMOM/OM9u8/Outlook.php	100%	SlashNext	Fake Login Page type: Phishing & Social usering	
http://https://sbccpro.com/OMMOM/OM9u8/Office365.php	100%	UrlScan	phishing brand: office 365	Browse
http://https://sbccpro.com/OMMOM/OM9u8/Outlook.php	100%	UrlScan	phishing brand: 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.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.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://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://https://eagleeyeproduce-my.sharepoint.com/personal/mckrayp_eagleep	0%	Avira URL Cloud	safe	
http://https://sbccpro.com/OMMOM/OM9u8/Othermail.php9u8/	100%	Avira URL Cloud	phishing	
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://https://eagleeyeproduce-my.sharepoint.com/favicon.ico	0%	Avira URL Cloud	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://https://sbccpro.com/OMMOM/OM9u8//	100%	Avira URL Cloud	phishing	
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://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://https://cdn.onenote.net/officeaddins/161351840456_Scripts/Instrumentation.js	0%	Avira URL Cloud	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	

Copyright null 2020

Source	Detection	Scanner	Label	Link
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://https://sbccpro.com/OMMOM/OM9u8/Outlook.phpZw	100%	Avira URL Cloud	phishing	
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://https://eagleeyeproduce-my.sharepoint.com/personal/mckrayp_eagleeyeproduce_com/_api/v2.0/drives/b	0%	Avira URL Cloud	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://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	
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://sbccpro.com/OMMOMk	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://https://sbccpro.com/OMMOM/OM9u8/Othermail.php0	100%	Avira URL Cloud	phishing	
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	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cdnjs.cloudflare.com	104.16.19.94	true	false		high
sbccpro.com	162.241.67.195	true	false		unknown

Copyright null 2020

Name	IP	Active	Malicious	Antivirus Detection	Reputation
eagleeyeproduce-my.sharepoint.com	unknown	unknown	false	• 0%, Virustotal, Browse	unknown
site-cdn.onenote.net	unknown	unknown	false	• 0%, Virustotal, Browse	unknown
onenoteonlinesync.onenote.com	unknown	unknown	false		high
code.jquery.com	unknown	unknown	false		high
maxcdn.bootstrapcdn.com	unknown	unknown	false		high
messaging.office.com	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	• 1%, Virustotal, Browse	unknown
ajax.aspnetcdn.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://sbccpro.com/OMMOM/OM9u8/Othermail.php	true	• SlashNext: Fake Login Page type: Phishing & Social usering	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://search.chol.com/favicon.ico	iexplore.exe, 00000001.00000002.471992806.00000268CD973000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.404496587.00000000F113000.00000002.00000001.sdmp	false		high
http://www.mercadolivre.com.br/	iexplore.exe, 00000001.00000002.471992806.00000268CD973000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.404496587.00000000F113000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.merlin.com.pl/favicon.ico	iexplore.exe, 00000001.00000002.471992806.00000268CD973000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.404496587.00000000F113000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.dailymail.co.uk/	iexplore.exe, 00000001.00000002.471992806.00000268CD973000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.404496587.00000000F113000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://eagleeyeproduce-my.sharepoint.com/personal/mckrayp_eagleep	iexplore.exe, 00000001.00000002.464762760.000000E589710000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000005.00000000.398408601.000000000B1A0000.00000002.00000001.sdmp	false		high
http://fr.search.yahoo.com/	iexplore.exe, 00000001.00000002.471992806.00000268CD973000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.404496587.00000000F113000.00000002.00000001.sdmp	false		high
http://in.search.yahoo.com/	iexplore.exe, 00000001.00000002.471992806.00000268CD973000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.404496587.00000000F113000.00000002.00000001.sdmp	false		high
http://https://sbccpro.com/OMMOM/OM9u8/Othermail.php9u8/	iexplore.exe, 00000001.00000002.491151422.00000268D0A5B000.00000004.00000001.sdmp	true	• Avira URL Cloud: phishing	unknown
http://https://github.com/twbs/bootstrap/graphs/contributors)	bootstrap.min[2].js.10.dr	false		high
http://img.shopzilla.com/shopzilla/shopzilla.ico	iexplore.exe, 00000001.00000002.471992806.00000268CD973000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.404496587.00000000F113000.00000002.00000001.sdmp	false		high
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000005.00000000.398408601.000000000B1A0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://msk.afisha.ru/	iexplore.exe, 00000001.00000002.471992806.00000268CD973000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.404496587.00000000F113000.00000002.00000001.sdmp	false		high
http://https://eagleeyeproduce-my.sharepoint.com/favicon.ico	iexplore.exe, 00000001.00000002.478788032.00000268CE38C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.reddit.com/	msapplication.xml4.1.dr	false		high
http://busca.igbusca.com.br//app/static/images/favicon.ico	iexplore.exe, 00000001.00000002.471992806.00000268CD973000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.404496587.00000000F113000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://sbccpro.com/OMMOM/OM9u8//	iexplore.exe, 00000001.00000002.490451697.00000268D099D000.00000004.00000001.sdmp	true	• Avira URL Cloud: phishing	unknown
http://www.autoitscript.com/autoit3/J	explorer.exe, 00000005.00000000.377823897.000000000095C000.00000004.00000020.sdmp	false		high
http://www.ya.com/favicon.ico	iexplore.exe, 00000001.00000002.471992806.00000268CD973000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.404496587.00000000F113000.00000002.00000001.sdmp	false		high
http://www.etmall.com.tw/favicon.ico	iexplore.exe, 00000001.00000002.471992806.00000268CD973000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.404496587.00000000F113000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://it.search.dada.net/favicon.ico	iexplore.exe, 00000001.00000002.471992806.00000268CD973000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.404496587.00000000F113000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.hanafos.com/favicon.ico	iexplore.exe, 00000001.00000002.471992806.00000268CD973000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.404496587.00000000F113000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cgi.search.biglobe.ne.jp/favicon.ico	iexplore.exe, 00000001.00000002.471992806.00000268CD973000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.404496587.00000000F113000.00000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
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://https://cdn.onenote.net/officeaddins/161351840456_Scripts/Instrumentation.js	learningtools[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://search.msn.co.jp/results.aspx?q=	explorer.exe, 00000005.00000000.404496587.000000000F113000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://buscar.ozu.es/	iexplore.exe, 00000001.00000002.471992806.00000268CD973000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.404496587.00000000F113000.00000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.microsofttranslator.com/BVPrev.aspx?ref=IE8Activity	iexplore.exe, 00000001.00000002.471992806.00000268CD973000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.404496587.00000000F113000.00000002.00000001.sdmp	false		high
http://www.ask.com/	iexplore.exe, 00000001.00000002.471992806.00000268CD973000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.404496587.00000000F113000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.google.it/	iexplore.exe, 00000001.00000002.471992806.00000268CD973000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.404496587.00000000F113000.00000002.00000001.sdmp	false		high
http://search.auction.co.kr/	iexplore.exe, 00000001.00000002.471992806.00000268CD973000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.404496587.00000000F113000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.amazon.de/	iexplore.exe, 00000001.00000002.471992806.00000268CD973000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.404496587.00000000F113000.00000002.00000001.sdmp	false		high
http://sads.myspace.com/	iexplore.exe, 00000001.00000002.471992806.00000268CD973000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.404496587.00000000F113000.00000002.00000001.sdmp	false		high
http://https://sbccpro.com/OMMOM/OM9u8/Outlook.phpZw	iexplore.exe, 00000001.00000002.490644346.00000268D09E5000.00000004.00000001.sdmp	true	• Avira URL Cloud: phishing	unknown
http://www.pchome.com.tw/favicon.ico	iexplore.exe, 00000001.00000002.471992806.00000268CD973000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.404496587.00000000F113000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://browse.guardian.co.uk/favicon.ico	iexplore.exe, 00000001.00000002.471992806.00000268CD973000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.404496587.00000000F113000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://google.pchome.com.tw/	iexplore.exe, 00000001.00000002.471992806.00000268CD973000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.404496587.00000000F113000.00000002.00000001.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, 00000001.00000002.471992806.00000268CD973000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.404496587.00000000F113000.00000002.00000001.sdmp	false		high
http://www.rambler.ru/favicon.ico	iexplore.exe, 00000001.00000002.471992806.00000268CD973000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.404496587.00000000F113000.00000002.00000001.sdmp	false		high
http://https://eagleeyeproduce-my.sharepoint.com/personal/mckrayp_eagleeyeproduce_com/_api/v2.0/drives/b	{CC75018C-2B89-11EB-90E5-ECF4BB2D2496}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://uk.search.yahoo.com/	iexplore.exe, 00000001.00000002.471992806.00000268CD973000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.404496587.00000000F113000.00000002.00000001.sdmp	false		high
http://www.ozu.es/favicon.ico	iexplore.exe, 00000001.00000002.471992806.00000268CD973000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.404496587.00000000F113000.00000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.sify.com/	iexplore.exe, 00000001.00000002.471992806.00000268CD973000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.404496587.00000000F113000.00000002.00000001.sdmp	false		high

Copyright null 2020

Name	Source	Malicious	Antivirus Detection	Reputation
http://openimage.interpark.com/interpark.ico	iexplore.exe, 00000001.00000002.471992806.00000268CD973000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.404496587.00000000F113000.00000002.00000001.sdmp	false		high
http://search.yahoo.co.jp/favicon.ico	iexplore.exe, 00000001.00000002.471992806.00000268CD973000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.404496587.00000000F113000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.gmarket.co.kr/	iexplore.exe, 00000001.00000002.471992806.00000268CD973000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.404496587.00000000F113000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000005.00000000.398408601.000000000B1A0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.nifty.com/	iexplore.exe, 00000001.00000002.471992806.00000268CD973000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.404496587.00000000F113000.00000002.00000001.sdmp	false		high
http://https://signup.live.com	Outlook[1].htm.10.dr	false		high
http://www.google.si/	iexplore.exe, 00000001.00000002.471992806.00000268CD973000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.404496587.00000000F113000.00000002.00000001.sdmp	false		high
http://www.soso.com/	iexplore.exe, 00000001.00000002.471992806.00000268CD973000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.404496587.00000000F113000.00000002.00000001.sdmp	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, 00000001.00000002.471992806.00000268CD973000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.404496587.00000000F113000.00000002.00000001.sdmp	false		high
http://cnweb.search.live.com/results.aspx?q=	iexplore.exe, 00000001.00000002.471992806.00000268CD973000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.404496587.00000000F113000.00000002.00000001.sdmp	false		high
http://www.twitter.com/	iexplore.exe, 00000001.00000002.478917872.00000268CE412000.00000004.00000001.sdmp	false		high
http://auto.search.msn.com/response.asp?MT=	iexplore.exe, 00000001.00000002.471339843.00000268CD880000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.404340191.00000000F020000.00000002.00000001.sdmp	false		high
http://www.target.com/	iexplore.exe, 00000001.00000002.471992806.00000268CD973000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.404496587.00000000F113000.00000002.00000001.sdmp	false		high
http://https://sbccpro.com/OMMOM/OM9u8/Office365.php	{E8888BAF-2B89-11EB-90E5-ECF4BB2D2496}.dat.1.dr, ~DF27CDF755FF987FC6.TMP.1.dr	true	• 100%, UrlScan, Browse • SlashNext: Fake Login Page type: Phishing & Social usering	unknown
http://search.orange.co.uk/favicon.ico	iexplore.exe, 00000001.00000002.471992806.00000268CD973000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.404496587.00000000F113000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

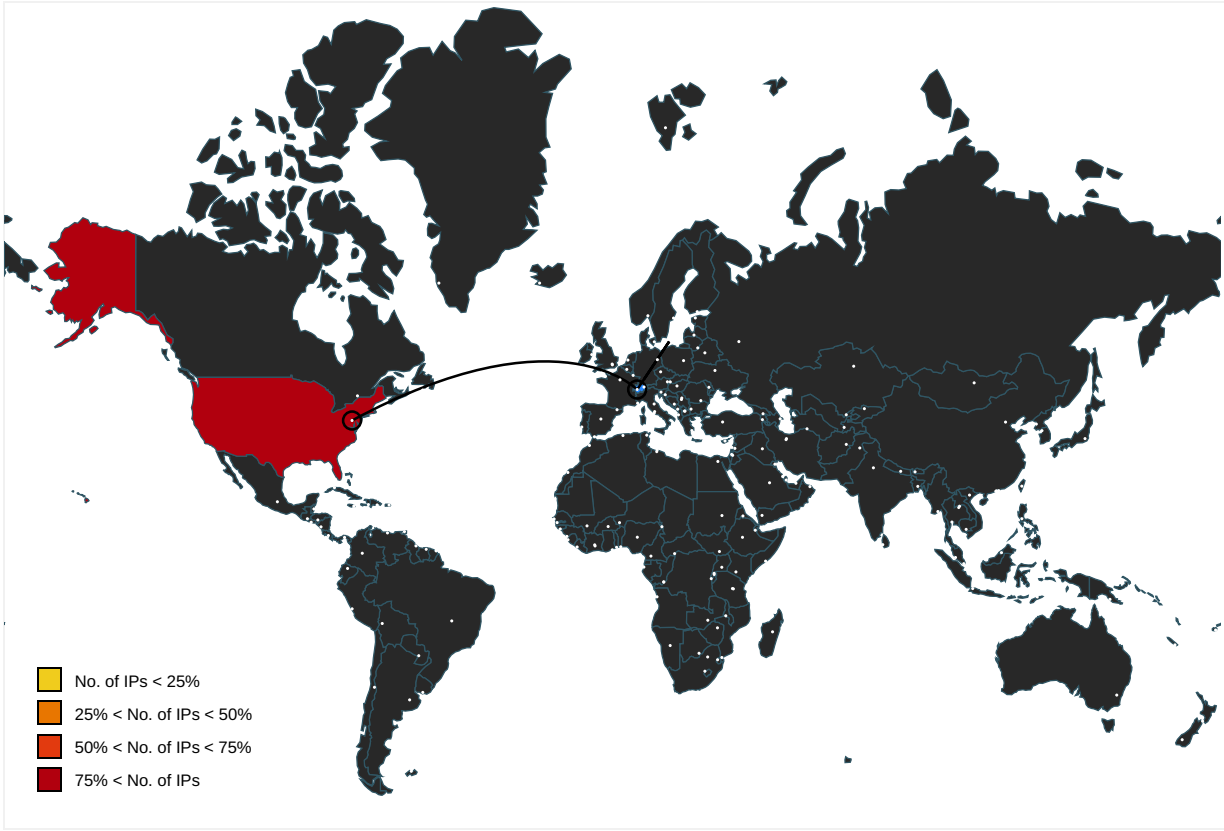
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.iask.com/	iexplore.exe, 00000001.00000002.471992806.00000268CD973000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.404496587.00000000F113000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://sbccpro.com/OMMOMk	{E8888BAF-2B89-11EB-90E5-ECF4BB2D2496}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://search.centrum.cz/favicon.ico	iexplore.exe, 00000001.00000002.471992806.00000268CD973000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.404496587.00000000F113000.00000002.00000001.sdmp	false		high
http://service2.bfast.com/	iexplore.exe, 00000001.00000002.471992806.00000268CD973000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.404496587.00000000F113000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ariadna.elmundo.es/	iexplore.exe, 00000001.00000002.471992806.00000268CD973000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.404496587.00000000F113000.00000002.00000001.sdmp	false		high
http://www.news.com.au/favicon.ico	iexplore.exe, 00000001.00000002.471992806.00000268CD973000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.404496587.00000000F113000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.cdiscount.com/	iexplore.exe, 00000001.00000002.471992806.00000268CD973000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.404496587.00000000F113000.00000002.00000001.sdmp	false		high
http://www.tiscali.it/favicon.ico	iexplore.exe, 00000001.00000002.471992806.00000268CD973000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.404496587.00000000F113000.00000002.00000001.sdmp	false		high
http://it.search.yahoo.com/	iexplore.exe, 00000001.00000002.471992806.00000268CD973000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.404496587.00000000F113000.00000002.00000001.sdmp	false		high
http://www.ceneo.pl/favicon.ico	iexplore.exe, 00000001.00000002.471992806.00000268CD973000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.404496587.00000000F113000.00000002.00000001.sdmp	false		high
http://www.servicios.clarin.com/	iexplore.exe, 00000001.00000002.471992806.00000268CD973000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.404496587.00000000F113000.00000002.00000001.sdmp	false		high
http://search.daum.net/favicon.ico	iexplore.exe, 00000001.00000002.471992806.00000268CD973000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.404496587.00000000F113000.00000002.00000001.sdmp	false		high
http://www.kkbox.com.tw/	iexplore.exe, 00000001.00000002.471992806.00000268CD973000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.404496587.00000000F113000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.goo.ne.jp/favicon.ico	iexplore.exe, 00000001.00000002.471992806.00000268CD973000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.404496587.00000000F113000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.msn.com/results.aspx?q=	explorer.exe, 00000005.00000000.404496587.000000000F113000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://sbccpro.com/OMMOM/OM9u8/Othermail.php0	iexplore.exe, 00000001.00000002.491151422.00000268D0A5B000.00000004.00000001.sdmp	true	• Avira URL Cloud: phishing	unknown
http://list.taobao.com/	iexplore.exe, 00000001.00000002.471992806.00000268CD973000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.404496587.00000000F113000.00000002.00000001.sdmp	false		high
http://www.nytimes.com/	iexplore.exe, 00000001.00000002.478917872.00000268CE412000.00000004.00000001.sdmp	false		high
http://www.taobao.com/favicon.ico	iexplore.exe, 00000001.00000002.471992806.00000268CD973000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.404496587.00000000F113000.00000002.00000001.sdmp	false		high
http://www.etmall.com.tw/	iexplore.exe, 00000001.00000002.471992806.00000268CD973000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.404496587.00000000F113000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ie.search.yahoo.com/os?command=	iexplore.exe, 00000001.00000002.471992806.00000268CD973000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.404496587.00000000F113000.00000002.00000001.sdmp	false		high
http://www.cnet.com/favicon.ico	iexplore.exe, 00000001.00000002.471992806.00000268CD973000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.404496587.00000000F113000.00000002.00000001.sdmp	false		high
http://www.linternaute.com/favicon.ico	iexplore.exe, 00000001.00000002.471992806.00000268CD973000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.404496587.00000000F113000.00000002.00000001.sdmp	false		high
http://www.amazon.co.uk/	iexplore.exe, 00000001.00000002.471992806.00000268CD973000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.404496587.00000000F113000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.cdiscount.com/favicon.ico	iexplore.exe, 00000001.00000002.471992806.00000268CD973000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.404496587.00000000F113000.00000002.00000001.sdmp	false		high
http://www.asharqalawsat.com/favicon.ico	iexplore.exe, 00000001.00000002.471992806.00000268CD973000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.404496587.00000000F113000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.google.fr/	iexplore.exe, 00000001.00000002.471992806.00000268CD973000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.404496587.00000000F113000.00000002.00000001.sdmp	false		high
http://search.gismeteo.ru/	iexplore.exe, 00000001.00000002.471992806.00000268CD973000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.404496587.00000000F113000.00000002.00000001.sdmp	false		high
http://www.rtl.de/	iexplore.exe, 00000001.00000002.471992806.00000268CD973000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.404496587.00000000F113000.00000002.00000001.sdmp	false		high

Copyright null 2020

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.soso.com/favicon.ico	iexplore.exe, 00000001.00000002.471992806.00000268CD973000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.404496587.00000000F113000.00000002.00000001.sdmp	false		high
http://www.univision.com/favicon.ico	iexplore.exe, 00000001.00000002.471992806.00000268CD973000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.404496587.00000000F113000.00000002.00000001.sdmp	false		high
http://search.ipop.co.kr/	iexplore.exe, 00000001.00000002.471992806.00000268CD973000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.404496587.00000000F113000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.auction.co.kr/auction.ico	iexplore.exe, 00000001.00000002.471992806.00000268CD973000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.404496587.00000000F113000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.orange.fr/	iexplore.exe, 00000001.00000002.471992806.00000268CD973000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.404496587.00000000F113000.00000002.00000001.sdmp	false		high
http://video.globo.com/favicon.ico	iexplore.exe, 00000001.00000002.471992806.00000268CD973000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.404496587.00000000F113000.00000002.00000001.sdmp	false		high
http://www.google.co.uk/	iexplore.exe, 00000001.00000002.471992806.00000268CD973000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.404496587.00000000F113000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	explorer.exe, 00000005.00000000.398408601.000000000B1A0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://cdnjs.cloudflare.com/ajax/libs/tether/1.4.0/js/tether.min.js	Outlook[1].htm.10.dr	false		high
http://buscador.terra.com/favicon.ico	iexplore.exe, 00000001.00000002.471992806.00000268CD973000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.404496587.00000000F113000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search1.taobao.com/	iexplore.exe, 00000001.00000002.471992806.00000268CD973000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.404496587.00000000F113000.00000002.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
162.241.67.195	unknown	United States		46606	UNIFIEDLAYER-AS-1US	false
104.16.19.94	unknown	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	321201
Start date:	20.11.2020
Start time:	15:39:52
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 23s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://eagleeyeproduce-my.sharepoint.com/:o:/p/mckrayp/EtopxtQDn3pOqhvY4g_gG3ABKX9ornSoGNhGOLlXyaU89Q?e=Ee0wW2
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:	16
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:	mal80.phis.win@6/136@13/2

Copyright null 2020

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://sbccpro .com/OMMOM/OM9u8 • Browsing link: https://sbccpro .com/OMMOM/OM9u8/Office365.php • Browsing link: https://sbccpro .com/OMMOM/OM9u8/Outlook.php • Browsing link: https://sbccpro .com/OMMOM/OM9u8/Othermail.php
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, dllhost.exe, BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • Excluded IPs from analysis (whitelisted): 40.88.32.150, 104.108.39.131, 13.107.136.9, 92.122.145.51, 92.122.213.216, 92.122.213.248, 52.108.56.22, 168.62.57.154, 52.109.88.143, 52.109.32.27, 52.109.124.71, 92.122.144.200, 2.21.58.96, 52.114.88.28, 52.109.76.2, 104.108.60.202, 152.199.19.160, 104.108.61.94, 51.104.139.180, 152.199.19.161, 51.103.5.186, 209.197.3.24, 216.58.208.42, 216.58.205.227, 209.197.3.15, 92.122.213.247, 92.122.213.194, 52.155.217.156 • Excluded domains from analysis (whitelisted): gstaticadssl.l.google.com, e2682.g.akamaiedge.net, cds.s5x3j6q5.hwcdn.net, arc.msn.com.nsatc.net, osiprod-sea-patriarch-000.cloudapp.net, c1-wildcard.cdn.office.net-c.edgekey.net.globalredir.akadns.net, browser.events.data.trafficmanager.net, appsforoffice.microsoft.com.edgekey.net, 20536-ipv4e.farm.prod.sharepointonline.com.akadns.net, fs-wildcard.microsoft.com.edgekey.net, wns.notify.windows.com.akadns.net, cdn.onenote.net.edgekey.net, e11290.dspg.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, prod-eu.reverseproxy-onenote.com.akadns.net, sea-000.omexmessaging.osi.office.net, prod.omexmessaging.live.com.akadns.net, officeclient.microsoft.com, watson.telemetry.microsoft.com, omexmessaging.osi.office.net, pnl1-arr.officeapps.live.com, prod-eur.onenoteonlinesync-onenote.com.akadns.net, fonts.googleapis.com, fs.microsoft.com, onenote.wac.trafficmanager.net.b-0016.b-msedge.net, displaycatalog.md.mp.microsoft.com.akadns.net, e19254.dscg.akamaiedge.net, site-cdn.onenote.net.edgekey.net, umwatsonrouting.trafficmanager.net, onenote.wac.trafficmanager.net, c1-officeapps-15.cdn.office.net, a1531.g2.akamai.net, e1553.dspg.akamaiedge.net, spoprod-a.akamaihd.net.edgesuite.net, browser.pipe.aria.microsoft.com, europe.configsvc1.live.com.akadns.net, spo-0004.spo-msedge.net, cs9.wpc.v0cdn.net, appsforoffice.microsoft.com, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, iecvlist.microsoft.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, c1-onenote-15.cdn.office.net, e5684.g.akamaiedge.net, par02p.wns.notify.windows.com.akadns.net, go.microsoft.com, mscomajax.vo.msecnd.net, skypedataprdcoleus12.cloudapp.net, skypedataprdcoluks04.cloudapp.net, emea1.notify.windows.com.akadns.net, 20536-ipv4.farm.prod.aa-rt.sharepoint.com.spo-0004.spo-msedge.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, onenote.officeapps.live.com, client.wns.windows.com, cs22.wpc.v0cdn.net, ie9comview.vo.msecnd.net, fonts.gstatic.com,

prod.configsvc1.live.com.akadns.net, c1-wildcard.cdn.office.net-c.edgekey.net, e1723.g.akamaiedge.net, prod-weu.onenoteonlinesync-onenote.com.akadns.net, prod.reverseproxy-onenote.com.akadns.net, browser.events.data.microsoft.com, config.officeapps.live.com, go.microsoft.com.edgekey.net, prod.onenoteonlinesync-onenote.com.akadns.net, cds.j3z9t3p6.hwcdn.net

- 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
15:41:04	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\6BAUBVPU\www.onenote[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	140
Entropy (8bit):	4.911057797251907
Encrypted:	false
SSDEEP:	3:D90aK1ryRtFwsOHQYMALfVAqUFTdwISTTuU3l2DDcTVvI9FCpRHFNRJAqSSVcT5b:JFK1rUFKlMufVAq6GvTLvcEFCphYSV+b
MD5:	F72A6041F656F941EE6A51A073962ADB
SHA1:	2883A3B3273FEFD84608F8C0716A1F81B1BE7B32
SHA-256:	5C2D90DD4BB042E669B216A8C77DFF5D3BD271F1AF771891E161F9372BF36503

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\6BAUBVPU\www.onenote[1].xml	
SHA-512:	1983BE4BBF3481C7F011454ECF5E53A9DCF95AAEAA959D3244033053D49BB0045A2D363616B9A5A745BC97C2305BCA1B741C8284EFD9A98CC2D7756D00989FE2
Malicious:	false
Reputation:	low
Preview:	<root></root><root><item name="Office API client" value="1206808e-5719-6275-619c-5a53af9b400a" ltime="2624272064" htime="30850966" /></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\EQAWN5DV\eagleeyeproduce-my.sharepoint[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	2.469670487371862
Encrypted:	false
SSDEEP:	3:D90aK1r0aKb:JFK1rFKb
MD5:	132294CA22370B52822C17DCB5BE3AF6
SHA1:	DD26B82638AD38AD471F7621A9EB79FED448A71C
SHA-256:	451ABBE0AEFC000F49967DABF8D42344D146429F03C8C8D4AE5E33FF9963CF77
SHA-512:	6D5808CAD199A785C82763C68F0AE1F4938C304B46B70529EA26B3D300EF9430AD496C688D95D01588576B3A577001D62245D98137FD5CD825AD62E17D36F15C
Malicious:	false
Reputation:	low
Preview:	<root></root><root></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\IB42RK38\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:	dropped
Size (bytes):	121191
Entropy (8bit):	5.082004542652738
Encrypted:	false
SSDEEP:	768:hQSOB58B5OAZ/OJQSOB58B5OAZ/OqQSOB58B5OAZ/OdQSOB58B5OAZ/OJQSOB58i:3
MD5:	501CD05598EE59A65F2B029A96FD3BF1
SHA1:	BE76041BC5473A0FDC612869F1D6613A570E95E4
SHA-256:	F4729A9E3DE3A03C2E2E142FB6B4041FF09158C342B926281B57E38FA7C8ACE5
SHA-512:	99C078ED189B69BEE1E93B830F2BF59BB953CE37BEF83958982EA452C3B4A7B516E6EC3BE7C7D5BCF18024EB68F24C42FE4F2523F185BF100E509A2F83E06CA0
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\Recovery\High\Active\RecoveryStore.{CC75018A-2B89-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	51400
Entropy (8bit):	2.060263383251775
Encrypted:	false
SSDEEP:	192:r2ZhZX2m9WAttfhhMSqrfscrpzVW3h+Ibg:rynGmUEFkSqrRpw3hn8
MD5:	450CB054C9A83185E1BA712D6F5AD3C1
SHA1:	C7A03CB0DF31D2770CB9C5C36F6AC90E1C94F5D5
SHA-256:	2DDA47E2CA09F5EAB43286F64198793E685EADA16E3A4C1CCDAFF1FD37CA5434
SHA-512:	109A587CD68ADACA09796A66AFAD6445150FC547371FDD81726D0ABB787B9FA008DC0EC2D7C00FD9EDD80922FFE2BDE5BAD6AD1F2C2BAC2C4793FE4B87FE025
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\{CC75018C-2B89-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	111762
Entropy (8bit):	4.086063750784828
Encrypted:	false
SSDEEP:	768:/ZzmRk0z0f38PuK3rKa0z0f38PuK3rH40z0f389uK3rl:/ZzmI38PLrH38PLrm389Lrl
MD5:	E32B432812AB243E924BF714D54E7750
SHA1:	1E7F0ED279B87EA101F36B70CF042B56A54E0A75
SHA-256:	3C340DA70AA90A37827FDC4778E78C26FFB222695C4CA503B08347596BDE1E73
SHA-512:	E3B7296B33EEA89304AA592914BBE80499A22ECB14E294ABE005D9E5F6E31E45BFD4F7BA36F83671FDFD357F2652C50708B792CC97623BB74A9F69F7F626A9A(
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\{D44132E7-2B89-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5647924814006202
Encrypted:	false
SSDEEP:	48:IwQGcpr4GwpaWG4pQqGrapbSTrGQpKZG7HpRwcsTGIpG:rUZgQm6cBSTFA4Twc4A
MD5:	D4ADAA9A198FA2FCC86850DFFCAB499E
SHA1:	607CCDF51FE631C5C47BC022262C342FBA302115
SHA-256:	2284E979D2923E1F32C7297A82860734A1B0429186656CD77C6F1F39B646225E
SHA-512:	ED27101A951D4C3EDF540EB8CCA44FDB9D72A869A788499C35342CF7E18B9605528B3C15ECF0D5BCC2708F4B50E4AC42674DE3B46FD52901FE6C4CDDD297FE9
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\{E8888BAF-2B89-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	59990
Entropy (8bit):	2.10023645223731
Encrypted:	false
SSDEEP:	384:rs0cIRhUI0St+mA0NgpE3ptPtzNv9br9AeAvDeMqE:VBRS
MD5:	0438F18C677625EC4FDA492F2F55FE19
SHA1:	B3C9584F1A4C334DF822BEBF050B7EEAC8890267
SHA-256:	85AAF0F5239AF442B35AA144C9C64BA2EDD5A563D9A0A901219ABBFC3A3F4F3C
SHA-512:	9777CFF3B9771425A7EFB36214804D78B4FDAC41D159A9E580B41513D7077355161188CFB74836FAD22406F47A35255BBF6F767F640E024622CF746B671C1798
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\{F1C56536-2B89-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5650526740763933
Encrypted:	false
SSDEEP:	48:IwpGcprEGwpa1G4pQ9GrapbSWrGQpKqoG7HpRlsTGIpG:rvZ8Qn6dBSWFA4Tl4A

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{F1C56536-2B89-11EB-90E5-ECF4BB2D2496}.dat	
MD5:	CFE741AEED8191C2DE685C8A0D1F306F
SHA1:	4F0DF58671E2C3114EAAB5449CA9FB60D2D8EBC1
SHA-256:	07D98234CC8072B8EFDA471135F55093DDB4EA252998B2171FDA6F0E62463D06
SHA-512:	56A91111D45920FDAF37FC7250A9815D7E407C098C0AFEC772380E8D196D2D50BD07BB6D06A96094A7D89FDBC624FA6F31486FDA675579AA2DAD926DFB4D4D8
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):	659
Entropy (8bit):	5.07506774092484
Encrypted:	false
SSDEEP:	12:TMHdNMNxOE4iLNnWimI002EtM3MHdNMNxOE4iLNnWimI00OVbVbkEtMb:2d6NxOfiLNSZHKd6NxOfiLNSZ7V6b
MD5:	936767C09FE5FAF6967ADD65A210CF19
SHA1:	261A6DE28B3990A25A6DDA9C7F93A1CDD6D25C47
SHA-256:	9EEF2A65B4DEC82A3A20E1F12F271D8BB66DE6150C3B17B2C920E0C4CC55CB97
SHA-512:	2AF15962CF077136034B3C166C063A8B218A4092B2C5E3B50C67CF5ED959D47CC247502F325D4C5CD2F477B476A5522828BD8594277AB23B4501E8194F2FB752
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0xa4a6ff30,0x01d6bf96</date><accdate>0xa4a6ff30,0x01d6bf96</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>0xa4a6ff30,0x01d6bf96</date><accdate>0xa4a6ff30,0x01d6bf96</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):	656
Entropy (8bit):	5.124383272733761
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2k18MNnWimI002EtM3MHdNMNxe2k18MNnWimI00OVbkak6EtMb:2d6Nxr48MNSZHKd6Nxr48MNSZ7VAa7b
MD5:	BC0CD58CBD55591457D52562D9A772F4
SHA1:	6034D62792EAFCFD36EEE28CBDD45994D2876F18
SHA-256:	4B7BE46CFB039ECA60B9C88378A7BF0EAA8E8EA8916A8A4D5D9D81FFD1BFDAD5
SHA-512:	CB59BF375B9D20F0137F63C4496D41833F556B624DD4A908F4633C90838A3B86A3D4C714E45AE2F3223462CB2BBF895CF0D927C7C2C439CE33D50557A8D1872
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0xa49d75da,0x01d6bf96</date><accdate>0xa49d75da,0x01d6bf96</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>0xa49d75da,0x01d6bf96</date><accdate>0xa49d75da,0x01d6bf96</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):	665
Entropy (8bit):	5.110415808270749
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLVT+BRT+BlNnWimI002EtM3MHdNMNxvLVT+BRT+BlNnWimI00OVbmZt:2d6NxvJ+p+lNSZHKd6NxvJ+p+lNSZ7VQ
MD5:	6F964854BE18399951772BBCA0AF16B4
SHA1:	94DE45F0C6D8E5F51D25C2FD4EEA1ACE06F3C0EA
SHA-256:	6B5CA65AA1CE5388DC5D6F34B87D585F5AFC8CFE25456D1ED49D588FF557485D
SHA-512:	DC204E7702D3FCDF7E15D10037A23E1F20BB79E6B9DC0744C4264290867A8DBB20B3C175CA48E15D79BA48D40FBEC7F2BE134ECA20546EB2DD43A1E574828C40
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0xa4a9617d,0x01d6bf96</date><accdate>0xa4a9617d,0x01d6bf96</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>0xa4a9617d,0x01d6bf96</date><accdate>0xa4a9617d,0x01d6bf96</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):	650
Entropy (8bit):	5.094289175220909
Encrypted:	false
SSDEEP:	12:TMHdNMNxi8hMNnWimI002EtM3MHdNMNxi8hMNnWimI00OVbd5EtMb:2d6NxnhMNSZHKd6NxnhMNSZ7VJjb
MD5:	2C7F4C967EC263342EBC3952FA6923F9
SHA1:	2F373ACF3A0D3FF7229F213E27273323C7DB7EAB
SHA-256:	0FA4555CF6A2F814E3F39766DFF43255271B28D2728775AAC887AC34CD106E7F
SHA-512:	C6C61B3E1C3F97311CB1C58F80FF20336D95FD1D07FC15E2CDE5AED55E2825F9995140B053F055A4E22CE9317E8714F31FD3FF45E44CB475386116935CF46E8
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0xa4a49cd0,0x01d6bf96</date><accdate>0xa4a49cd0,0x01d6bf96</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>0xa4a49cd0,0x01d6bf96</date><accdate>0xa4a49cd0,0x01d6bf96</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):	659
Entropy (8bit):	5.124364258065086
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwVT+BRT+BlNnWimI002EtM3MHdNMNxhGwVT+BRT+BlNnWimI00OVbi:2d6NxQW+p+lNSZHKd6NxQW+p+lNSZ7VG
MD5:	406CF2007B61BFD4104274870E7EFDBA
SHA1:	7382F79322CED3D0C421CA1806889CE6B329E273
SHA-256:	2B7477C70321461A5FF60BCC1484C7244501505134C85A4149B91B6A73536B2A
SHA-512:	46CEBAEFA1921AB146DA7011EB7788650B33377CE678D38ADE886395AC551618EB347D04FCFEE04D7D95E12140597C20D5A452BD17824570FD4635F209D30B3
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0xa4a9617d,0x01d6bf96</date><accdate>0xa4a9617d,0x01d6bf96</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>0xa4a9617d,0x01d6bf96</date><accdate>0xa4a9617d,0x01d6bf96</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):	656
Entropy (8bit):	5.078787994565476
Encrypted:	false
SSDEEP:	12:TMHdNMNx0n4iLNnWimI002EtM3MHdNMNx0n4iLNnWimI00OVbxEtMb:2d6Nx04iLNSZHKd6Nx04iLNSZ7Vnb
MD5:	950484E37E821D83C319873670FF6445
SHA1:	09945CB9EEE058938A830EB9160FAAFDA11003F9
SHA-256:	F8C7AE988889907FFCA0B3306BB1D5AFE1CFC7275644B40F2C53FA799D767C2F
SHA-512:	078F9C3EC561A78A903DA6C98B7A23926A66C71BBD0FF0EA4873CEA9273F79575720E1104A5800D9615B3288E4DE687E1851CE2E54DEEA573E261BE1A45A9FA
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0xa4a6ff30,0x01d6bf96</date><accdate>0xa4a6ff30,0x01d6bf96</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>0xa4a6ff30,0x01d6bf96</date><accdate>0xa4a6ff30,0x01d6bf96</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):	659
Entropy (8bit):	5.11486884288704
Encrypted:	false
SSDEEP:	12:TMHdNMNxx4iLNnWimI002EtM3MHdNMNxx4iLNnWimI00OVb6Kq5EtMb:2d6NxWiLNSZHKd6NxWiLNSZ7Vob
MD5:	76404F1BA9B40D0B591B4375D5F92012
SHA1:	4723F452B480FED8C900471D67C779B971D27D09
SHA-256:	DC1784F8C5B7D38642E40B46066D746CB76F27B29C586978D725BCB7BD257DF0
SHA-512:	B133A9822D1DC8134CD3E1A27F72BFE9EA02C205DBEBCFEDF1AAA8AEDD77BB8EC5BE1EF82914737F33C6CDFA6E3F4CA4171D2939B43F34499D4207D5B3236 236
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0xa4a6ff30,0x01d6bf96</date> accdate>0xa4a6ff30,0x01d6bf96</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>0xa4a6ff30,0x01d6bf96</date><accdate>0 xa4a6ff30,0x01d6bf96</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):	662
Entropy (8bit):	5.115956998133289
Encrypted:	false
SSDEEP:	12:TMHdNMNxcpNnWimI002EtM3MHdNMNxcpNnWimI00OVbVEtMb:2d6NxMNSZHKd6NxMNSZ7VDb
MD5:	7BA7580FB8D8B580A0CA24E4E2380FEF
SHA1:	10CD42A669C10E3F81B0921CAEB2348E9C6169E3
SHA-256:	9E507E21334CC930A5A7A2AD7CD8AD254D7067E00635981FF75FB8D33B20505A
SHA-512:	7564A2750B07FA57C77187BF5297BCD55893B1CEC44CBDC365FF246D19BABC3DA814047EBD4854F1055415262FA9C6FC243980ADAF75C0613DFFFBEDD29E4A 0
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0xa4a23a91,0x01d6bf96</date> <accdate>0xa4a23a91,0x01d6bf96</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>0xa4a23a91,0x01d6bf96</date><accdate >0xa4a23a91,0x01d6bf96</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):	656
Entropy (8bit):	5.079857128135405
Encrypted:	false
SSDEEP:	12:TMHdNMNxfn8hMNnWimI002EtM3MHdNMNxfn8hMNnWimI00OVbe5EtMb:2d6NxEhMNSZHKd6NxEhMNSZ7Vijb
MD5:	B64A45B8A998A24F6DE114B61171DC6C
SHA1:	647ABE97085EBBD3595F03D90750F8EA90A1B228
SHA-256:	28BBD51EDB47CE5F160DB2E62182A499C8F9BFCAF6F7E3DA79212C84A5764CBD
SHA-512:	D08274ED67EA958E5CFB3ECDE6105A6A2D67DE02ED02F062E8F0969CD585DFCD560280C8F37F5CB5FD74A10B4788FAB3E676AD3B16916C002F15093E4342EA 3
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0xa4a49cd0,0x01d6bf96</date><a ccdate>0xa4a49cd0,0x01d6bf96</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>0xa4a49cd0,0x01d6bf96</date><accdate>0xa 4a49cd0,0x01d6bf96</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\wlm7n14\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\wlm7n14\imagestore.dat	
Size (bytes):	8450
Entropy (8bit):	3.8243436370124493
Encrypted:	false
SSDEEP:	96:NfXOmS/+CtmE8mmmmm08mmmmmtf8mmmmmO8mmmmm+8mmmmmo8mmmmmo8mmmmmSQP:NfwQfMfmHFP
MD5:	EF977945EE80F6B5E813491E15D44002
SHA1:	A7883C26CF9BCB0C502F85F18CB1281102DB1016
SHA-256:	5E814112599472F2A600F1DE625E1BA3F2A346D7CE125AFE7E4A35C2A9DF8C8C
SHA-512:	1EFD77398F3DA2F82A64087BF51ECE4975525B2E993F93578195D6B4C686C80CF5B6148AE7314175CC43CC252821879E28F5D1DBDF0869D9F31AEA3185264033
Malicious:	false
Reputation:	low
Preview:	I.h.t.t.p.s.:.//.c.1.-.o.n.e.n.o.t.e.-.1.5...c.d.n...o.f.f.i.c.e...n.e.t./.o./.r.e.s.o.u.r.c.e.s./.1.0.3.3./.F.a.v.I.c.o.n._.O.n.e.N.o.t.e...i.c.o..... ....(... ...@..... ....d...d...d...d...d...d...d...d...d...d...d...d...d...d...d...d...w...w...w...w...w...w.....d...d...d...d...d...d...d...d...d...d...d...d...d...d...d...d...w...w...w...w...w...w...w...w...w...w.....d...d...d...d...d...d...d...d...d...d...d...d...d...d...d...d...w...w...w...w...w...w...w.....P...P...P...P...P...P...P...P...T...d...d...d...d...d...d...d...w...w...w...w...w...w.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\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/1613510410007_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\3Y2ADQKS\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):	90754
Entropy (8bit):	5.144463422002279
Encrypted:	false
SSDEEP:	1536:NKMLN5vGL78J0JsCxtzXnCG+Uhk0Bvj0Bac3d:FWJ2G+8Bvo
MD5:	00DCA553EEDCAAD1F089A47AE988F72E
SHA1:	6223314FF4D289DA09CB40383B8DCBDFF8A6FA67
SHA-256:	82E985F6850F8FCE54E9A2B645A79D42117FE421E48A1986EC24B0ECED40F13D
SHA-512:	D315AF0FB4B67D2A71DC8CEBD0975BDAD1D5205D6CEF3B0D4AA101C1C1BF3125AF53DCC588E4774239D8E94376A149D09FBC2E3576606E1F64E99D609B0DC10
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c1-officeapps-15.cdn.office.net/o/s/1613510410007_App_Scripts/1033/CommonIntl.js
Preview:	CommonStrings={afrikaans:"Afrikaans",albanian:"Albanian",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:"Belarusian",bosnian_Cyrillic:"Bosnian (Cyrillic)",bosnian_Latin:"Bosnian (Latin)",breton:"Breton",bulgarian:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\Meetings_manifest[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\Meetings_manifest[1].xml	
Category:	downloaded
Size (bytes):	89749
Entropy (8bit):	5.907896932868388
Encrypted:	false
SSDEEP:	1536:TF7qkDiiBSPqAYXUJqc9a/qc9aJyXUEUx:J7j7B4S6RaVC
MD5:	1BF11FC2DBDB5C48B7D60F5005583417
SHA1:	DF52B131F6B151E674204CBA77082EFAEFBC3F8C
SHA-256:	172E218E70CC419328B7AAB580615DA2A562E1508EAC9AC3014C52C51F2F50EC
SHA-512:	A40545B0B88AAF5EC4D28015B72451CE6F19073FC7E1CF6A8B08EEAB6D173CCE9E62553CACFDA7FE0FB4DDECB2E09E8B966C6466AE50AC31193481D82898ECB6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c1-onenote-15.cdn.office.net/o/s/161351041007_resources/1033/Meetings_manifest.xml
Preview:	.<?xml version="1.0" encoding="UTF-8"?>..<OfficeApp xmlns="http://schemas.microsoft.com/office/appforoffice/1.1" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:bt="http://schemas.microsoft.com/office/officeappbasictypes/1.0" xmlns:ov="http://schemas.microsoft.com/office/taskpaneappversionoverrides" xsi:type="TaskPaneApp">...<Id>90da59be-5361-4260-9218-2262af1dc334</Id>...<Version>1.0.0.0</Version>...<ProviderName>Microsoft Corporation</ProviderName>...<DefaultLocale>en-US</DefaultLocale>...<DisplayName DefaultValue="Add Meeting Details">.... START STRING LOCALIZATION REPLACEMENT (StringID: OfficeAddIns.Meetings.ManifestDisplayName -->.....<Override Locale="af-ZA" Value="Voeg vergaderingbesonderhede by" />....<Override Locale="en-US" Value="Add Meeting Details" />....<Override Locale="am-ET" Value="..... ...." />....<Override Locale="ar-SA" Value="..... ...." />....<Override Locale="as-IN" Value="..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\OM9u8[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	240
Entropy (8bit):	5.141428244866365
Encrypted:	false
SSDEEP:	6:pn0+Dy9xwol6hEr6VX16hu9nPVrHbU+KqD:J0+ox0RJWWPxfT
MD5:	98A9E4BD022349D51C13290BF7D861BB
SHA1:	71834E1DB25A55B6F1A2315FDE93E6DAA1970F45
SHA-256:	38E4FA490BD7C4492C664C15F3501B5B363375280BF9320D818E7C22D678B01F
SHA-512:	391823CFFFADA621E6BD8D4845F1A02E588F18A15D4ED595F0DF3015C12C849B0F3B99913416B871A0F5AC735F4B149964CB2488758B6300B2BC573756FB6021
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_Obshtml, Description: Yara detected obfuscated html page, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\OM9u8[1].htm, Author: Joe Security • Rule: JoeSecurity_Encryptedhtml, Description: Yara detected Encrypted html page by third party sevices, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\OM9u8[1].htm, Author: Joe Security
Reputation:	low
Preview:	<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">.<html><head>.<title>301 Moved Permanently</title>.</head><body>. Moved Permanently . The document has moved here. .</body></html>.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\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/161351041007_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 = "PATCH";.. Constants.httpMethodDelete = "DELETE";..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\OneNote.Refresh[1].css	
Category:	downloaded
Size (bytes):	417934
Entropy (8bit):	5.309711696088552
Encrypted:	false
SSDEEP:	6144:Wa+MX8gWd5eL5Ac4nb+9xVpO0KSZ+9j8S37v5sr:j+MX8guc4nb+9xVpO0KSZ+9j8S37v5sr
MD5:	879B88B9CF22E9CA83075614914399D4
SHA1:	C600172AF089F3B13C9C76AFDED10DB1BFFC51F9
SHA-256:	6AE2EB85AD0995D38385F81A1E94705A7E29C0ECF43F573E38C25142E4B35715
SHA-512:	77F20389FD7C91D704A7AC3E9CDCF8FCDA1C93F8B43F5F02B7BDC937FA5650DA2EA5CC7E8367D9F6E74ED726D5C836F9CFE2E596188E65E652136C70714C93F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c1-onenote-15.cdn.office.net/o/s/161351041007_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-height: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;display: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\3Y2ADQKS\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):	31243
Entropy (8bit):	4.890289295492406
Encrypted:	false
SSDEEP:	384:+gNpdtptTNzZ6TJcB/pw+UkNqJ3ncwKVXYMCwDp5molHuE7:+2dtptTNzrpmkNqJ3c1xYhwd5n97
MD5:	2775482A053DE666DC7D18DB85DBA950
SHA1:	EE5671D6E9F22A17224CDD64E74BEF8126EBC506
SHA-256:	69B7ED5D9D02C622B0AF88236436AD5AEDA8C4C8E5030D8A930BB71F9D5A7E72
SHA-512:	A5D1361D6181950DCB731724CFF7F387867AFAC20AE9DEE36DCF4BA9C68D2A33F401227382C3C3B74A3CBFD3C6A0719980537B59EE37C2F5467E00A75D5FB1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c1-onenote-15.cdn.office.net/o/s/161351041007_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\3Y2ADQKS\OneNote[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	2851479
Entropy (8bit):	5.613495796938069
Encrypted:	false
SSDEEP:	49152:DD58WiWeUVaFQFb3S/xvAOePAlt0cUxdAUTM7l/2wuJP7GEHCr4YyJ5n+J:eDs3K
MD5:	EE1718E26116238D56642A9DFD37393E
SHA1:	F9C292E97F1BFDA1E54171E49B60BEBB379BF6EB
SHA-256:	62956F12C24DD07339A5A130A5DCB23F867C33A1D3A220FF77BE6DA7FE81F863
SHA-512:	7CD41CBE6F40F5559FCF9A4BDFB6804F98418BECFC5947F8C9590B70DAD6B1567278D1622B444236E2216E2C6DDAA820CEA1E17B574BC89A563F546634ECBAD
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c1-onenote-15.cdn.office.net/o/s/161351041007_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(){},IEnumerable.registerInterface("IEnumerable"));"undefined"==typeof IEnumerator&&(IEnumerator=function(){},IEnumerator.registerInterface("IEnumerator"));"undefined"==typeof Sys&&Type.registerNamespace("Sys");"undefined"==typeof Sys.gs&&(Sys.gs=function(){},Sys.gs.registerInterface("Sys.IEnumerable$1"));."undefined"==typeof Sys.ox&&(Sys.ox=function(){},Sys.ox.registerInterface("Sys.IEnumerator$1"));Type.registerNamespace("Diag");var wac_aa=window.Diag||{};function wac_baa(){}wac_baa.registerInterface("Diag.IUlsHost");wac_aa.Zcb=function(){};wac_aa.Zcb.prototype={};wac_aa.Zcb.registerEnum("Diag.ULSTraceLevel",!1);function wac_ba(a,b,c,d,e,f,g,h){this.Mcb=a;this.LIa=b;this.ZA=c;this.xo=d;this.sr=e||"";this.WLa=f;this.X8a=g;this.Pp=h}wac_ba.prototype={Mcb:0,LIa:0,ZA:0,xo:0,sr:null,WLa:0,X8a:!1,Pp:null};.function wac_ca(a){wac_ca.initializeBase

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\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):	540122
Entropy (8bit):	5.342092583024336
Encrypted:	false
SSDEEP:	6144:FUdprM5afIb7dMyaTpEIDm9STsGVay0xKOzwje2X2xdKoC9l5eNgiKqQWYsg3orL:ktEIDlSgOzwI
MD5:	817A4ADC1C127AEC2C51155D1D9DDFB7
SHA1:	F13AA5210EE76E22CD2D74E0CE59FF080678D440
SHA-256:	1100DD3F7C471F0550038B22915CEF0E5546AE8D74B6CF220E44A42C1F94CCAD
SHA-512:	BCF883AA8A73D39A3B28F1A65473BC4580939783BF4618902049047553263AEF56642A176B5977E5DC82BCA12B7B18B1F4C232540C5310400F0C0CCD924CD744
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c1-onenote-15.cdn.office.net/o/s/161351041007_App_Scripts/OsfRuntimeOneNoteWAC.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\3Y2ADQKS\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/161351041007_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\3Y2ADQKS\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/161351041007_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\3Y2ADQKS\jquery-3.1.1.slim.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	69309
Entropy (8bit):	5.3700159283175415
Encrypted:	false
SSDEEP:	1536:dNhEyjjTikEJO4edXXe9J578go6MWXqcVhzLyB4Lw13sh2bTQKmPNsvDU8Cur:Dxcq0hzLZwpsYbIyvDU8Cur
MD5:	550DDFE84A114F79A767C087DF97F3BC
SHA1:	310BD0C04196573315C2E8446776685AC2961724
SHA-256:	FD222B36ABFC87A406283B8DA0B180E22ADEB7E9327AC0A41C6CD5514574B217
SHA-512:	B6A9146FFE380A32C89D48BAF900DD5E346B0D603B8AFCFAD070970E56BDC744E8A8B053C2EF8A3107F4A3C2BDD11EE470E05557F542FFEDE5FF54468EE186C4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://code.jquery.com/jquery-3.1.1.slim.min.js
Preview:	/*! jQuery v3.1.1 -ajax,-ajax/jsonp,-ajax/load,-ajax/parseXML,-ajax/script,-ajax/var/location,-ajax/var/nonce,-ajax/var/rquery,-ajax/xhr,-manipulation/_evalUrl,-event/ajax,-effects,-effects/animatedSelector,-effects/Tween,-deprecated	(c) jQuery Foundation	jquery.org/license */.!function(a,b){"use strict";"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a document");return b(a)}:b(a)}("undefined"!=typeof window?window:this,function(a,b){"use strict";var c=[],d=a.document,e=Object.getPrototypeOf,f=c.slice,g=c.concat,h=c.push,i=c.indexOf,j={},k=j.toString,l=j.hasOwnProperty,m=l.toString,n=m.call(Object),o={};function p(a,b){b=b||d;var c=b.createElement("script");c.text=a,b.head.appendChild(c).parentNode.removeChild(c)}var q="3.1.1 -ajax,-ajax/jsonp,-ajax/load,-ajax/parseXML,-ajax/script,-ajax/var/location,-ajax/var/nonce,-ajax/var/rquery,-ajax/xhr,-manipulation/_evalUrl,

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\landing-devices-bg[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 1200x800, frames 3
Category:	downloaded
Size (bytes):	160872
Entropy (8bit):	7.983227926427131
Encrypted:	false
SSDEEP:	3072:2uSUXBjNQkwlonMsi5EixPv7LxYLHV0zXIHTQaihnyga+:2dUXN4lqLixPv7t2QXCQaid9
MD5:	55174EA1C3DF4966ED13D25A6223999D
SHA1:	FA1E418627CE2C16FF594A9615B1D53E5F676FFF
SHA-256:	C86C4A6731077F1994A8CAECCB1FC06477EA35A5B6ABBB4ABDE1D06B8EF9FF32
SHA-512:	BD5FB38C3BBCCD3F9C7E9E21DE86CD5C1846CF54406FB999649D76CD92D98214585BF00554FE44AE63B97EC9E30252D36CEDD39459A365ECF54E110911D8CBAD
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://sbccpro.com/OMMOM/OM9u8/images/landing-devices-bg.jpg
Preview:	......JFIF.....C.....!*$..(..%2%(,-/0/.#484.7*./....C..... ....=... @..... ....'.W].8 @..... .....hS....A J.....s.....2j.l.!m..C..M& ...8..0.8... p`@..!....;.....5..$0..!0.a"g#.UN.3.NT.D.L.D.sz.OO.y..D..b(.g!.|...o.9.8.WK..\....LK..@i.Y...N.M ..56.mR./`.@...A..A.....(9...;,@.....RET.n".....F....BT.8.Wf$_?...oAVd...M...`!...H.46...4...80 d8& d pL`HA..U...p.'?..$C.. .....C.i...D.....G/.S..../..M.D.is..3.5..0..5b...y.C.t.Z...." .n5....m\..sb...B.....*.75.-.Q.....PEA..D.....e....@.r ..l.O..LLv..\.Y.U..F.....4...l..6.6.....&$ @.....=w....>../...j...17c;..^..|..l...(.....4..L6N...+:r.yW..Y..u\.N\.O2T....8^;.~ ..g..f.x.x...}.=.....qj..V)[`.l.....@.....V.L.....l...@(....R... N9.@.!Y.q|..d.)..y.q....)...h..l..&.a.0.h... @.....@...!...../

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\mail[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 100 x 87, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	1106
Entropy (8bit):	7.176105528957688
Encrypted:	false
SSDEEP:	24:rTtaBegujKwSx2UKzpZtPcCdBR1uj7cxRqnwFT2C4z2MlNvM2NOYVrng:rTtWSwxKzpZvoExQwFJfKiyOYVLg
MD5:	D9F81CF593394338BD133AA77B0ECBAF
SHA1:	24AB26A812E74CBB08BB17E495F8852A3DF5A038
SHA-256:	2EBC65A696544B8D69ADE5F136250A9548D4BADF1B9AD459E63FF68E7A985C69
SHA-512:	28370A1CE7F1F3CA386187DF2FBADAE154E151DE5794913FD0DAE42B26545BE39E9A6E2C855F4EB3D267210768FF7AE7D15268C3BEDA53D88FE9AA878ECF065
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://sbccpro.com/OMMOM/OM9u8/images/mail.png
Preview:	.PNG.....IHDR...d...W.....e....PLTE.....wy....4tRNS.9.....j...0!.....A.I<4.\.bN,'...|nfXFu.V.R6xs.....IDATh...r.@.E.k3c..(j...D3....[..P....b..K.L.....2..b...;@1./...C9.....s..w..d..P.9.....e..''..E3..A:;P.sf2..../..b.,..Z/Sd$..[..>@c...Jo:DF...<..h6N.c.. .....'wr%..|..Z6.%....Gm...9pW.I?.'.Q.0.?....:..^G-.}.....TE...2.|.?..2..!.Q....c..*!....R.9....*0c...xR..5.]V.$._.x^..t.'..o.....;|<.rF...bE..'...F..$.m;.%h;v.!PC.....!.C..F=.t9|....!.\.....^ ..^_.|.....H...1..*_'!o*..g...!.2.&.K.F=.0....(Dc...-.L'..@.d.O..6nh....[..YJ....\.nTH,.....qA\n.w.}..Dp.8E....OV..&.{..I..mi[..)0.K.....;M$..''C.O..h....l..C}.....c'.h.....+....T...e2_kI..5^z..... U...nv.r.t.t.....U%....h[...M.RM.a.n}...y.n.$....T`$.[{V2K.V.6.lgOH..C...N..L.^.^tTF.....%..I..>.?..H4...@-....#./C>Bm.@..}I..D....=.....o

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\mem6YaGs126MiZpBA-UFUK0Zdcs[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 17440, version 1.1
Category:	downloaded
Size (bytes):	17440
Entropy (8bit):	7.962704570077627
Encrypted:	false
SSDEEP:	384:2QHZz7pdg60gyjkXImq2+GTFGc+Hq8pMG2dKQWS:9HTyAYa+GIHzyKQX
MD5:	06B4BFDA4E139EAF3AB9872A6D66F42F
SHA1:	E5C5999D6AF4869BC60EEA92D1A8C328FB0E1378
SHA-256:	39EC493A5A688A85B60A1E889A22CFB93F23C900E0FDC0BE8AB8543DC9DAA783
SHA-512:	D6665B3CDD7E759D4A2B1BF916654A9C7FCA24ACBEBA1FB4A75668F5B451C7542B5683C097A6A62ACCE76B98694A4F6847CE2DC5193113D02200A04EC85A658
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/opensans/v18/mem6YaGs126MiZpBA-UFUK0Zdcs.woff
Preview:	wOFF.....D .....d@.....GDEF.....GPOS.....GSUB.....X...t...OS/2.....]...`~l.=cmap...`.....X..cvt .....W.....fpgm...l.....~a..gasp.....#glyf... ...4...M..o*.head..< ...6...6..z.hhea..<X..."...$. ..hmtx..<\|...*.....=A.loca..>.....\|.maxp..@h... ... .name..@.....%`@.post..At.....x.I..prep..C0.....T..... .....x...5.A.....m."gW..`.L..&N".?.....IF....a.^...b1.....Uh."4...>..=x.c`f.f.....:....Q.B3_dHcb```.fccfeabbi``P..x.....:.;302(...&.O.....)B..q>H..u..R``..?i.....x.\.!..q..... .#aff...#1Q@.'U..@5.".llt.Aa#.f\|c.W....'..X..!..C...ITPE.;..V.j.....0. .L0E...Yd.mN....:.....F....GG.g.s,x.>0....v..I;o..<.$G9.\f2...e{}.IS2..uc]p.....M.x.c.a.g.c..$KY...e@.,,.."..... ...?.....g....Z...[..5..=.d.....p.a.C?C..L...FF~..,...x.uTGw.F.....)..)7.W.$`*.....G.Kz.)e....t.|.1.7...s.g...3.7mgf..~{1...s.3.S...co..o.~.Zy.u...kW.\.t...N.KG.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\memnYaGs126MiZpBA-UFUKW-U9hrIqU[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 17788, version 1.1
Category:	downloaded
Size (bytes):	17788
Entropy (8bit):	7.967181593577758
Encrypted:	false
SSDEEP:	384:Vp3UxvLq7eMDKdiXVYFbQk9YlD/XmhJGSiQ3L+CEW/9fE+QH:jgjq7ejOQMUeD/AGO6CB/98+QH
MD5:	92DA6F116D973BD334CF9B3AFDB29C4F
SHA1:	C7E59C92F4D8391276FB0A3A55528CF3965478E7
SHA-256:	49B6274BCCB5C6B31E20CEBB213D96197B522B1FB9C95B8649A0626EDB5BD9D8
SHA-512:	B3483F5137EAE074BDC95262B8C5D6049C4E7AF276F3EB1DDC3097ED3FBFB2C43110341B78E0B388E6B9B5D186168CD86DA324496CB08F909C60FEBFB3E207F9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/opensans/v18/memnYaGs126MiZpBA-UFUKW-U9hrIqU.woff
Preview:	wOFF.....E|.....f.....GDEF.....GPOS.....GSUB.....X...t...OS/2.....]...`....cmap...`.....X..cvt .....o.....fpgm.....s.ugasp...(.....#glyf...8 ..4...N.-.W.head..=0...6...6....hhea..=h..."...$....hmtx..=....8.....\|&.loca..?.....P..maxp..A.... ... .name..A.....8Gtpost..B.....x.I..prep..D`.....@..R..... .x...5.A.....m."gW..`.L..&N".?.....IF....a.^...b1.....Uh."4...>..=x.%..@0...?.%.N.O:Zg..TjL...Bk..-.a ..5.j.F...`...^..3.V.P..P.4..c....[..]..9.... ..T(.q...x.\.!..q.....#aff...#1Q@.' U..@5.".llt.Aa#.f\|c.W....'..X..!..C...ITPE.;..V.j.....0. .L0E...Yd.mN....:.....F....GG.g.s,x.>0....v..I;o..<.$G9.\f2...e{}.IS2..uc]p.....M.x.c.a.g.c..$KY...e@.,,.."..9....x.....3.....e.. =L.....`.Q..1.Q.....uF.F[F}Fe.....-.p..... ..x.TGw.F.....)..)7.W..`*.j.-...=*'_..sI...2...O>....[tt....TK]..|...G.....^.m..=..x

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\microbg[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 1920x1080, frames 3
Category:	dropped
Size (bytes):	180224
Entropy (8bit):	7.973734325413064
Encrypted:	false
SSDEEP:	3072:1tCHaIq+IP65jlKmSYZdgLO8TWRLz8AQ/jQRCBV3YBK0e:fCbqQ5UnngLOssLz8NL7c9e
MD5:	6B25BD89F80EC4502D8917B127C8FA85
SHA1:	C832D9A04BF647AE231FAC028EB5462BE23799F6
SHA-256:	92F3B7F5A652DD92625FC352980A3A2EAA085DA38F68E2488DE370B828CB1185
SHA-512:	6478A6536DD3652DB4CF5A042D76EF421BA2CEAC57EC632FEB59D62F60FF4987594296A142E42D79A7FDB91A66C833677DD1C4638A1701477F9242FBC33982A3
Malicious:	false
Reputation:	low
Preview:	.....JFIF.....C.....%...#... , #&')*)..-0-(0%()(...C.....(...((((((

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\microsoftlogo[1].png	
Category:	downloaded
Size (bytes):	697
Entropy (8bit):	7.573455613491714
Encrypted:	false
SSDEEP:	12:6v/7CZCVY4qjw64PjBxIpZDyGhCRGk0gOEsX09+tg+I/fux2KMiHxqDCDl3MAuk9:bZCVY4qjA7BGZDjhC0hVEKS+I+71RVCq
MD5:	E8F6445B7B7F0B26B63CD135E8BB3B3D
SHA1:	52C38CDD5696EE485D076F1B0FE40032B1BC608D
SHA-256:	089AA7FA65A4038B4AB9130D083E6BCC24B0E33F5018984EF1463B8516BC7993
SHA-512:	9AECE19461CF95558FA97EB0D7FB9D7CB5133FC31D651F76EA8B29986B4EBD1FB9D70B6D35DB13EFB9E27E0F6C71595D54B029E8673A37C39329450AF2898B76
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://sbccpro.com/OMMOM/OM9u8/images/microsoftlogo.png
Preview:	.PNG.....IHDR...s.....f.F...KPLTE...sss..3~.....=..>...O3....N3.O4.....{{{.....O3..$...)IDATH..... ....U.....KhE;....[Z.....@..#m..,g..l.->....-..._f..r.?..... 1... ....+.L.&1LD..&.g.q.....D.j..=.b.{...I....7...+.....{.....$.I.....4..m...B.Ef..v.....g3((c....r.....C'..]=.O.w...J$..3a..Dx.`.cY...1\..8k.IeZ.Z$...:..x..\.,.I.....-]^.g.1..8_Ke.D.....`b....a. KAr....y...p...U*3.+.%.`...za-.X8>.W..9g6..\0Q...7.....1R.(...bJ.:u..0.8.0.Po(.=N...)[s.1]..,.....V.ucN..P.K.4~.LY;...#..A.....Ll..*L.N..,D!_1C.U.Ju.....O.....C.JnO.^k/.).h.?....Pq.. '..2.)c..?&.9.\..k.s.I.....q6..}`.S.....U.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\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/161351041007_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\3Y2ADQKS\office[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 512 x 512, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	6290
Entropy (8bit):	7.704429943211795
Encrypted:	false
SSDEEP:	192:5PesVaBqtC11xXiQU2SrR9PDD+2p4SWnR3m4UMWx:Zwyi3iQZSrRBDHmfHUMe
MD5:	1AC039422D7C9CEE436B2CAE5C00BD8C
SHA1:	60D9B9A6E2DF337578C35472344F1387775046D8
SHA-256:	1500514ADF9E666A3D20530815DF881BC94812C6906A53BD4C216D051D18C372
SHA-512:	03B225379AD1B46E3AF9AA3218812AED61D70431B17D75842E3CD426DBD960E940FB8C127F8D9DF7251039034A43848CE3EB612ED7B98D9A69050AF7CE7B0D7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://sbccpro.com/OMMOM/OM9u8/images/office.png
Preview:	.PNG.....IHDR.....$.....PLTE....'..)..'.,,,..)..*..*..(..(..)..-..'..(..(..)..*..)..*..-..*..'..)..+..+..+..,,,..+..(.,,..+..+..+..+..+..(..+..+..*.,,..<.....8..'..:.....zQ.....5..;..2..0.....8.....9..7. .6.....@..2..I..5..F..P..B..8.....M..e5.0...q.*.4..1.....c.X%.T .3..,.....j..X..y.].oC.a0.../..+.....~....-..wM.i;.:.....=.....sH....I?.5.....(.....7..2..;..:..*..0.....)tRNS..... .....cVPA-...\jfsH..7z=.s;....IDATx...i..A...gfr..ksm...e2..$fF...[RH.$. l9.UTa.../...E.;..}.....t.....*...=..L4#...i..&.m.....#...l%DA..]..... .=.zn.....h n.....q.v.....5....o..J!.,....]..5....n....n.iw].....M..r$....n.i....k..Z&R... ..]Q.....+.....5P.hq.....J..;:...Zv..A..M.\.._s.Q2Z.=.....Z...).....,_.....t.o..".&.,.....RK$.%m...Cm{ n.DQ...:0....$..)..7.v...@5\....n=.y.pU.....UIY.:x...*.H...{.X%.Uc..>.X.....>..K.x.....6.i.l.`.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\oreolazylegacy[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\3Y2ADQKS\oreolazylegacy[1].js	
Size (bytes):	178185
Entropy (8bit):	5.318051417022481
Encrypted:	false
SSDEEP:	1536:6P4JABh+feZpBBZ95BM7Syn6lFhoDusHYCKf7SKENC3YPhtzn34bGYXT209lFem:hQBM2yn6VoXHxS207J
MD5:	4B2BB5EC10F6AE38EDB681DC3DB5D887
SHA1:	F78BD467E16CF41250C6D371F2E89C0D878A8099
SHA-256:	8D8C85092C0BB45F7B97EA98C52578181A1FF0E57554EBE048564A551BCA0E4D
SHA-512:	B4D6F54F904BA726E01F3DABF4AB01EB112C0F2CCEC24586E256A53A60DB826EFDF52F36670DB1001C955627AE380B5221C5D30C11A214CF56229653C21D0C7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c1-onenote-15.cdn.office.net/o/s/161351041007_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\3Y2ADQKS\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/161351041007_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\3Y2ADQKS\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):	114384
Entropy (8bit):	5.361393638753441
Encrypted:	false
SSDEEP:	1536:76kVo7kHOxMFVA8n3Zv99kE/XdpJO0/zsZcZTzMAVyLZrOsWE:pVo7dxMF119JzocMzrOsWE
MD5:	7E8BB40C3F91A85BA4055DEDC5BE8859
SHA1:	AF78F5E08E26A2DBF5EE0B56A1002B69F2409B1E
SHA-256:	439AFF99AA293D041973E06996F4B3BDF7E4BA64C3935B2751ADA48F012DEC89
SHA-512:	2E7BB0632704D2839AA7C71B861BBC82F6D824F1312D21ED454F18C1122B2620DA673B54D7AB90C9FBB7FFDE49E86CB3281A19C15B0940BBEB441F512E75A21
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c1-onenote-15.cdn.office.net/o/s/161351041007_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=10)}([,,,,function(e,t){var n="undefined"!=typeof crypto&&crypto.getRandom

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\oteljs_agave[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\oteljs_agave[1].js	
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\3Y2ADQKS\outlook[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 213 x 211, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	1746
Entropy (8bit):	7.472505060810825
Encrypted:	false
SSDEEP:	48:lq3EkZ80zZgcSoWu+NIG208DXIbsXzVLp:qEGZgcMMGx8DYgXBp
MD5:	CACDEE9959D34380D727718FD02B3711
SHA1:	EB971467C555EA2299CC31018C8BC85F67DA59D7
SHA-256:	17F02FDB590800C9A21E2B6166F5F22CC54952D58897F09D8E82BB9195BC2071
SHA-512:	4F0A4BB3219BA1F9AAE6B527B9125FEE3327BDCA82142DFC23E6E6C5F4481065A221291A35BBCF1E35CFE9EE658AB22E4BC85DC58C17A2B95C5FC2846986FB66
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://sbccpro.com/OMMOM/OM9u8/images/outlook.png
Preview:	.PNG.....IHDR.....!.....PLTE.....T...2tRNS...Ji.Gd.=.@....X.g...\:. ..aMC.....}!.u'.P.5.S...p*Gi2....IDATx...is.@...n.....}.#.f...[t....qa...[.E.&O..A*.EQ.EQ.EQ.EQ.EQ.EQ.EQ.EQ.Y.U.....=.....aU..c...T..b.ztPu.;.ytPY.f..tP-....@U..... h..S....TVn .ytP9... ..s..h.....j\Z.D.....j...A...#..B"...HE..HE*!R.*$R.J.T...TiQ.!,.....`.^%....4...2..ei...L.U..b.HG.k.N....V...4:W8.Q.1.V.Tmx./.I.../UeN.n*dN}.T...P...._..H...h.....T]._]..q>.O... Cu.....s W.jU....p........"......BU..*..!..*S...P'.p...Q..~E.*i....E%.....U..>Q..j.B.q.%..q...T....j.Q.P..O....\..U.8j.JT...!2....KV.....*l.....{....JF-..<Y...Q.t.OSL.....U.%*.....OO,.-.H.....E.-i....g.Y."U3|9.'...A.J..Q.W./..G5z.H.]...:%MA...%.t...BC|f..e...3.0.]._f-.QPMPeG.4..;....[.(u*.{.F.W..L...r.Q=P..{.8G.Y0..X..gMP.._.3@...u.*...[....@.j.c.Y.P!L..w.#a.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\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\3Y2ADQKS\plt.resx-plt.chunk[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):	558

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\plt.resx-plt.chunk[1].js	
Entropy (8bit):	5.041396051587785
Encrypted:	false
SSDEEP:	12:lD7Uz1NUyZer8jliPWf5QHvEz77K7OCi8zfz1Qp71aX4cJT7LXH:lDYBeKer8jliE2HcnehiWfKpJ24cJTP3
MD5:	74C0A497402AB1504DCBD4A027E9EF15
SHA1:	43CD282060D94F937CD27E68685EC57528002E21
SHA-256:	4C67C128892766417F504625C83F99D248EF73776BC8104D78261598AABDD366
SHA-512:	78E79BB2B820BF070B0C0E9EB0EE7D02BB20881B0E95957E61D650AA63CF55B7D4F35BAE7BD382E580AD229FAADD7B2CA9989D8A02F30AE9717EF59883DB7307
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://spoprod-a.akamaihd.net/files/odsp-next-prod-webpack_2020-11-06-sts_20201106.001/wachostwebpack/en-us/plt.resx-plt.chunk.js
Preview:	(window.odspNextWebpackJsonp=window.odspNextWebpackJsonp||[]).push([["plt.resx-plt"],{32:function(t,e){e.e={"ShareDialogTitle":"Share","SSOSignInNeededNotification_Title":"Sign In","SSOSignInNeededNotification_Description":"For added security, Office needs to further verify your account. Please sign in to continue using your add-ins.","SSOSignInNeededNotification_SignInButton":"Sign In","SSOSignInNeededNotification_CloseButton":"Close","PickerDialog_MoveToFolderPickerTitle":"Move to","PickerDialog_MoveToFolderPickerCompleteButtonText":"Move here"}}}]);

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\Acl1033[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	19181
Entropy (8bit):	4.3590974373798
Encrypted:	false
SSDEEP:	384:im1leaXgjDSEcE+fg1gKzqF9meWFaUOKco5FXp/kf/oezD:b1leajD0kiDlgMJkly
MD5:	D9604CC18F364A6ADE707B7FAAEC642C
SHA1:	F38F0B94764184D4373886FDA1CA87D352BFCE5A
SHA-256:	F282423F48F12F56419363384F3B10002C8D3D106BC1AC8FF721602AA2B2FD9B
SHA-512:	7B305607B79F077539E3C37CD46EAFBB9E4C9B2A8825217187515CD20FFBFE204BAC43E918CD4440EB65A3A2DCFFC4140D06B43845613D48566448765B3D5DF
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://onenote.officeapps.live.com/o/App_Scripts/Acl/Acl1033.js
Preview:	.var AutoCorrectList={"(c)":".","(r)":".","(tm)":".","...":".","abbout":"about","abotu":"about","abouta":"about a","aboutit":"about it","aboutthe":"about the","abscence":"absence","accesories":"accessories","accidant":"accident","accomodate":"accommodate","accordingto":"according to","accross":"across","acheive":"achieve","acheived":"achieved","acheiving":"achieving","acn":"can","acommodate":"accommodate","acomodate":"accommodate","actualyl":"actually","additinal":"additional","addtional":"additional","adequit":"adequate","adequite":"adequate","adn":"and","advanage":"advantage","affraid":"afraid","afterthe":"after the","againstt he":"against the","aganist":"against","aggresive":"aggressive","agian":"again","agreemeent":"agreement","agreemeents":"agreements","agreemnet":"agreement","agreemnets":"agreements","agressive":"aggressive","ahppen":"happen","ahve":"have","allwasy":"always","allwyas":"always","almots":"almost","almsot":"almost","alomst":"almost","alot":"a lot","alraedy":

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\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
SHA-512:	7831E45A05F1F589F379449808C49F9AA8B615E9981331703F7FB588DCC0AB059084DF4C807DD2AA007A2BF4F34F67F72C4C9E2572E28B1DE473595E6AD1D1F2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c1-officeapps-15.cdn.office.net/o/s/161351041007_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\9QTQHWWN\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):	1380286
Entropy (8bit):	5.609047396336263

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\OneNote.box4.dll2[1].js	
Encrypted:	false
SSDEEP:	24576:dMGqdBgsOFgRILxyPejPitnXR11XaNc+PqNX83Lfw4bHvNLQttWRujWHmreKXbX:dMGqdBgsOFgRILxyPejPitnXR11XaNcb
MD5:	D2BB4B31EA071799CA5D118706B3CF06
SHA1:	022E9148A04F3C37F30F4DF67CF213D4F95D546C
SHA-256:	AE0CA6F4ABB29FEA51360670C4D50DDFC36B49313E4152AB0786D33BF170447A
SHA-512:	C4A584B9BF7762CCC0DBFCE332EE8ACF9C5DFA96605526C5471AE02F22BAF06ECAB7B6CF998069BA8399FF0E6ED9580A69228C1D69EDF33B53F4B1A2B9414F33
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c1-onenote-15.cdn.office.net/o/s/1613510410007_App_Scripts/OneNote.box4.dll2.js
Preview:	function wac_M4(){return wac_d3b.qa()}var wac_N4=!1;function wac_O4(a){a&&!wac_M4().jc(a.zj)&&String.format("Tag Indent Type not defined for tag {0}.",a.zj)}function wac_z9b(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_A9b=null;function wac_B9b(a){if(!a)return null;wac_O4(a);var b="";1===wac_M4().H(a.zj)?b="\n":2===wac_M4().H(a.zj)?b="":wac_M4().H(a.zj)||(b="\n");wac_N4=!wac_42(b);return b}.function wac_C9b(a,b,c){if(!b)return null;wac_O4(b);if(c&&1===wac_M4().H(b.zj))return wac_N4=!0,"\n";if(c)return"";a=a?2===wac_M4().H(b.zj)?"":"\n":1===wac_M4().H(b.zj)?"\n":"";wac_N4=!wac_42(a);return a}function wac_D9b(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.zj)){for(var c=0;c<a.xub;c++)b.append("\t");return b.toString()}return""}.function wac_E9b(a,b,c){if(!a)return null;wac_O4(a);var d=new Sys.StringBuilder("");if(!(a.gi&&1===wac_M4().H(a.gi.zj)||wac_N4||2!==wac_M

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\Outlook[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	9075
Entropy (8bit):	5.166359155420789
Encrypted:	false
SSDEEP:	96:RL9O4DZ+Stb/jY+eo4hAryAes9mBYYQgWLDmnhGzoxLrPPDlcOyeBLYYnNdt72tR:x9ToSBjlevudl9nKwMxzNYYN/mma
MD5:	41533DAD7B078D172234686E36B80E5B
SHA1:	695F0E1AE148DC62106C2044C362DEBCEED2F4C9
SHA-256:	6353840890F462A1DE1A412650A42F45E935071015B837C1D703C0BBAAFED53C
SHA-512:	D31D54559490C6B16ABA5477029F85D4EE7F4002404DE44201D4810A809E8697D2729470517630A66969917132BA84BFE2F1E1E75EEFAA335EA7DAE77574E7A0
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://sbccpro.com/OMMOM/OM9u8/Outlook.php
Preview:	<!DOCTYPE html>.<html lang="en">. <head>. Required meta tags -->. <meta charset="utf-8">. <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">. <title>Sign in to your Microsoft account</title>.... <link rel="stylesheet" href="css/bootstrap.min.css">. Font Awesome CSS -->. <link rel="stylesheet" type="text/css" href="https://maxcdn.bootstrapcdn.com/font-awesome/4.7.0/css/font-awesome.min.css">. Bootstrap CSS -->. <link rel="stylesheet" type="text/css" href="css/style.css">..</head>.<body>. .. . .<svg xmlns="http://www.w3.org/2000/svg" width="108" height="24" viewBox="0 0 108 24"><title>assets</title><path d="M44.836,4.6V18.4h-2.4V7.583H42.4L38.119,18.4H36.531L32.142,7.583h-.029V18.4H29.9V4.6h3.436L37.3,14.83h.058L41.545,4.6Zm2,1.049a1.268,1.268,0,0,1,

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\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):	614119
Entropy (8bit):	5.329974265240377
Encrypted:	false
SSDEEP:	6144:mhC807hbNdMCCH5Bu32WGPCOcmmRGnlG4Wx2Bo36Mi1+oevOnjF:mhC8WaBteRGIVxIM/oe2B
MD5:	236184CE940B144634053CA3C5D9E367
SHA1:	A30C085BB47CD74478753806F6527AEC2E4D5AE7
SHA-256:	582EECF7578F0311A7DEAD1478CE91B76316F12912E9883FB89E0CB65EAFA2E9
SHA-512:	19E9B91B3B4F79F550935252497CAE2BEB38EB132AD50A4849FF86C6EDC6DDC2631BDB80261F0F0CB45FBB5668B15D713F83C4B85CDF174B5781C7505D457AB0
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c1-onenote-15.cdn.office.net/o/s/1613510410007_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\9QTQHWWN\appChromeLazy.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\appChromeLazy.min[1].js	
Size (bytes):	582461
Entropy (8bit):	5.411377423337266
Encrypted:	false
SSDEEP:	6144:UmS0ON2LUKrnKmx1G1AMVUL+EwjzMGsTghSki+4YDCEA+hNHFYOg:UmS0yg5GOLovsAJ/AANK
MD5:	474225C3C74E6E5D3D358CCA837CA23F
SHA1:	AB7BBDF48D4D49104EF0E46AB8ED2349510E7ABF
SHA-256:	5482972424873FB298D438E3385116F145FEE968EF76873F6926C156BC20485D
SHA-512:	A41B88745CEFDDC59D33CC0ABAA83BC1337EE9EA42B51B9016527B987A8E27FD46BD5533306F6297EF6C0B0F3449AFA4282E8C71F40EE54D5968C50D7705195
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c1-onenote-15.cdn.office.net/o/s/161351041007_App_Scripts/appChromeLazy.min.js
Preview:	(window.webpackJsonp_name_=window.webpackJsonp_name_||[]).push([[5],{1397:function(e,t,n){"use strict";n.r(t);var o=n(954),r=n(0),i=n(1),a=n(13),l=n(1454),s=n(1474),c=n(509),u=n(65),d=n(1955),p=function(e){function t(){return null!==e&&e.apply(this,arguments)||this}return Object(r.d)(t,e),t.prototype.render=function(){return i.createElement(d.a,Object(r.a)({},this.props))},t}(i.PureComponent);var h=n(1455),f=n(1456),b=n(1941);var m=n(1927),g=n(1928),v=n(1929),y=n(1482),C=n(1479),O=n(1930),S=n(1956),T=n(3),j=Object(a.c)((function(e){return{root:{height:40,marginRight:8,display:"flex",alignItems:"center"},wrapper:{display:"flex"},fieldGroup:{height:28,display:"flex",alignItems:"center",marginLeft:10,background:"#ffffff"},field:{height:24,width:e||130,paddingLeft:4,paddingRight:0}}})),k=n(40),x=n(153),w=Object(a.c)((function(e,t){return Object(T.H)(j(e),t)})),I=function(e){function t(t){var n=e.call(this,t)||this;return n.ribbonInputWrapper=i.createRef(),n.appInput=i.createRef(),n.keydown

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\appIconsLazy.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):	291691
Entropy (8bit):	5.333695935208213
Encrypted:	false
SSDEEP:	6144:pkK30j1m+AvPSIoPaVNNmz+iANGt4VCpgYT:pj0jkNO+iF
MD5:	B89C248D2B5336A75190A0A78064D388
SHA1:	BB4CE3C03FB6140D8CE10D8EAE9BB5613E7524F1
SHA-256:	302DC3A093E5D83B59E59AA23A27E7EE288E4DEEA0A123D67F3BE282D2F0BA1D
SHA-512:	D349032900E2526F5FC171D20B73B66BEA66ED747140A78B3CCA580D46616162F98526B2314E96BE5AE98E5258196204325BA2CE92FA5ECA5BD64B6F0A190BAD
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c1-onenote-15.cdn.office.net/o/s/161351041007_App_Scripts/appIconsLazy.min.js
Preview:	(window.webpackJsonp_name_=window.webpackJsonp_name_||[]).push([[6],{1490:function(t,e){var r=t.exports={version:"2.6.11"};"number"==typeof __e&&(__e=r)},1494:function(t,e){var r=t.exports="undefined"!=typeof window&&window.Math==Math?window:"undefined"!=typeof self&&self.Math==Math?self:Function("return this")();"number"==typeof __g&&(__g=r)},1495:function(t,e,r){t.exports=!r(1506)((function(){return 7!=Object.defineProperty({},"a",{get:function(){return 7}}).a}))},1498:function(t,e,r){var i=r(1494),s=r(1490),a=r(1600),n=r(1504),o=r(1500),h=function(t,e,r){var l,p,f,m=t&h.F,c=t&h.G,d=t&h.S,u=t&h.P,y=t&h.B,g=t&h.W,v=c?s:s[e]||(s[e]={}),b=v.prototype,x=c?i:d?i[e]:(i[e]||{}).prototype;for(l in c&&(r=e),r)(p=!m&&x&&void 0!==x[l])&&o(v,l)||(f=p?x[l]:r[l],v[l]=c&&"function"!=typeof x[l]?r[l]:y&&p?a(f,i):g&&x[l]==f?function(t){var e=function(e,r,i){if(this instanceof t){switch(arguments.length){case 0:return new t;case 1:return new t(e);case 2:return new t(e,r)}return new t(e,r,i)}return t.a

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\bootstrap.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	144877
Entropy (8bit):	5.049937202697915
Encrypted:	false
SSDEEP:	1536:GcoqwrUPyDHU7c7TcDEBi82NcuSELL4d/+oENM6HN26Q:VoPgPard2oENM6HN26Q
MD5:	450FC463B8B1A349DF717056FBB3E078
SHA1:	895125A4522A3B10EE7ADA06EE6503587CBF95C5
SHA-256:	2C0F3DCFE93D7E380C290FE4AB838ED8CADFF1596D62697F5444BE460D1F876D
SHA-512:	93BF1ED5F6D8B34F53413A86EFD4A925D578C97ABC757EA871F3F46F340745E4126C48219D2E8040713605B64A9ECF7AD986AA8102F5EA5ECF9228801D962F5D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://sbccpro.com/OMMOM/OM9u8/css/bootstrap.min.css
Preview:	/*!. * Bootstrap v4.0.0 (https://getbootstrap.com). * Copyright 2011-2018 The Bootstrap Authors. * Copyright 2011-2018 Twitter, Inc.. * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE). */:root{--blue:#007bff;--indigo:#6610f2;--purple:#6f42c1;--pink:#e83e8c;--red:#dc3545;--orange:#fd7e14;--yellow:#ffc107;--green:#28a745;--teal:#20c997;--cyan:#17a2b8;--white:#fff;--gray:#6c757d;--gray-dark:#343a40;--primary:#007bff;--secondary:#6c757d;--success:#28a745;--info:#17a2b8;--warning:#ffc107;--danger:#dc3545;--light:#f8f9fa;--dark:#343a40;--breakpoint-xs:0;--breakpoint-sm:576px;--breakpoint-md:768px;--breakpoint-lg:992px;--breakpoint-xl:1200px;--font-family-sans-serif:-apple-system,BlinkMacSystemFont,"Segoe UI",Roboto,"Helvetica Neue",Arial,sans-serif,"Apple Color Emoji","Segoe UI Emoji","Segoe UI Symbol";--font-family-monospace:SFMono-Regular,Menlo,Monaco,Consolas,"Liberation Mono","Courier New",monospace}*,::after,::before{box-sizing:border-box}html{font-family:sans

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\box43[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 102 x 102, 8-bit/color RGBA, non-interlaced
Category:	downloaded

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\box43[1].png	
Size (bytes):	1922
Entropy (8bit):	7.799930090275787
Encrypted:	false
SSDEEP:	48:cENciM7PxxsRcCzKzVT0waLFE8ASYXamdHN:cENIgiCSVT0EJSYXamdt
MD5:	D212459353E8FD1D2514C77703D44F1F
SHA1:	A0CABB548A218E87FBCB4D4ADDEA47068A4288D3
SHA-256:	7AD89A907BFE47019D905B92D0C203082AA75852D39B480E6FBE1718A8EA3647
SHA-512:	8AA0C6904EFE31A38B2A52F05F79153D933BC48C028D18C110F59089D0EB7EAF2D97E84A42F81BAA8906AFD2BBD8C895FE53D8E998A4417422B97497556E1B7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c1-onenote-15.cdn.office.net/o/s/161351041007_resources/1033/m2/box43.png
Preview:	.PNG.....IHDR...f...f.....9..b...IIDATx^.ml.E..o.E.....B....'_$..&.&.....h....A..4.....[.....]iC..h1.HjE.....K&.....>....<3;{._.....X$..T\\(.o..#..2K....g.....Oe...C..`..p..ee%...g`. e.8....b.k.c.P.:B.tv^W..2RW.,.g.j.....y..i....2.P.....T.G...Z..5.....5H..?.H...P...9..(.h.....p}..9.tS0.....q}..`pWFK..9..(....8.....L..]O..z<.%.".4..Lj:F....4.....@..s$../bux.N.%.`. .$IN...%'{#.....<..]|....0..AYt..CDI..$...=....H)..W>.>.+G>....1b.....(..1?R.A...Q...C`...X...C..q]..&....."~.o~0.P....~(|`..^Ph....."....P.]._U0.....k.t....e.%.y3.....C`.{...._$..'....k.5.. J.`R.....'.A....0..P(4.....g...m...Z.d.I...Q.QbA..f._.nm..."....K...Cw4...k..F.e..=~..d....|s....`.V.*..`...j..ww....-..V....f.....C...6v...p.9Y..h..Wj]..._`.....Z..G.m.?..*..w)...~...(..... =a=.]a.+R...5.`.H$..D..ehW...@..2..#..j..T.w...c..T.w...#~....e.....e.k.....C.c..e.F.2.`..j..1._:....o_.j:.!0...%....9..c.....OY0.;....0|.U>.@`...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\css[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	1887
Entropy (8bit):	5.187998229445049
Encrypted:	false
SSDEEP:	48:SY3QW9Y3QLZY3QxTGY3QC7Y3Qw6QOWGOLpOxTvOChOw6b:SYgW9YgLZYgxTGYgC7Ygw6QOWGOLpOxo
MD5:	7AD11B51C8A9918ADE502DA9DE063EFF
SHA1:	ABF598711588628073EE60E294F288AB76EA187A
SHA-256:	5A270BD50EF12A93ABAE711C806D6C59D58B0E0D2A9B3463A8268DC3D2EA6857
SHA-512:	6932EACAB01B2443439A31537BC694BB6F611473BE6FC702DBCA92BC2DE27736F2A363744F14CCCDE7C05E660ACCADDA66523E5068371EFBDD8551B2375458A
Malicious:	false
Reputation:	low
Preview:	@font-face {. font-family: 'Open Sans';. font-style: italic;. font-weight: 300;. src: url(https://fonts.gstatic.com/s/opensans/v18/memnYaGs126MiZpBA-UFUKWyV9hrIqU.woff) format('woff');.}.@font-face {. font-family: 'Open Sans';. font-style: italic;. font-weight: 400;. src: url(https://fonts.gstatic.com/s/opensans/v18/mem6YaGs126MiZpBA-UFUK0Zdcs.woff) format('woff');.}.@font-face {. font-family: 'Open Sans';. font-style: italic;. font-weight: 600;. src: url(https://fonts.gstatic.com/s/opensans/v18/memnYaGs126MiZpBA-UFUKXGUdhrIqU.woff) format('woff');.}.@font-face {. font-family: 'Open Sans';. font-style: italic;. font-weight: 700;. src: url(https://fonts.gstatic.com/s/opensans/v18/memnYaGs126MiZpBA-UFUKWiUNhrIqU.woff) format('woff');.}.@font-face {. font-family: 'Open Sans';. font-style: italic;. font-weight: 800;. src: url(https://fonts.gstatic.com/s/opensans/v18/memnYaGs126MiZpBA-UFUKW-U9hrIqU.woff) format('woff');.}.@font-face {. font-family: 'Open Sans';. font-s

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\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):	5.292369583998287
Encrypted:	false
SSDEEP:	48:EqQWqp+CNWqp+JTY4TbgNWqp+aNWqp+nNWqp+PNWqp+qrogAdPZXQ1n791RapkHH:hQWqp+eWqp+jbQWqp+mWqp+NWqp+FWqv
MD5:	319A74BD0205E9B1C13D266FA86A9115
SHA1:	32A21756C24FAD2779BCC2DDA8852D23568ABA30
SHA-256:	4DFAC1D58ED8160FC92FAB50F2BA2D31E294F35A6944A418A2C868A6A575DECD
SHA-512:	C50114A249D68D470F4DF5D529EB7E1ED9D9182B12A9D13035DE61738DA3FBD279F56F40161B234FF60CC664037EB21C9E1B8FE991CF09995255C9E5E994322
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/161351840456_Scripts/CommonDiagnostics.js" crossorigin="anonymous"></script>...<script type="text/javascript" src="https://cdn.onenote.net/officeaddins/161351840456_Scripts/BrowserUIs.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/161351840456_Scripts/ExternalResources/js-cookie.js" crossorigin="anonymous"></script>...<script type="text/javascript" src="https://cdn.onenote.net/officeaddins/161351840456_Scripts/pickadate.min.js" crossorigin="anonymous"></script>...<script type="text/javascript" src="https://cdn.onenote.net/officeaddins/161351840456_Scripts/Instrumentation.js" c

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\mem5YaGs126MiZpBA-UN7rgOUuhv[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 18900, version 1.1
Category:	downloaded
Size (bytes):	18900

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\mem5YaGs126MiZpBA-UN7rgOUuhv[1].woff	
Entropy (8bit):	7.96514104643824
Encrypted:	false
SSDEEP:	384:nejx4dDcsFhu/3v79dEAUdH6XSw1fz9fKQm9LQNG/X1epB:ejadDrhYTf3Udaieza98Nbz
MD5:	1F85E92D8FF443980BC0F83AD7B23B60
SHA1:	EE8642C4FAE325BB460EC29C0C2C9AD8A4C7817D
SHA-256:	EA20E5DB3BA915C503173FAE268445FC2745FC9A5DCE2F58D47F5A355E1CDB18
SHA-512:	F34099C30F35F782C8BB2B92D7F44549013D90E9EEDE13816D4C7380147D5B2C8373CC4D858CDF3248AAA8A73948350340EE57DAE9734038FC80615848C7133E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/opensans/v18/mem5YaGs126MiZpBA-UN7rgOUuhv.woff
Preview:	wOFF.....l.....p.....GDEF.....GPOS.....GSUB.....X...t...OS/2.....^...`....cmap...`.....X..cvt .....]....-...fpgm...t.....s.ugasp.....glyf...$ ..9...Y..(.head..A....6...6.%l.hhea..B,.....$.)..hmtx..BL.....O,loca..D`.....9yfmaxp..F$... ... .q..name..FD.....#.>.post..G4.....x.U..prep..H.....k..... .....x...5.A.....m."gW..`.L..&N".?.....IF....a.^...b1.....Uh."4...>..=x.c`f.g.....:....Q.B3_dHc.....@`...../..?....^..... 9.8.m@J....w..!..x.\.!..q.....#aff...#1Q@ .'U..@5.".llt.Aa#.f|c.W....'..X..!..C...ITPE.;..V.j.....0. .L0E...Yd.mN....:....F....GG.g.s,x.>0....v..l;o..<.$G9.\f2...e{}.IS2..uc]p.....M.x.c.a.g``..$KY...e@.,q@.j...o@<..O.H.t..... .....c .p@.....3lbd.....-.}.M...!...!....x.TGw.F.....)..)7.W..`*.j.-...=*'_..sI...2...O>....[tt....TK]..|...G.....^.m..=..x.q...+./].p...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\mem5YaGs126MiZpBA-UN8rsOUuhv[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 19072, version 1.1
Category:	downloaded
Size (bytes):	19072
Entropy (8bit):	7.966673384993769
Encrypted:	false
SSDEEP:	384:UCwUC2nJxPRk+P/Qvm6DBM1W71wcdDmyBE+2fweE9m0aGuTeopiH:PJC2nJxP++P/36QWpwNyb2tqgk
MD5:	05EBDBE10796850F045FCD484F35788D
SHA1:	07744CFE76B8C37096443A6BCC3FBD04F93AD05B
SHA-256:	35EB714D45479FE35586513C7D372CED0AE3E26EB05883950BEA2669C6E802AA
SHA-512:	D4F293115640C05E3134D635AA077BC91BF35E80463C93C14646D97784CD9FC8D4CD4E10EEAA7BE621DBD9FA0DE5BE943328014ED505C217E61769F76BFA7F4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/opensans/v18/mem5YaGs126MiZpBA-UN8rsOUuhv.woff
Preview:	wOFF.....J.....p.....GDEF.....GPOS.....GSUB.....X...t...OS/2.....^...`...vcmap...`.....X..cvt .....g.....o.[fpgm...|.....s.ugasp... .....#glyf...0 ...".."..Yr....head..BT...6...6....hhea..B.....$....hmtx..B....*....#.C.loca..D.....n..maxp..F.... ... .name..F.....%.@cpost..G.....x.U..prep..lp.....1..S..... x...5.A.....m."gW..`.L..&N".?.....IF....a.^...b1.....Uh."4...>..=x.c`f.cV``e``..j...(.../2.11s01qs.1s.01.400.300x.....:.;380(...&.O.....)B..q>H.%.u..R``.....x.\.!..q..... .#aff...#1Q@.'U..@5.".llt.Aa#.f\|c.W....'..X..!..C...ITPE.;..V.j.....0. .L0E...Yd.mN....:.....F....GG.g.s,x.>0....v..l;o..<.$G9.\f2...e{}.IS2..uc]p.....M.x.c.a.g``..$K..(..`.e.a.a`....C ..L..@t.....A..L..&.....1\gta.e....320.0...2.g.j...=...x.TGw.F.....)..)7.W..`*.j.-...=*'_..sI...2...O>....[tt....TK]..|...G.....^.m..=..x.q...+.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\mem5YaGs126MiZpBA-UN_r8OUuhv[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 18668, version 1.1
Category:	downloaded
Size (bytes):	18668
Entropy (8bit):	7.969106009002288
Encrypted:	false
SSDEEP:	384:Wv4QHZChiRh3lwLOf8cWN78NXpcr6gBUA9CD/q4cOPZmPO:WvwhNOkvvxC7qnc
MD5:	A7622F60C56DDD5301549A786B54E6E6
SHA1:	D55574524345932DB3968C675E1AEA08C68A456F
SHA-256:	6E8A28A0638C920E5B76177E5F03BA94FCDEDD3E3ECD347C333D82876B51C9C0
SHA-512:	1A842E5EDFFFFBAE353AD16545D9886E3E176755F22B86ECCC9B8B010FC79DB7194B7C5518CC190BF5B78B332C7D542B70A6A53B3BAF23366708DF348C2C2D 9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/opensans/v18/mem5YaGs126MiZpBA-UN_r8OUuhv.woff
Preview:	wOFF.....H.....n0.....GDEF.....GPOS.....GSUB.....X...t...OS/2.....^...`}...cmap...`.....X..cvt .....].....fpgm...t.....~a..gasp.....#glyf... ..8...WP..M.head..@....6...6..F.hhea..A.....$...chmtx..A8....._{loca..CL.....K.4&maxp..E.... .. ....name..E0....."c?Jpost..F.....x.U..prep..G.....:..]..... .....x...5.A.....m."gW..`.L..&N".?.....IF....a.^...b1.....Uh."4...>..=x.c`fig.a`e``..j...(.../2.1..`b.ffcfeabbi``Pg``..b.. 0t.vfp`P...M...C.G/S....\|...=.6 .....m/....x.\.!..q.....#aff... #1Q@.'U..@5.".llt.Aa#.f\|c.W.....'..X..!..C...ITPE.;..V.j.....0. .L0E...Yd.mN....:.....F....GG.g.s,x.>0....v..l;o..<.$G9.\f2...e{}.IS2..uc]p.....M.x.c.a.g.c..$K..$..`.g.e..... ..... R.g.....?.....x.)d.....$...."....0.#.A@X..0.....x.uTGw.F.....)..)7.W.$`*.....G.Kz.)e....t.\.1.7...s.g...3.7mgf..~{1...s.3.S...co..o.~.Zy.u...kW.\.t...N

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\mem5YaGs126MiZpBA-UNirkOUuhv[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 18696, version 1.1
Category:	downloaded
Size (bytes):	18696
Entropy (8bit):	7.96597476007567
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\mem5YaGs126MiZpBA-UNirkOUuhv[1].woff	
SSDEEP:	384:yeQHZsdOZKOIVrf0uvAxZEw5w7Yc3XGi/L6:dBbVwuvAYYw7THc
MD5:	449D681CD6006390E1BEE3C3A660430B
SHA1:	2A9777AFC07BF0BB4BB48F233ED7C4BCBDB60760
SHA-256:	57C79375B1419EE1D984F443CDA77C04B9B38C0BE5330B2D41D65103115FFD72
SHA-512:	8B8436670BB4D742AFA60ABA29D7A78F3788CBEF9353C2896AA492618CF1B22E9A0679972AB930E2F2D4732F3B979C023D25AA0FA86C813AC674524FD4ECA2BE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/opensans/v18/mem5YaGs126MiZpBA-UNirkOUuhv.woff
Preview:	wOFF.....I.....m.....GDEF.....GPOS.....GSUB.....X...t...OS/2.....^...`.-..cmap...`.....X..cvt .....[.....4fpgm...p.....~a..gasp.....glyf... ...8...W.J.4.head..A....6...6...Mhhea..A<.....$...#hmtx..A\... .....lT.loca..C\.....6..umaxp..E@... ... .t..name..E`.....#.@Ppost..FP.....x.U..prep..H.....x..n..... .....x...5.A.....m."gW..`.L..&N".?.....IF....a.^...b1.....Uh."4...>..=x.c`fy.....:....Q.B3_dHc.....@`...../..?....^..... 9. .m@J.....x.\.!..q.....#aff... #1Q@.'U..@5.".llt.Aa#.f\|c.W.....'..X..!..C...ITPE.;..V.j.....0. .L0E...Yd.mN....:.....F....GG.g.s,x.>0....v..I;o..<.$G9.\f2...e{}.IS2..uc]p.....M.x.c.a.g.c..$KY...e@.,A.".m....x.....3 .....?.[.o...2...:...a..b.)@.Y.....v1.b4d...36 ..x.uTGw.F.....)..)7.W.$`*.....G.Kz.)e....t.|.1.7...s.g...3.7mgf..~{1...s.3.S...co..o.~.Zy.u...kW.\.t...N.KG.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\mem8YaGs126MiZpBA-UFVZ0d[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 18100, version 1.1
Category:	downloaded
Size (bytes):	18100
Entropy (8bit):	7.962027637722169
Encrypted:	false
SSDEEP:	384:aHQHZuiZQFFImUy1oml4hN2Vmw1Qa57YC74ObDDj08X0UJQiXc:1ZQT0UySml4bEmAP5EC7PbDH4U1M
MD5:	DE0869E324680C99EFA1250515B4B41C
SHA1:	8033A128504F11145EA791E481E3CF79DCD290E2
SHA-256:	81F0EC27796225EA29F9F1C7B74F083EDCD7BC97A09D5FC4E8D03C0134E62445
SHA-512:	CD616DB99B91C6CBF427969F715197D54287BAFA60C3B58B93FF7837C21A6AAC1A984451AEEB9E07FD5B1B0EC465FE020ACBE1BFF8320E1628E970DDF37B0F0E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/opensans/v18/mem8YaGs126MiZpBA-UFVZ0d.woff
Preview:	wOFF.....F.....i.....GDEF.....GPOS.....GSUB.....X...t...OS/2.....^...`~]..cmap...`.....X..cvt .....Y.....M..fpgm...p.....~a..gasp.....#glyf... ...6...S...]head..>....6...6..cphhea..>.....$....hmtx..?.....[$loca..A4.....f..maxp..B.... ... .name..C.....&:A.post..D.....x.U..prep..E.....C..... ..x...5.A.....m."gW..`.L..&N".?.....IF....a.^...b1.....Uh."4...>..=x.c`f..8.....u..1...<.f.....A.....5....1...A.._6..".-..L.....Ar,.....3..(....x.\.!..q.....#aff...#1Q@.'U..@5." .llt.Aa#.f|c.W.....'..X..!..C...ITPE.;..V.j.....0. .L0E...Yd.mN....:.....F....GG.g.s,x.>0....v..I;o..<.$G9.\f2...e{}.IS2..uc]p.....M.x.c.a.g.c..$KY...e@.,.."..... .....?....%.g....Z..... ("..o..Y..Bu342.e.....0.....M=.....x.uTGw.F.....)..)7.W.$`*.....G.Kz.)e....t.|.1.7...s.g...3.7mgf..~{1...s.3.S...co..o.~.Zy.u...kW.\.t...N.KG.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\office[1].js	
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):	57201
Entropy (8bit):	5.309039085120872
Encrypted:	false
SSDEEP:	768:tJorInC5jiwkD9Hr09qZsOVeeo7BhEvmU7NOLS9KRuiUYg+Chgs3R3fHNaCyMJ/k:tCcnUVzUgS9OuGoGCl/U
MD5:	D57F7BF8C18FC2648AAD45BFE836F62A
SHA1:	A63A3F24DAEE2C8CFCD7496DB9B29049E5F13A33
SHA-256:	FD9F453B6F3860B242C515B0E2F33561F0434F9A67E0D1011E1A5905DB6BEC04
SHA-512:	22ED5F6DCF54C7B56EE05830E5046D49399F82472EF076DB59A9A21D83A08F81070B3F6943DC3200D66B1EFC3FE52B740A72AD77F810A532647CAA53540D23D8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://appsforoffice.microsoft.com/lib/1.1/hosted/office.js
Preview:	var OSFPerformance;.(function (OSFPerformance) {. OSFPerformance.officeExecuteStartDate = 0;. OSFPerformance.officeExecuteStart = 0;. OSFPerformance.officeExecuteEnd = 0;. OSFPerformance.hostInitializationStart = 0;. OSFPerformance.hostInitializationEnd = 0;. OSFPerformance.getAppContextStart = 0;. OSFPerformance.getAppContextEnd = 0;. OSFPerformance.createOMEnd = 0;. OSFPerformance.officeOnReady = 0;. OSFPerformance.hostSpecificFileName = "";. function now() {. if (performance && performance.now) {. return performance.now();. }. else {. return 0;. }. }. OSFPerformance.now = now;.})(OSFPerformance || (OSFPerformance = {}));.;.OSFPerformance.officeExecuteStartDate = Date.now();.OSFPerformance.officeExecuteStart = OSFPerformance.now();..../* Office JavaScript API library */..../*...Copyright (c) Microsoft Corporation. All rights reserved...*/...../*.. Your use of this file is governed by the Mic

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\office_strings[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):	20232
Entropy (8bit):	4.949749847854573
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\office_strings[1].js	
SSDEEP:	384:jZKKceMj+xa6rLg4dHg1wdR7tVTvQLsljRei:jZWj+86rLg3mtpvLhRei
MD5:	02E133FBDA09AA66A741248C885CA25B
SHA1:	6DD2ABB11142E18C605072FACD7DEE3A973DE7EC
SHA-256:	0947C0AEC3A96F12CD2E8160E0D771B148B48249504C1E0474F489279D8BECD7
SHA-512:	4A46F169B5986DA71FAB7804DE4AAAF370F308D424F692C7D69E940C68C3034E4A8822E2A458068721EC77D1252EE9132436D7530F7F26D59CAE8DA3CFA57DC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://appsforoffice.microsoft.com/lib/1.1/hosted/en-us/office_strings.js
Preview:	if (window.Type && window.Type.registerNamespace) {..Type.registerNamespace("Strings");} else {..if(typeof(window["'Strings"']) == 'undefined') {..window["'Strings"'] = new Object(); window["'Strings"']. __namespace = true;..}....}..Strings.OfficeOM=function(){};if (Strings.OfficeOM.registerClass) Strings.OfficeOM.registerClass("Strings.OfficeOM");Strings.OfficeOM.L_APICallFailed="API Call Failed";Strings.OfficeOM.L_APINotSupported="API Not Supported";Strings.OfficeOM.L_ActivityLimitReached="Activity limit has been reached.";Strings.OfficeOM.L_AddBindingFromPromptDefaultText="Please make a selection.";Strings.OfficeOM.L_AddinIsAlreadyRequestingToken="Add-in is already requesting an access token.";Strings.OfficeOM.L_AddinIsAlreadyRequestingTokenMessage="The operation failed because this add-in is already requesting an access token.";Strings.OfficeOM.L_ApiNotFoundDetails="The method or property {0} is part of the {1} requirement set, which is not available in your version of {2}.";String

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\one[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 452 x 444, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	50003
Entropy (8bit):	7.954829391916008
Encrypted:	false
SSDEEP:	768:9dQqx3vH2atnqVC7X7vHisrbBElzPf+hgncNX13sWvWqcK4h1IaKOz6Uwyg069RX:Dn3vRyUXj9B02r2K4h1L5z60369RX
MD5:	31E74EFE4A35E34FF2D7BB8B37692715
SHA1:	D45F7511E3688513A9ED3A76A2F722DAEE6FBC3D
SHA-256:	4EC63BB97F6689A5C42F2018A9B841C2B4AB235F9C38650C3C5A82B2CA7F8150
SHA-512:	6E93CFB6E49E84AF9119925EF04818AD8C13EE7029E2E68B1CD668A8849411FC20ED59E3C655547044C818A7657B74CF836FAC0915C5E70AEE34CA8C92D1CE5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c1-onenote-15.cdn.office.net/o/s/1613510410007_resources/1033/m2/one.png
Preview:	.PNG.....IHDR.....@.....IDATx^...U..];..../...eG1jh5D....P...Sa.($.`4..'Z .M.@..J@d..BTd..(..... ."...`.b.....;..n.....L.....{....=.....}.....P.:....C.....\|....w.5.....q.e..Ow~ ..7...'T.....y+G?..yy...=..=...!...4..`.D.9.Y#*\.B..#.....+.9..mhK..F...M....I.....e..{..1....A\|..Z..2.=.r..*W\2.=..U.o5...k..m...Kn....n.5...=%....o.....8.....E...$.G\..m.|Wjkk.A.. ...PTh..0lhh@.k..f.....!.H...6.+...n.5.X.`.W.....E....=..>.e....s."..}QCq..}e.....Q.g.Y.....;....{6.7.x..M...9...hC. @.ur..3....s.1.....].$ *B.+.q;....#.....&..Q...y....`.2-D`v.....=..; G6...y..Zy4k.....[...D..2.c1f.../z.P.`.1.}.=..&..\.^E5ee...~.....P<kr..m.V...E.....-}...~....o..[.....Z...^...G....w.Z}.Vf+@.5.....\..\.3H...o5a..D....aX.@Q..-...../:.Pl5.2.....*.....#..../< ...r7.....w..b...{.....'.....C_.`,U.....j..k.A....WN.|...sY...C_h8....z...7)V!p...k..;\...X....@.D(b..).../n.bl.`.4...P.@....Y].@1h ...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\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
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/1613510410007_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\9QTQHWWN\onenote-web-16.00[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):	679886
Entropy (8bit):	5.257220825724702
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\onenote-web-16.00[1].js	
SSDEEP:	6144:819A78Mw0yNPekKhcdb2CQQs204jdmE6wX/Qg:o1ekKh6TfF
MD5:	CC89A8D8941AAF1A4F5C1B6A38ADE56E
SHA1:	D0C07AC9AF0F751B30D910C3B7383879CA424725
SHA-256:	C60100FD8398CDEB223D6B0C1908773F63ACD3963394663CD794D3D5A13634C5
SHA-512:	5AE452D4A095D3E84F7EB0B5788C08539F82A37A89D491A853D8F3E124EB5F4E94C3B80EBCAF69427372742A3D698FF307B37687996B85E883D79DDE6E876BBD
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://appsforoffice.microsoft.com/lib/1.1/hosted/onenote-web-16.00.js
Preview:	/*...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...*/..../*..* @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..*/...../// Sources:..// osfweb: 16.0\13426.10000..// runtime: 16.0\13426.10000..// core: 16.0\13426.10000..// host: 16.0\13426.10000.....var __extends=this&&this.__extends||function(e,t){for(var n in t)t.hasOwnProperty(n)&&(e[n]=t[n]);function o(){this.constructor=e}e.prototype=null===t?Object.create(t):(o.prototype=t.prototype,new o)};!function(e){var t=function(){function e(){}return e.prototype.isMsAjaxLoaded=function(){return!!("undefine

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\oreonotebookpanelegacy[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	93055
Entropy (8bit):	5.761950482750406
Encrypted:	false
SSDEEP:	1536:SaIPhshxMyiCS8y5W/kGSwKarTJeVdFR5z/5RyENE+MW5C7ilpo5YKO2WHkkOZvz:SaA8iCS8y5W/kGSwKaH8Xx/5RyENEnrz
MD5:	3077B9A39F3CF596DE6F81A3846AA312
SHA1:	FCF5EEE342DB9BC338C44E1080954674954BC000
SHA-256:	75DCF292D21C4EA337F683725BB7608B3F9F255193D74BB908CFEFB2D75E72D9
SHA-512:	0346026930032829B4916BEAF69216A46C8133A3C867C4E2E9DED7D26920A1B3E0F032B401F358B90364AE585206BADD10231CFE81A4336194CD3959353EFF6A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c1-onenote-15.cdn.office.net/o/s/161351041007_App_Scripts/oreonotebookpanelegacy.js
Preview:	/*! Copyright (C) Microsoft Corporation. All rights reserved. */.(window.webpackJsonporeo_name_=window.webpackJsonporeo_name_||[]).push([[4],{532:function(e,t,n){"use strict";n.d(t,"a",(function(){return A}));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\9QTQHWWN\oreosearchpanelegacy[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with escape sequences
Category:	downloaded
Size (bytes):	153080
Entropy (8bit):	5.571140882416507
Encrypted:	false
SSDEEP:	3072:DCS8y5W/kGSwKa7BIG7y1WQ92KD9NoAwpP5CWBejCZZE:DCS8y5W/kGSwKagDwpPEWej5
MD5:	153DC017F5AB2EA6F6CE849B7865204B
SHA1:	99CE952F45BBB14985491A79A2A1DAC889DA4D84
SHA-256:	16C945194B23D671E4F2773EBF601BB3E57A68D2DA828D76D1FD87A7D66186DE
SHA-512:	268FEFB4B6F9FAD16FBF03390810CE5FD8FEC9FB48D5CB16C9564289CD4259D9426E39101DE0505AEA35AB8E5F960A0584738D46AEE6A092B81755B488C92A0E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c1-onenote-15.cdn.office.net/o/s/161351041007_App_Scripts/oreosearchpanelegacy.js
Preview:	/*! Copyright (C) Microsoft Corporation. All rights reserved. */.(window.webpackJsonporeo_name_=window.webpackJsonporeo_name_||[]).push([[5],{537:function(e,t,n){"use strict";e.exports=function(e,t){return t||(t={}),"string"!=typeof(e=e&&e.__esModule?e.default:e)?e:(/^['"].*['"]$/.test(e)&&(e=e.slice(1,-1)),t.hash&&(e+=t.hash),/["'() \t\n]/.test(e)||t.needQuotes?"".concat(e.replace(/"/g,'\\"').replace(/\n/g,"\\n"),""):e)}},549:function(e,t,n){var r=n(102),o=n(611);"string"==typeof(o=o.__esModule?o.default:o)&&(o=[[e.i,o,""]]);var a={insert:"head",singleton:!1};r(o,a);e.exports=o.locals||{}},567:function(e,t,n){"use strict";n.d(t,"a",(function(){return A}));var r=n(0),o=n(234),a={assets:[],layers:[{ddd:0,ind:0,ty:3,nm:"ROTATOR",ks:{o:{k:0},r:{k:[{i:{x:[.833],y:[.833]},o:{x:[.167],y:[.167]},n:["0p833_0p833_0p167_0p167"],t:0,s:[0],e:[360]},{t:755}]},p:{k:[250,250,0]},a:{k:[0,0,0]},s:{k:[500,500,100]}},ao:0,ip:0,op:768,st:-5062,bm:0,sr:1},{ddd:0,ind:1,ty:4,nm:"Shape Layer 15",parent:0,ks

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\osfruntime_strings[1].js	
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/1613510410007_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\9QTQHWWN\require[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	31022
Entropy (8bit):	5.181280216730189
Encrypted:	false
SSDEEP:	768:KWY0RjkG8EnrxM3IVIUsho3h8W8kBUHkIEDylyy1CLroIJt4wKb:Kj0RjkzEnrxMr+nULlg5gwKb
MD5:	E42B9CC8413D0300908B0F6105A93087
SHA1:	D703087CF79FC175AD689C4980AAE343C59C1DB6
SHA-256:	77D85EA73EB065BC9FFA6569DFC10093573C969921182314E2851D564C0B27B9
SHA-512:	9A251AF530C9268FDD625E3E6B5DDDEACF3C5B34809BA9F91C70F92656C2C419DB3CFBB69F8C522FDB74A86DD6FFB93D24F597CA071ACD0A00DD038C172D874
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://spoprod-a.akamaihd.net/files/odsp-next-prod-webpack_2020-11-06-sts_20201106.001/require.js
Preview:	/** vim: et:ts=4:sw=4:sts=4. * @license RequireJS 2.2.0 Copyright jQuery Foundation and other contributors.. * Released under MIT license, http://github.com/requirejs/requirejs/LICENSE. */.var requirejs,require,define;!function(){if("PerformanceLongTaskTiming"in window){var e=window.__tti={e:[]};e.o=new PerformanceObserver((function(t){e.e=e.e.concat(t.getEntries())})),e.o.observe({entryTypes:["longtask"]})}}(),function(e,t){"object"==typeof exports&&"object"==typeof module?module.exports=t():"function"==typeof define&&define.amd?define([],t):"object"==typeof exports?exports["es6-symbol"]=t():(e["es6-symbol"]=t(),e.Symbol=e.Symbol||e["es6-symbol"])}(window,(function(){return function(e){var t={};function r(n){if(t[n])return t[n].exports;var i=t[n]={i:n,l:!1,exports:{}};return e[n].call(i.exports,i,i.exports,r),i.l=!0,i.exports}return r.m=e,r.c=t,r.d=function(e,t,n){r.o(e,t)||Object.defineProperty(e,t,{enumerable:!0,get:n})},r.r=function(e){"undefined"!=typeof Symbol&&Symbol.toStringTag

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\style[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	10084
Entropy (8bit):	5.0668781976760915
Encrypted:	false
SSDEEP:	192:4Sz3ZfziAkFTF5bkJq0QU9esLFcqH72V2LFs:4a3ZPkFTF2g0X9ZLFjRs
MD5:	9D8F3FCC24C20CA06678AD500BF55150
SHA1:	E0100DE345BCFA97AF7C15957D7BC1B2BBE91061
SHA-256:	CC4703F492AA58E929D57812FD5A8580258006E0121DD097E866B4EE38A800AA
SHA-512:	39E2611748104EFBF9F90EC4242DF3BA33176C80B2A61343F69746F34D0FAF4E2967E5D3129F4430963AE1D2CBE3CDCC1BD6D6ECEA2D00436B1FD76364138A5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://sbccpro.com/OMMOM/OM9u8/css/style.css
Preview:	@import url('https://fonts.googleapis.com/css?family=Open+Sans:300,300i,400,400i,600,600i,700,700i,800,800i');...wrap {..overflow:hidden;.}.a:hover,a:focus {..text-decoration:none;.}..btn:focus {..box-shadow: none;.}.img {..max-width:100%;.}..webmaillogo.{. text-align: center;.}..webmaillogo img.{. margin-top: 125px;.}..webmailloginform.{. width: 300px;. margin:20px auto;.}..orangeclr .input-group-addon.{. color: #ec6933;. border-color: #ec6933;.}..orangeclr .form-control.{. color: #ec6933;. border-color: #ec6933;.}..orangeclr .form-control:focus.{. border-color: #ec6933;.}..mainpage.{..background: url("../images/landing-devices-bg.jpg");..background-repeat: no-repeat;..background-size: cover;.}..onedriveform.{..background: #1082df;..padding: 20px 70px 50px 70px;..min-height: 100vh;.}..logo.{..text-align: center;.}..logo img.{..margin-top: 31px;.}..onedriveform p.{. font-family: 'Open Sans', sans-serif;. text-align: center;. color: #fff;. font-siz

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\wacairspaceanimationlibrary[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\wacairspaceanimationlibrary[1].js	
Size (bytes):	40741
Entropy (8bit):	5.3446429692362365
Encrypted:	false
SSDEEP:	384:wwstGDociKcWpWSYnDkci6h25fZ2tF3t97D0QeIHcTzeC:wBLnDkci6h25fZyt97QLIUz
MD5:	4D07AF76BAB425647A1882400750B489
SHA1:	0C6CD11C0C329044F846641520AF0813D3B27501
SHA-256:	234CAE682920AB63F3184948F1E4103B89201A274977ED31097B844CC323AFA1
SHA-512:	94B4E969945EA18F84F0549471F35B8C99106A44AACF5E6DDB693B421AF71D02BE716198CEDE4306AFA8670A6A5E379A2535759CE84C98CD8ED1ABD3C761276
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c1-officeapps-15.cdn.office.net/o/s/161351041007_App_Scripts/wacairspaceanimationlibrary.js
Preview:	function WacCurve(n,t,i,r,u,f){this.ID=n;this.type=t;this.x1=i;this.y1=r;this.x2=u;this.y2=f}function WacIntWrapper(n,t){this.value=n;this.contextId=t}function WacKeyFram e(n,t,i,r,u,f,e,o){this.type=n;this.curveID=t;this.startTime=i==null||i.value==undefined?new WacIntWrapper(i,null):i;this.endTime=r==null||r.value==undefined?new WacIntWr apper(r,null):r;this.startValue=u==null||u.value==undefined?new WacIntWrapper(u,null):u;this.endValue=f==null||f.value==undefined?new WacIntWrapper(f,null):f;th is.relativeTo=e;this.operationType=o}function WacAnimation_ContextVariableManager(){}function WacAnim(n,t){this.ID=n;this.keyFrames=t}function WacAnimationuser() {this.AnimationQueue=new Array(0);this.sharedTimer=null;this.sharedCancelTimer=null;this.resetInterval=5e3;this.sharedTimerRefs=0;this.conflictTable=new Array(0);this.currentAnimationIndex=-1;this.temporaryIDGenerator=0}function WacAnimation_State(){this.Index=0;this.Data=new Array(0);this.AnimateRight=!1}function Wac Animation_Object(n

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\webmaillogo[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 322 x 50, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	2869
Entropy (8bit):	7.911258790344632
Encrypted:	false
SSDEEP:	48:zUrFP7iiGbmCytjS8WTZgoQWY+BCJdfJCSrUyGfwZAq53AQkvQg9wTIIs9:zUrd7JG8tOLTyoQj+B5SrUfe1pg9wTIh
MD5:	85F7EBDACD174413927BD4B787997558
SHA1:	B03207C7F3EA92E9EA0EBDC2F804947CC726965D
SHA-256:	E298D32D99708F56D68EF9CD0C44EC85910A4DF7552B5B2041FCAA48D5EE9742
SHA-512:	0806DCF23E25EF775838F30C919ABB18E49B889E24EC56FA1045EFE26406C595A13E98B437A6E0BF87A3EE66888D6B37A14825500D93C856973F4BB3C5F7818E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://sbccpro.com/OMMOM/OM9u8/images/webmaillogo.png
Preview:	.PNG.....IHDR...B...2.....&".....PLTE.i3.....t7.P.l.....n3.m3.q3....|C...v:....Y.l.....y.b....e.....T.x>.....}.....s.q..].M.....i.....%.E...HIDATh..m{.@..gR...B" B.z."......#..ds...k...'..F...;>T...[..pX.s.....y.d?...s[...:\....P.1.h..~...)...T.5.....v.....(1.S.D....Lh[z`.W.mz.....%D.X"0..`..0)v..=..D....y..7..B.X..Z.`h.....\.t.....*.d.:.G...r....X&&..`...c. .....K..."d...W...V...]....7jk...Eh.p..\..s..).~.....T.....~+6..".uJx.<.x..k.q..pB.....*..u.%.6%.-.....?e9B#.odJ..Pl|Y.....:-...20..)#..$jm4...%l.fJ.l."{..W.{.....\&.....*.,.p.pj.K.[...n.o'\.Z...*4 .Oz....%..r).C..v...8...#2.....<.a.z.IT[h^M...E./6..G^._.v.~0ju..b..j.....k9..\..3.8..S.9...-.H..):O..~Sw....;).jr.....K..F...~.m&u..iD...!0..j...o..>..i.2..P>mWG.{..!."..I...Rx..B[g. U.}s.g..s...o....G...)~...,....1..$.....<...b.`.....Qu...w5.X..].oQQ.%3*....~.=.%.1e....N..U..`@..m%....LR"K.#....:.8c*...D..._..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\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
SHA1:	6E6B66DC5C85BFC387D3DA5F4ED4FB84D6CC4876
SHA-256:	58027377795E427EDEF6224D56CF32F9641F938ADF6C919DC829CE4F748D9AFAB
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...Z...m. .M.....<.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\G62TDH9B\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\44327025345[1]	
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....>.....head.....\...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\G62TDH9B\AppSettingsHandler[1].json	
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):	1074
Entropy (8bit):	4.654118456352204
Encrypted:	false
SSDEEP:	24:YS8DZXlO/DMA3MyHQDTcoSkCcH7QwTSSGWQoKA/9WYrUkF3gMi:Yfa/DhXw/rSkTH7QwT1GWz1EZkFxi
MD5:	9D0ED8ADE7DCC1C4CC8139B5589F9B0A
SHA1:	6E0FC7E96F54DBE30F2B15CFF0C3C160545C9B86
SHA-256:	948AB2443A88C7EDBD96F33458D9C47899D0DE08F795DD92876094F00B2D9078
SHA-512:	86F0E32524566F3BFF7035F7ACB2F6459F32DF56C7245E943780D5864F46CE49E6F6BF7977D45720A9BD47F2907CA09872F1C36BFE82D4E3AE59F1E746FA480B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://onenote.officeapps.live.com/o/AppSettingsHandler.ashx?app=OneNote&usid=e36bd1de-4537-4044-9bf8-b13069c5af47&build=16.0.13510.41007
Preview:	{"timestamp":1605883275434,"BootstrapperUlsHeartBeatIsEnabled":false,"BootstrapperSettingsFetchPeriod":60000,"BootstrapperUlsHeartbeatIntervalMs":5000,"BootstrapperMaxUlsHeartbeatTime":300000,"BootstrapperNoCompleteWarning1Time":120000,"BootstrapperNoCompleteWarning2Time":180000,"BootstrapperUlsUploadCadenceMs":60000,"RemoteUlsETag":"4B8F3ED6C501271CA22B01EFB4359A5EC4565B11","RemoteUlsSuppressions":"378069,4298965,4298968,4298969,5306497,6375195,17162522,17358857,22401293,22946650,23909858,24401375,24462656,24515087,33592839,34388130,35682372,36546380,36546381,36546382,36569418,36708451,36773964,36791688,36811158,36811159,36963655,37288035,37876293,37876294,37889309,38293640,38535900,38543496,38580697,38637954,39076766,39076767,39105358,39966341,40437001,41003225,41207258,41502555,41711299,41952657,41964885,42272991,42496725,42815875,42857251,50406866,50431969,51451613,51504083,51667010,577626581,578164000,587862985,592556551,593780815,593838232,594134597,594830612,595137156,595714715,

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\FavIcon_OneNote[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):	3.675002721266739
Encrypted:	false
SSDEEP:	96:HOmS/+CtmE8mmmmm08mmmmmtf8mmmmmO8mmmmm+8mmmmmo8mmmmmo8mmmmmSC3on:AGHFk
MD5:	7A7A4890CAAA77025E1B33A6D6E474EE
SHA1:	DC735B99D9EF0C76B4A7AEAE8BAA4CBD9551BA77
SHA-256:	9E1DA5BF715135491519A188CAD977DB6CBA414071E2407B69D63221379D8802
SHA-512:	291692981A555857F95A3378B511E27B60154B95EA0BA0452B3A5536D9A63A16B00518066E4F4B60E6A73CBD2A7C46B99A18102EA5970989B9736E57A6474D30
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c1-onenote-15.cdn.office.net/o/resources/1033/FavIcon_OneNote.ico
Preview:	....6..... ..... .h...f...(... ...@..... .....d...d...d...d...d...d...d...d...d...d...d...d...d...d...d...d...w...w...w...w...w...w.....d...d...d...d...d...d...d...d...d...d...d...d...d...d...d...d...w...w...w...w...w...w...w...w.....P...P...P...P...P...P...P...P...T...d...d...d...d...d...d...d...w...w...w...w...w...w...w.....H...H...H...H...H...H...H...H...H...\...d...d...d...d...d...d...w...w...w...w...w...w...w.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\GetImage[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 203 x 249, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	4329

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\GetImage[1].png	
Entropy (8bit):	7.920359730272469
Encrypted:	false
SSDEEP:	96:KcU8PevXkPCqCV9JTrVsfbCSkcqr4OU3ACXypUbRCFi4F69uHZ0EQ:Kk89RmTCqqUOUQCXyWb8FrF6jp
MD5:	1673C9D4D3EB60DD03276F552418A3B0
SHA1:	AFD74FA09D70A5DEBD9CB50C3DC9289E0CC7C89B
SHA-256:	75EFED03580C8A249AF01B33DF7494C2D370D7C558C875B7FF08DF0FF040259F
SHA-512:	05D3B21631A43A3A5195B5BE12098582F3C728A375851B075C980212BCD4121C7D5966A3B8212098FB19D52783C9EDF365068B287A4D4CC9168B87FD824D1E3B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://onenote.officeapps.live.com/o/GetImage.ashx? &WOPIsrc=https%3A%2F%2Feagleeyeproduce%2Dmy%2Esharepoint%2Ecom%2Fpersonal%2Fmckrayp%5Feagleeyeproduce%5Fcom%2F%5Fvti%5Fbin%2Fwopi%2Eashx%2Ffiles%2Fbf301b8a577644f3ad8d5c8cee8ca044&access_token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6IkcydDJKYzlkMVZ6RkdjdzZUZy02YUhZVXk2VSJ9%2EeyJhdWQiOiJ3b3BpL2VhZ2xlZXllcHJvZHVjZS1teS5zaGFyZXBvaW50LmNvbUBkZTJhMzZlOS0xMGI2LTRjMmItYTA4OS1kMGU3MjY1ZTNmMDYiLCJpc3MiOiIwMDAwMDAwMy0wMDAwLTBmZjEtY2UwMC0wMDAwMDAwMDAwMDBAOTAxNDAxMjItODUxNi0xMWUxLThlZmYtNDkzMDQ5MjQwMTliIiwibmJmIjoiMTYwNTg4MzI0NiIsImV4cCI6IjE2MDU5MTkyNDYiLCJuYW1laWQiOiIwIy5mfG1lbWJlcnNoaXB8dXJuJTNhc3BvJTNhYW5vbiM2MzUyM2IzYTljOGFlOWQzYTZlZTUyM2YyNzJkZDk2MGE0ODRjNDU4ZDMwMGRkOWM5MDI1NTNjMTg0MjE1ZDU0IiwibmlpIjoibWljcm9zb2Z0LnNoYXJlcG9pbnQiLCJpc3VzZXIiOiJ0cnVlIiwiY2FjaGVrZXkiOiIwaC5mfG1lbWJlcnNoaXB8dXJuJTNhc3BvJTNhYW5vbiM2MzUyM2IzYTljOGFlOWQzYTZlZTUyM2YyNzJkZDk2MGE0ODRjNDU4ZDMwMGRkOWM5MDI1NTNjMTg0MjE1ZDU0IiwiY2hhcmluZ2lkIjoiR3k2VnltRlRzayTYTStEQ1M1UmRGZyIsImNpZCI6IjY4ODQ4ZjlmLTAwZmMtYjAwMC05NjE4LTJhYTJkODFlZTFkOSIsImlzbG9vcGJhY2siOiJUcnVlIiwiYXBwY3R4IjoiYmYzMDFiOGE1Nzc2NDRmM2FkOGQ1YzhjZWU4Y2EwNDQ7dlhqbUZlRWpsc2p4TTFaeTMxT2ZFvmlKQUUwPTtEZWZhdWx0O2U1ZTdiMDg5MWQ4OTRjODQ4ZGY4ZjUwYWQ1YjZkMDQ1OztUcnVlOzs7Njg7Njg4NDhmOWYtMDBmYy1iMDAwLTk2MTgtMmFhMmQ4MWVlMWQ5In0%2EMP44F7r0DLotHGXMvjLvnUznaQ3LiXc%5FSSP150hYNpnIFvAojFO1I8d1w7IMryRWbCLBxEdH31D%2DLjAzqNACOl9zFpNseCPyTraoZoxgQYRvgLjy1bxpuzAQ2oBo008CjuX62TWz2cD0d3%2Dh0Yx2lBujG4ZdDqhy4l4iOAGzfrGJyV9aveOzhPi6NXL9nqU7bBTfidWOpTvbfceQqkeEoaWaOLgTjIN56mq4L9cOQtL95aw19hZ4oksDPw%5FF53U4EWoik58eclfzg41y5IbxX5o7hAaVqNhzxYzqApeAqkjCpZHuK0y86FpJlug623yaz9KRQvco6xXJxhgyfxCWmA&access_token_ttl=1605919246590&ObjectDataBlobId=%7Bf5886e3f-3d4c-4db0-8270-908a4e929d46%7D%7B1%7D&usid=e36bd1de-4537-4044-9bf8-b13069c5af47&build=16.0.13510.41007&waccluster=PNL1&wdwacuseragent=MSWACONSync
Preview:	.PNG.....IHDR.....1.....sRGB.....gAMA.....a.....PLTE....!...,,,.....tp.d].....(((.....333.....CCC...$$$OOO.....kkk.....=5./%cccXXX.ga..... ..XR.....SL.....3*.JC.xs.....~....lg.....B:.KD.....www..'.....pHYs.....o.d....IDATx^.}W...[h...A....@]....r.o}...$S.*.....af.I..Z...Y.m..A.j.....".#.9\|.S.P,<iQ.X^.;...8.Cq ....=.l.?-+X...c.N.c.....L.ay..)!.ii..Y..`1).!M..Z...)2....X.....Gq/.d...J.....p.-J.v.? ..Z....._..f.A.i...v4p.\Tp+....._gL;..3.....8kn..n!.2]....<".....4.$*..8Kk.+.qt..fN.f.t...`yh.?V..... .v.&....33,).b.a..2....r.....b.!c.T..lc.-..OPo..XY.5.L.....4b...B."c..L.{.h. .m3]f..f.o.f...O.u,!E2...l...i.....3..h...;X./.udGl.zid.....MM.t.d.o!..1..o{M.Y@.D,..zo.....y-#.....d.E3.U..|..ge ..`.pT.e2..1w.Z...e.....Gg.....c..b.....f...e.6..f.EcN;..h...Lg.cO...Q.X.&t3...&K,,.)f2..0.`..`>^=.....r..}.g2..g..nF.g.....nF.n.9..e..e...0..2^.A@.d....-.E..i..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\OM9u8[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	5605
Entropy (8bit):	3.3836916804006383
Encrypted:	false
SSDEEP:	96:pafFagxo1n1lVJDc0HaqqxvP54WXhKRDm:pafFagxo1n1wJDR1UvP54ShKRDm
MD5:	3BB47566F1DB61E9D7C05BA9713CB6AB
SHA1:	098C1CE436BD93F74F4C300C0B793330B587110D
SHA-256:	5A9D4B74A3AC81087E1ED71BF83BE9ECE6CE033C96FEC633C0FDE8ABDAFDAB09
SHA-512:	85A1DD7F9675286CBDCE829A6288AAA06238220FF93CF150DBECDC5D67CB215F7465990300FCB28FA285223CEB71F8424EA0C20EBF7D436337632306286EAF0
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://sbccpro.com/OMMOM/OM9u8/
Preview:	<script type="text/javascript">.. HTML Encryption provided by www.webtoolhub.com -->.. ..document.write(unescape('%3c%21%44%4f%43%54%59%50%45%20%68 %74%6d%6c%3e%0d%0a%3c%68%74%6d%6c%20%6c%61%6e%67%3d%22%65%6e%22%3e%0d%0a%20%20%3c%68%65%61%64%3e%0d%0a%20%20%2 0%20%3c%21%2d%2d%20%52%65%71%75%69%72%65%64%20%6d%65%74%61%20%74%61%67%73%20%2d%2d%3e%0d%0a%20%20%20%20%3c%6d% 65%74%61%20%63%68%61%72%73%65%74%3d%22%75%74%66%2d%38%22%3e%0d%0a%20%20%20%20%3c%6d%65%74%61%20%68%74%74%70%2d %65%71%75%69%76%3d%22%63%6f%6e%74%65%6e%74%2d%74%79%70%65%22%20%63%6f%6e%74%65%6e%74%3d%22%74%65%78%74%2f%68%7 4%6d%6c%22%20%2f%3e%0d%0a%20%20%20%20%3c%6d%65%74%61%20%6e%61%6d%65%3d%22%76%69%65%77%70%6f%72%74%22%20%63%6f% 6e%74%65%6e%74%3d%22%77%69%64%74%68%3d%64%65%76%69%63%65%2d%77%69%64%74%68%2c%20%69%6e%69%74%69%61%6c%2d%73%63 %61%6c%65%3d%31%2c%20%73%68%72%69%6e%6b%2d%74%6f%2d%66%69%74%3d%6e%6f%22%3e%0d%0a%20%20%20%20%3c%74%69%74%6c%6 5%3e%4f%6e%65%20%44%72%69%76%65%3c%2f%74%69%74%6c%65%3e%0d%0a%09%0d%0a%20%20

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\Office365[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	downloaded
Size (bytes):	5495
Entropy (8bit):	4.462568215272766
Encrypted:	false
SSDEEP:	48:mvzmTKL2pUDGKcbDiHjzafvnMuaQtxPyatjEhLHMczSH2d4yUz6E1eeLYOOGpbTj:Sx0ED+fvnMYtxaat+LHXzSHPyU3LYebn
MD5:	E52D762B4E73E5F5924D5CC544B1E765
SHA1:	1248AC98038C71D032ED1AB2105BB133B6846B3D
SHA-256:	399C3592FBFF1A1C12B4C97DC1F6720E1A3316FF33FBFA069BD7CF0FFF40E606
SHA-512:	A01BCF9FF279AA7E9390AA1BDD07E0BC3817B1E901FE96F899E59EEA1A2192B705273CA9A4C8864035FDDFA4273D1E69489BC4B20219F8FD7092468147CC7EC 3
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\Office365[1].htm	
IE Cache URL:	http://https://sbccpro.com/OMMOM/OM9u8/Office365.php
Preview:	<!DOCTYPE html>.<html lang="en">. <head>. Required meta tags -->. <meta charset="utf-8">. <meta http-equiv="content-type" content="text/html" />. <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">. <title>One Drive</title>.. Font Awesome CSS -->. <link rel="stylesheet" type="text/css" href="https://maxcdn.bootstrapcdn.com/font-awesome/4.7.0/css/font-awesome.min.css">. Bootstrap CSS -->. <link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0-alpha.6/css/bootstrap.min.css" integrity="sha384-rwoIResjU2yc3z8GV/NPeZWAv56rSmLldC3R/AZzGRnGxQQKnKkoFVhFQhNUwEyJ" crossorigin="anonymous">. <link rel="stylesheet" type="text/css" href="css/style.css">..</head>.<body>.. . . . <img class="img-fluid ofc" src="images/officebg.jpg" alt="Office">. . <div class="col-md-4

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\OneNote.box4.dll1[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	2009024
Entropy (8bit):	5.663205116875028
Encrypted:	false
SSDEEP:	49152:A7oFwwjzakKR0G3Z5t33cOB8PYEoIUn2uQ629exjgrp:RPpU2uQ629etgrp
MD5:	3BEACFE9CB6EC64094CE999E3651B95A
SHA1:	6C3FBDC08421A52DFF79B5D0C31967CDC70CCDAD
SHA-256:	6772FDE6BF78C00D2C0D9851CE6F524EAAE70917C4F5F9ECB1FF3CA57A51635E
SHA-512:	0B7A18B4CD3F970BA9829E038562017C52AAEBD09B5DABB7DC6480B3D82CFF6057A6CEF22B92986C2C786CA692F536F54DCA72BB5B5AC9B32C821A12AA5FA313
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c1-onenote-15.cdn.office.net/o/s/161351041007_App_Scripts/OneNote.box4.dll1.js
Preview:	function wac_xpb(a,b,c,d){var e=wac_Qy(b.Bd());if(e){var f=wac_bG(b);if(f&&f.XH&&c){for(var f=f.Ec(),g=0;g<c.length;g++){var h=c[g];if(-1===Array.indexOf([wac_Rs,wac_Ts,wac_cu,wac_Eu,wac_qs,wac_Vt,wac_Ot,wac_VAa],h)){if(wac_Q().H(61)){if(h===wac_hs)continue;if(h===wac_9s){var k=wac_6Sa(b);if(k&&wac_$F(a.ei(),k)===wac_aG())continue}}wac_ze(f,h)}}d&&wac_Q().H(54)&&f.ja(wac_gya,!0);f.xqa()?a=wac_2u(e,f):(wac_4u(e,f,null),a=f);wac_8F(b,a.la())}}}.function wac_ypb(a,b,c){a.Tb||wac_TG(a,new wac_UG(a));c=new wac_SG(a,c.hA,c.pR,c.b1,c.Nn,c.Ke,c.te,c.Oo,c.yf,c.xPa,c.Ay,c.CM(),null);a.Tb.Fj(c,b);return c}function wac_zpb(a,b,c,d){a.ma()?b?b>a.ma()?wac_qF(a,a.ma()-1,32,1):wac_qF(a,b-1,32,1):wac_NF(a,b,32):wac_cH(a,c,d);a.yx.N(b,c.yx.H(d));a.EA.N(b,c.EA.H(d))}function wac_Apb(a,b){return 4===a.Og()&&1===a.MJ&&a.Om===b?!0:!1}.function wac_Bpb(a,b,c,d){if(!a.ss)return wac_b(23410763,368,15,"ContentControlChpHelper should not be null in IsDirectParentContentControlEditable"),!1;a=a.ss.VZd(b,c,d);retu

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\Onedrive-logo[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 170 x 114, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	4423
Entropy (8bit):	7.924731439527259
Encrypted:	false
SSDEEP:	96:hYNgH0x07J2QQZHs6JKaDsZV3ZN/C+5bGUR3vUcmt1B3:INQEHx5Dcbal1d
MD5:	FFC68AE7FD5A2D7A7CEC7185717B6E88
SHA1:	ABBCEBC2E0794C8F30DF0035881D4405D3A1D69B
SHA-256:	4603EA1B2F9DF0C9D4F2A253C550FFBAF27EA2CB53ECDE4277B2ACF9DDE33979
SHA-512:	F90CABBC9E1F2A1F8386C9C6C51729FC6678D35EAD9C0B7C02D50E5413BA88F5BE0B45327761B0C4617D8D2A2109EEF887A1F486F919BF554A6089AF8ED5C236
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://sbccpro.com/OMMOM/OM9u8/images/Onedrive-logo.png
Preview:	.PNG.....IHDR.....r.....PLTE.....+.....tRNS.....8.....=.UP0&..~!...hW+....J.u.....vkZ...dL?.....`[F.....C3.....mk["'.....pT.....|?!.....|m-.....WTPHB;94.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\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):	886979
Entropy (8bit):	5.43771151446558
Encrypted:	false
SSDEEP:	12288:rfG5BtLFTEBwfFlBcqnm1m47AGBqgDhnxgn8g:r8cIO73BqePg
MD5:	810BE58686D2168189347888FCE03D34
SHA1:	7FA6826132B6B6B2AD42E8DF65A661A96C8B1685
SHA-256:	EB147012F41965E3D8AE58FD5BC9DB6AAE031B38FBD1AC6F0527B9B15849D27E
SHA-512:	011748542458A1DB924E0A972420867CD3294C977217256FCEE57DDFA832061CCE1F54AE7E37BB3BDF27B162DC6CCF8FF00752F20F1D3DDA50D0CD8E5EC8E95

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\OreoSlice1[1].js	
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c1-onenote-15.cdn.office.net/o/s/161351041007_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\G62TDH9B\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:	7B389747818635BCA6FE76F5E3226EDA36AF53D8F27526796BC975EBD440A395
SHA-512:	A0104DBB40429BCA5F54061CE6D36A695283D883CE1B732CA87A30743234D29BEBA07A0100DE0DE0B274A70C8C7C289574F6343DF16C3E4C7B6453F60E8737B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c1-onenote-15.cdn.office.net/o/s/161351041007_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$....]<I.....#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.I.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\G62TDH9B\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:	31915EB859D432D714CAA2DFF74B7E760DFFE3A672CD872EB8CF07EDDC3B544578640C315CD47802B34F4BF06B31D290C9CBEAB228BC1FA64BDAF36DC5232 3A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c1-onenote-15.cdn.office.net/o/s/161351041007_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.$C...G....|'N...jk.f.....i..X0....X8....C....^;v..:..:.a.m....rz.x<..c..q..>..S...t.s....<...o..Cw.y.....<x...*....6e.....3..._..9H.f..}.._.....m.F.#.Wd...(.J.....|yB....|...+."O+.B.=..^.6- cK...|./.t..m .f._...F.E.oum\..>.7l..l.<.f..[.H.mZFiC...-._.#....[.d..{.....Z.~dd.....t.../`S.^.z.....-....Gm...n....m..2...#n!%..Ci.j..t....7..M.....8t.....^..h..d..]a.....K....L.....x6|6xM .s.M.../.]...=.....<4..l.....e.....>J1.....D.;w.|..fY...x.....m....W.+...9.Q>S.l..J.U.f0..._Z..Y....._s.O..!.2....u&..zo.z.-..>S..p..... .....x=u..2.M.jGb..G9.V.<;d."x@...@.....c.f.p... ...5....ZQ..8].<^.)c..f(.W....[...^.....gCW&.$i...I.&x.0.~8..!.x.t../>.c..:.(..cN..]XD..-...gk{.gCW9....<.'.l... ..v.....<.....).

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\fontawesome-webfont[1].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), FontAwesome family
Category:	downloaded
Size (bytes):	165742
Entropy (8bit):	6.705073372195656
Encrypted:	false
SSDEEP:	3072:qbhEnD+IzsU9z9QJ6/P3Xe2iEiEPGFCMW1JVJG6wVTDsk6BmG6S1yKshojskO+b2:qenD+IzsU9z9QJ6/PO2FiEP2C/DVJG6I
MD5:	674F50D287A8C48DC19BA404D20FE713
SHA1:	D980C2CE873DC43AF460D4D572D441304499F400
SHA-256:	7BFCAB6DB99D5CFBF1705CA0536DDC78585432CC5FA41BBD7AD0F009033B2979
SHA-512:	C160D3D77E67EFF986043461693B2A831E1175F579490D7F0B411005EA81BD4F5850FF534F6721B727C002973F3F9027EA960FAC4317D37DB1D4CB53EC9D343A
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\fontawesome-webfont[1].eot	
Reputation:	low
IE Cache URL:	http://https://maxcdn.bootstrapcdn.com/font-awesome/4.7.0/fonts/fontawesome-webfont.eot?
Preview:	n.....LP.....Yx.....F.o.n.t.A.w.e.s.o.m.e.....R.e.g.u.l.a.r...$.V.e.r.s.i.o.n. .4...7...0. .2.0.1.6.....F.o.n.t.A.w.e.s.o.m.e.....PFFTMk .G.....GDEF.....p... OS/2.2z@...X...`cmap..:.....gasp.....h....glyf...M.....L.head...-.....6hhea.....$hmtxEy.....loca...\.....maxp.,.....8... name....gh....post.....k.... u.....xY_.<.....3.2.....3.2.....'.....@.....i.....3.....3...s.....pyrs.@. ....p.....U..... .....]..... .....y...n.....2.....@..... ....z.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\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
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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\memnYaGs126MiZpBA-UFUKWiUNhrIqU[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 17452, version 1.1
Category:	downloaded
Size (bytes):	17452
Entropy (8bit):	7.960788191365059
Encrypted:	false
SSDEEP:	384:gVRT8VGShcBuPgTnSzgEuY86rgt710WmLonjMKsZMQAZ:s3ShcBuASzgEuYPNn0nDRQAZ
MD5:	BF72679CA22E53320BEAEA090E8BB07D
SHA1:	F3BAA33E986EC10D6F0C8211A826242441D52CC7
SHA-256:	1E742589D91A4B7E3888284A43A73675F312D3D6C4E78B3B76EBC36292646100
SHA-512:	F8FFC70E2E187EFBC785A52959BB26F605FEFB904D27B73EA4E1012DCC35569A78144751F761AA30D7B4AB0E5951B91322EA322BAF792C18E359C2ED79BBAF6E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/opensans/v18/memnYaGs126MiZpBA-UFUKWiUNhrIqU.woff
Preview:	wOFF.....D,.....eT.....GDEF.....GPOS.....GSUB.....X...t...OS/2.....]...`....cmap...`.....X..cvt .....b.....g.ifpgm...x.....s.ugasp.....glyf...(..3...NH7X..head..<....6...6..{.hhea..<T..."...$...ahmtx..<x...).....>/Sloca..>.....maxp..@l.. ... .x..name..@...../)C.post..A.....x.I..prep..C<..... x...5.A.....m."gW..`.L..&N".?.....IF....a.^...b1.....Uh."4...>..=x.c`f9.....u..1...<.f.....b.. 0t.vfPdP...M...C.G/S....|..K..6 ....t.....x.\.!..q.....#aff...#1Q@ .'U..@5.".llt.Aa#.f|c.W....'..X..!..C...ITPE.;..V.j.....0. .L0E...Yd.mN....:.....F....GG.g.s,x.>0....v..l;o..<.$G9.\f2...e{}.IS2..uc]p.....M.x.c.a.g.c..$KY...e@.,q.....x.....3... .....%..=.d.....#..6.e..L@6.3.e.....1._....#...x.TGw.F.....)..)7.W..`*.j.-...=*'_..sI...2...O>....[tt....TK]..|...G.....^.m..=..x.q...+./].p

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\memnYaGs126MiZpBA-UFUKWyV9hrIqU[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 17668, version 1.1
Category:	downloaded
Size (bytes):	17668
Entropy (8bit):	7.9576211916710635
Encrypted:	false
SSDEEP:	384:TQHZiJiLqdJVOpEbXHYV0cIeLg8hDHNbCqe+WQN:NWuV1X/eRHNbCqefQN
MD5:	793B1237017AEACD646FB80911425566
SHA1:	51E3023140BE407FD5FBFD27E0A5D2C30AE66F31
SHA-256:	5BB07410994C14D60F72CE3F6E19B172FCD7BC515F9BAEAF1F74C6CC2216E86A
SHA-512:	95C6644C1C1A2E369075D429E86736491451431C6046BA74545C0BF91C1CABEA1B1A4FCFD8FC5BB6A37269E4F80AF5B792BF80C968EC6A3B8B325F33EC66331
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\memnYaGs126MiZpBA-UFUKWyV9hrIqU[1].woff	
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/opensans/v18/memnYaGs126MiZpBA-UFUKWyV9hrIqU.woff
Preview:	wOFF.....E.....c.....GDEF.....GPOS.....GSUB.....X...t...OS/2.....]...`~...cmap...`.....X..cvt .....^.....M..fpgm...t.....~a..gasp.....#glyf... ..4...Lv$.#.head..<....6...6./{.hhea..=...."...$....hmtx..=4...@....}.K.loca..?t.....*maxp..A4... ... .name..AT.....*.D9post..BD.....x.I..prep..D.....$...J..... .....x...5.A.....m."gW..`..L..&N".?.....IF....a.^...b1.....Uh."4...>..=x.%..@@.@.....T.2..Q.1dB...!.j@..}(../y..]...V....b.b.D#5/....(..v.p...'e.7.....@@?.9.....x.\.!..q..... #aff...#1Q@.'U..@5.".llt.Aa#.f\|c.W....'..X..!..C...ITPE.;..V.j.....0. .L0E...Yd.mN....:....F....GG.g.s,x.>0....v..I;o..<.$G9.\f2...e{}.IS2..uc]p.....M.x.c.a.g.c.. .P...,..`....b`....C ..D@$P..)._.....a .p@.0.(.@.8. ..0....a8.....x.uTGw.F.....)..)7.W.$`*.....G.Kz.)e....t.|.1.7...s.g...3.7mgf..~{1...s.3.S...co..o.~.Zy.u...kW.\.t...N

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\memnYaGs126MiZpBA-UFUKXGUdhrIqU[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 17492, version 1.1
Category:	downloaded
Size (bytes):	17492
Entropy (8bit):	7.957749340429713
Encrypted:	false
SSDEEP:	384:bQHZhYs3a6PsVt9W9Z3owyC3bSZjyVO9Gz8W6EaJQgacXcK1cDVQgx:gq6PMK9Z3WCyc5z6lnXcYcxQU
MD5:	56E5756B696615D6164A625E1BCB1A9E
SHA1:	E2AEF56F577DBB78254066B73C2D0FBE30B40AE0
SHA-256:	BB87838929C15E1D0A05693C375323B95B6B4690FE207D3639E3A432C44AEF35
SHA-512:	BB998858AB9DF11375B0844EA008D31ABE4377826F6BE73C6F1DDE2E85C6F9A0404FADFDA9C081318F2F59614A22A1CF7F32376B25232887EDE8C7FBA323CB1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/opensans/v18/memnYaGs126MiZpBA-UFUKXGUdhrIqU.woff
Preview:	wOFF.....DT.....dD.....GDEF.....GPOS.....GSUB.....X...t...OS/2.....]...`.7.rcmap...`.....X..cvt .....^.....fpgm...t.....~a..gasp.....glyf.....4 ..M4.]2.head..<<...6...6..zghhea..<t..."...$.{.@hmtx..<....,.....V9Vloca..>.....rimaxp..@.... ... .name..@.....,.G.post..A.....x.I..prep..CT.....x..%..... ..x...5.A.....m."gW..`.L..&N".?.....IF....a.^...b1.....Uh."4...>..=x.c`f.....:....Q.B3_dHcb```.fgc.`abbi``P..x.....:.;302(...&.O.....)B..q>H.%.u..R``..<.....x.\.!..q.....#aff...# 1Q@.'U..@5.".llt.Aa#.f\|c.W....'..X..!..C...ITPE.;..V.j.....0. .L0E...Yd.mN....:.....F....GG.g.s,x.>0....v..I;o..<.$G9.\f2...e{}.IS2..uc]p.....M.x.c.a.g.c..$KY...e@.,A.".m....x.....3 .....[.o....=.d...u.a.....S....G..3.b..h...."...x.uTGw.F.....)..)7.W.$`*.....G.Kz.)e....t.|.1.7...s.g...3.7mgf..~{1...s.3.S...co..o.~.Zy.u...kW.\.t...N

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\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
SHA-256:	77DD1463FE34BE51528C6535C5AAF5590EE90BBD3B76AE8E362657C45E9F90FD
SHA-512:	2668E7EEFF653ECDEF04058FDC43328A80F297EE601839737F35A860737DAD438B03298C1A452E83DAED31DDDA540F7F065FE8F22FB05FC150A9FEAB08FFC91 D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c1-onenote-15.cdn.office.net/o/s/161351041007_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:98155F5CD83 911E1ACDEFDB8BE9BCEAA" 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\G62TDH9B\officebg[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 1420x1080, frames 3
Category:	downloaded
Size (bytes):	199781
Entropy (8bit):	7.986685505356506
Encrypted:	false
SSDEEP:	3072:GqroO3SvvO1a2DzHMuaXi8NHYpw97qefRS1XATbNr31uR+lGjcobBKTyl6XUV1:Uvv69Mlxpd5qXAThr31urDboT/q1
MD5:	058E25C4AA0FCCB6A280E543B4C108E8
SHA1:	05AF10D488E0651737E4AE510DF17DA2166463DA
SHA-256:	7A2C0B0E1E16041B12DD1A7D18438CEB14063C980799BAEE1D55CB2F04892777
SHA-512:	D98759E65DA318FD8092B5E03C9875FB782C7DBA4C01DD85FCACFA4E5747F2C105A96F04C9032F977554229D425CBBA9254692CB5AA4841F401BCC31A481FE7
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\officebg[1].jpg	
Reputation:	low
IE Cache URL:	http://https://sbccpro.com/OMMOM/OM9u8/images/officebg.jpg
Preview:	......JFIF.....C.....%!'&$!$#).;2),8,#$3F48=?BCB(1HMH@M;AB?...C.....?*$*???.....8...." .....X.>....:...p..:....Q...Q.....b.[...Q.@.9.8t...).T..a.....+....t...YC...;0+H.D...V.....7Q.....].P.....:.....;.....t9..FH.T. 93...qj-....*..''r..Wst.Pj.6.Q..J.....j0.c.....?@(S.....9.X.>jQ...}(...J_...../Dc.E.@.@9.8t+.Bxt..(...w...0.1@....(. a..(.....[..>..=..;....u..v>~._..''...+..t.Wc<L&.(J . .....V..L. ....:.....s..0.....`j..!'..?P...:..qX.....tf.L.5&...f.....&_T.O.jnf.K.S3..-I.7s..fp.dQ:.e..9.....(....8.....t.{.w..%F.F.A.FR..T.....@.....B..s.....z>~.N.....1....7P...0.8.HF... ..>.....N.w.t.....:0....Kf.....$..@O...j....4`H..D.K...rk'.F...'''*Pi.8._....N.....{Q.3...dEp.K]....H.k...f.V$n.s.t8..!q..@..?...|.....>..q...y>....@...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\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:	DE0553C5729844FEEE10383135403A6D0B6882BDEA6A1D77FB718BE858D5AB01079A787CC58BEFB8F972AC1C3363D8D97A3AC3A58E2029E72E28B91FEA2F08E A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c1-officeapps-15.cdn.office.net/o/s/161351041007_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{positi on: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-alig n: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\G62TDH9B\officebrowserfeedback_floodgate[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):	444805
Entropy (8bit):	5.561289105657843
Encrypted:	false
SSDEEP:	3072:ynvTCSaqJWTchUVRK6oxxJwgE+N3luPsOw7iyILysQOL4dafT58:0HcQh/6oKN+N3MPsv7iNLysQOL2
MD5:	3EE1E7921FA6FA81E2368CA82340F09F
SHA1:	5CE31569DB286CC2BC37273628DCCD2B779ADAD1
SHA-256:	CCBC51272BDDBED11AEFA47D08D4C90E354C050F91244799064E65D34E8AB184
SHA-512:	EFDE1EE619EC635CAA5853BEFF33E1004604C7C2A42E6A9C1C8EB3DC42B3962C02DDF2BC64BAF595ACC832E2D5747A4BE97A69A47E5B443C152B51EF5CD4C 142
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c1-officeapps-15.cdn.office.net/o/s/161351041007_App_Scripts/Feedback/latest/officebrowserfeedback_floodgate.js
Preview:	/*! For license information please see officebrowserfeedback_floodgate.min.js.LICENSE.txt */.!function(e){var t={};function A(n){if(t[n])return t[n].exports;var r=t[n]={i:n,l:!1,ex ports:{}};return e[n].call(r.exports,r,r.exports,A),r.l=!0,r.exports}A.m=e,A.c=t,A.d=function(e,t,n){A.o(e,t)||Object.defineProperty(e,t,{enumerable:!0,get:n})},A.r=function(e){"un defined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(e,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(e,"__esModule",{value:!0})},A.t= function(e,t){if(1&t&&(e=A(e)),8&t)return e;if(4&t&&"object"==typeof e&&e&&e.__esModule)return e;var n=Object.create(null);if(A.r(n),Object.defineProperty(n,"default",{en umerable:!0,value:e}),2&t&&"string"!=typeof e)for(var r in e)A.d(n,r,function(t){return e[t]}.bind(null,r));return n},A.n=function(e){var t=e&&e.__esModule?function(){return e.default}:function(){return e};return A.d(t,"a",t),t},A.o=function(e,t){return Object.prototype.hasOwnProperty.call(e,t)},A.p="",A(A.s=

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\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:	CE8DC9AB884DC9F18F0A2011B9BDDA7A80CE7239794B9918ADF2A681A1D148263486343AE8FE5017C612AE803F1F5ADDCD7238E8FD58FEA3F978D8EC64424A DD

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\officebrowserfeedbackstrings[1].js	
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c1-officeapps-15.cdn.office.net/o/s/161351041007_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\G62TDH9B\officelogo[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 163 x 75, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	1223
Entropy (8bit):	7.435397013783005
Encrypted:	false
SSDEEP:	24:gidVU+bg/fKMNezOpBlETR/CjB3EUlKd1i4hDHm+IH7AsbX:gidVU+M/CisOTlzjB3EUlK/iqmrH7R
MD5:	8DB2ADD18C0D34794B35DEEE1FDC14DB
SHA1:	6E72801F98A832E9193A4D9F4389AEAE1E5233DD
SHA-256:	EFACCC2B190FCCE0F0AB41064D882FB4A701C6AED6B1035595A16138E32A0A50
SHA-512:	FC0FEC864045DE68E355E61E3DDAFB103BA5E2ABCD5838ECCB80AEB55200F4659719A15CF25E1BCEC1F631B0F4F4319F18C662E526714E9EBBF56131CC7AEA05
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://sbccpro.com/OMMOM/OM9u8/images/officelogo.png
Preview:	.PNG.....IHDR.....K.....+..]....PLTE....<..<..<..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\progress[1].gif	
SHA-512:	F7984FFEAEC122EFCBE36218979BB4C35E27007CC091BA5A8829BA5088999A3F9F7A7D5E11D90A05904D58644EC0B4E5EE1D57C68DD5270B7F456A762D8D699A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c1-onenote-15.cdn.office.net/o/s/161351041007_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\G62TDH9B\tether.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):	24989
Entropy (8bit):	5.18502272346698
Encrypted:	false
SSDEEP:	768:1Jc67wdFbgDo6h+T7zMczQvoK/ww8l31g9CZQ5nAgM:zn74bsopz+AK/wM5Af
MD5:	ECDFD3DC464CEDA5F483BB5C96A6E3D2
SHA1:	CBDD0A2B2DD7A9CFC5DB3F33E34323AFA0CA55A3
SHA-256:	80BD626EB6D57112072A508EE4E5CE3C2FE5673FE0A5D029810033B24AAA5E9F
SHA-512:	1EC6758BDBE5A34D656DA7BE28897FFFA28FC6438EEB148F2363DE7EC6620BC2E6496F4A0D63182BD8E136A13D5EC6E31B2AE740067AB121EFB67475DAC24F8C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdnjs.cloudflare.com/ajax/libs/tether/1.4.0/js/tether.min.js
Preview:	!function(t,e){"function"==typeof define&&define.amd?define(e):"object"==typeof exports?module.exports=e(require,exports,module):t.Tether=e()}(this,function(t,e,o){"use strict";function i(t,e){if(!(t instanceof e))throw new TypeError("Cannot call a class as a function")}function n(t){var e=t.getBoundingClientRect(),o={};for(var i in e)o[i]=e[i];if(t.ownerDocument!==document){var r=t.ownerDocument.defaultView.frameElement;if(r){var s=n(r);o.top+=s.top,o.bottom+=s.top,o.left+=s.left,o.right+=s.left}}return o}function r(t){var e=getComputedStyle(t)||{},o=e.position,i=[];if("fixed"===o)return[t];for(var n=t;(n=n.parentNode)&&n&&1===n.nodeType;){var r=void 0;try{r=getComputedStyle(n)}catch(s){}if("undefined"==typeof r||null===r)return i.push(n),i;var a=r,f=a.overflow,l=a.overflowX,h=a.overflowY;/(auto|scroll)/.test(f+h+l)&&("absolute"!==o||["relative","absolute","fixed"].indexOf(r.position)>=0)&&i.push(n)}return i.push(t.ownerDocument.body),t.ownerDocument!==document&&i.push(t.ownerDocument

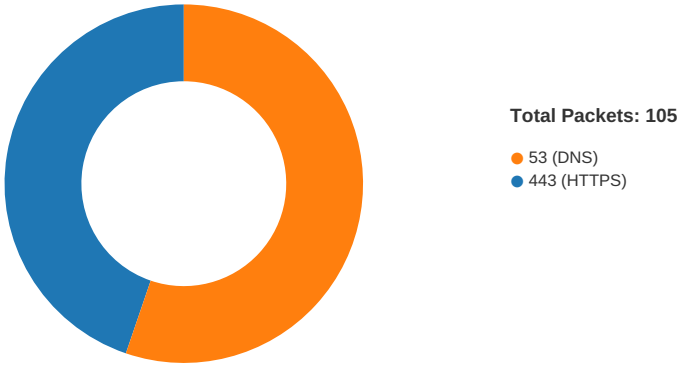
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\wachostwebpack[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	854392
Entropy (8bit):	5.414490877463858
Encrypted:	false
SSDEEP:	6144:PAcWhNsmTv4MFwkNredz2ty6NmfCKf1Xb40JszvMJ7KGWYlqAQx2uL:PAjCkNqdzaKfjF7qJL
MD5:	1F59813B3070F0ED0C9F52E9DBFE0F93
SHA1:	D5E4B4200D9BE58BD6D88B75B432D35DD7DFCAB7
SHA-256:	CC771E5A3668978A2E9757DAC7437F19D03E5782A2141C164BA1BC4F93D37FB6
SHA-512:	206700976B8973014BCF9936B5F80AE0D8B9FF4FCAC60174866A291031964DC928015FC623303FC3CDEDE7243C8F4A24D38170F12A06517A64761149BB958E1B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://spoprod-a.akamaihd.net/files/odsp-next-prod-webpack_2020-11-06-sts_20201106.001/wachostwebpack/wachostwebpack.js
Preview:	/*! For license information please see undefined.LICENSE.txt */.define("odsp-next/roots/WacHost",[],function(){return(function(e){function t(t){for(var r,o,u=t[0],a=t[1],f=t[2],l=0,h=[];l<u.length;l++){o=u[l];Object.prototype.hasOwnProperty.call(i,o)&&i[o]&&h.push(i[o][0]);i[o]=0}for(r in a)Object.prototype.hasOwnProperty.call(a,r)&&(e[r]=a[r]);c&&c(t);for(;h.length;)h.shift()();s.push.apply(s,f||[]);return n()}function n(){for(var e,t=0;t<s.length;t++){for(var n=s[t],r=!0,o=1;o<n.length;o++){var a=n[o];0!==i[a]&&(r=!1)}if(r){s.splice(t--,1);e=u(u.s=n[0])}}return e}var r={},i={wachostwebpack:0},s=[];function o(e,t){var n=u.p,r=(function(){var e=window.__backupBaseUrl;e&&(e="/"!==e.slice(-1)?e+"/":e)+"wachostwebpack/");return e})();t&&r&&(n=r);return n+(function(e){var t=window.__odsp_culture||window._spPageContextInfo&&window._spPageContextInfo.currentUICultureName;return t&&["plt.resx-plt","deferred.resx-deferred","ondemand.resx-ondemand"].indexOf(e)>=0&&t.toLowerCase()+"/"||""})(e)+

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 15:41:29.568725109 CET	49772	443	192.168.2.6	162.241.67.195
Nov 20, 2020 15:41:29.569010019 CET	49773	443	192.168.2.6	162.241.67.195
Nov 20, 2020 15:41:29.703614950 CET	443	49772	162.241.67.195	192.168.2.6
Nov 20, 2020 15:41:29.703811884 CET	49772	443	192.168.2.6	162.241.67.195
Nov 20, 2020 15:41:29.705156088 CET	443	49773	162.241.67.195	192.168.2.6
Nov 20, 2020 15:41:29.705313921 CET	49773	443	192.168.2.6	162.241.67.195
Nov 20, 2020 15:41:29.710836887 CET	49772	443	192.168.2.6	162.241.67.195
Nov 20, 2020 15:41:29.712738037 CET	49773	443	192.168.2.6	162.241.67.195
Nov 20, 2020 15:41:29.845576048 CET	443	49772	162.241.67.195	192.168.2.6
Nov 20, 2020 15:41:29.846158981 CET	443	49772	162.241.67.195	192.168.2.6
Nov 20, 2020 15:41:29.846180916 CET	443	49772	162.241.67.195	192.168.2.6
Nov 20, 2020 15:41:29.846194029 CET	443	49772	162.241.67.195	192.168.2.6
Nov 20, 2020 15:41:29.846201897 CET	443	49772	162.241.67.195	192.168.2.6
Nov 20, 2020 15:41:29.846273899 CET	49772	443	192.168.2.6	162.241.67.195
Nov 20, 2020 15:41:29.846297979 CET	49772	443	192.168.2.6	162.241.67.195
Nov 20, 2020 15:41:29.846976042 CET	443	49773	162.241.67.195	192.168.2.6
Nov 20, 2020 15:41:29.847384930 CET	443	49773	162.241.67.195	192.168.2.6
Nov 20, 2020 15:41:29.847418070 CET	443	49773	162.241.67.195	192.168.2.6
Nov 20, 2020 15:41:29.847439051 CET	443	49773	162.241.67.195	192.168.2.6
Nov 20, 2020 15:41:29.847450972 CET	443	49773	162.241.67.195	192.168.2.6
Nov 20, 2020 15:41:29.847465038 CET	49773	443	192.168.2.6	162.241.67.195
Nov 20, 2020 15:41:29.847496033 CET	49773	443	192.168.2.6	162.241.67.195
Nov 20, 2020 15:41:29.848064899 CET	443	49772	162.241.67.195	192.168.2.6
Nov 20, 2020 15:41:29.848144054 CET	49772	443	192.168.2.6	162.241.67.195
Nov 20, 2020 15:41:29.849347115 CET	443	49773	162.241.67.195	192.168.2.6
Nov 20, 2020 15:41:29.849447966 CET	49773	443	192.168.2.6	162.241.67.195
Nov 20, 2020 15:41:29.942920923 CET	49772	443	192.168.2.6	162.241.67.195
Nov 20, 2020 15:41:29.946738005 CET	49773	443	192.168.2.6	162.241.67.195
Nov 20, 2020 15:41:29.952424049 CET	49772	443	192.168.2.6	162.241.67.195
Nov 20, 2020 15:41:30.077788115 CET	443	49772	162.241.67.195	192.168.2.6
Nov 20, 2020 15:41:30.077888966 CET	49772	443	192.168.2.6	162.241.67.195
Nov 20, 2020 15:41:30.080981016 CET	443	49773	162.241.67.195	192.168.2.6
Nov 20, 2020 15:41:30.081047058 CET	49773	443	192.168.2.6	162.241.67.195
Nov 20, 2020 15:41:30.087371111 CET	443	49772	162.241.67.195	192.168.2.6
Nov 20, 2020 15:41:30.087498903 CET	49772	443	192.168.2.6	162.241.67.195
Nov 20, 2020 15:41:30.092305899 CET	49772	443	192.168.2.6	162.241.67.195
Nov 20, 2020 15:41:30.266483068 CET	443	49772	162.241.67.195	192.168.2.6
Nov 20, 2020 15:41:30.273780107 CET	443	49772	162.241.67.195	192.168.2.6
Nov 20, 2020 15:41:30.273838043 CET	443	49772	162.241.67.195	192.168.2.6
Nov 20, 2020 15:41:30.273885965 CET	443	49772	162.241.67.195	192.168.2.6
Nov 20, 2020 15:41:30.273931980 CET	443	49772	162.241.67.195	192.168.2.6
Nov 20, 2020 15:41:30.273964882 CET	49772	443	192.168.2.6	162.241.67.195

Copyright null 2020

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 15:41:30.273967028 CET	443	49772	162.241.67.195	192.168.2.6
Nov 20, 2020 15:41:30.273989916 CET	49772	443	192.168.2.6	162.241.67.195
Nov 20, 2020 15:41:30.273996115 CET	443	49772	162.241.67.195	192.168.2.6
Nov 20, 2020 15:41:30.274013042 CET	49772	443	192.168.2.6	162.241.67.195
Nov 20, 2020 15:41:30.274043083 CET	49772	443	192.168.2.6	162.241.67.195
Nov 20, 2020 15:41:30.278112888 CET	443	49772	162.241.67.195	192.168.2.6
Nov 20, 2020 15:41:30.278342009 CET	49772	443	192.168.2.6	162.241.67.195
Nov 20, 2020 15:41:30.433470011 CET	49772	443	192.168.2.6	162.241.67.195
Nov 20, 2020 15:41:30.434375048 CET	49773	443	192.168.2.6	162.241.67.195
Nov 20, 2020 15:41:30.436297894 CET	49774	443	192.168.2.6	162.241.67.195
Nov 20, 2020 15:41:30.567837000 CET	443	49772	162.241.67.195	192.168.2.6
Nov 20, 2020 15:41:30.568320036 CET	443	49773	162.241.67.195	192.168.2.6
Nov 20, 2020 15:41:30.568351984 CET	443	49773	162.241.67.195	192.168.2.6
Nov 20, 2020 15:41:30.568368912 CET	443	49773	162.241.67.195	192.168.2.6
Nov 20, 2020 15:41:30.568383932 CET	443	49773	162.241.67.195	192.168.2.6
Nov 20, 2020 15:41:30.568399906 CET	443	49773	162.241.67.195	192.168.2.6
Nov 20, 2020 15:41:30.568402052 CET	49773	443	192.168.2.6	162.241.67.195
Nov 20, 2020 15:41:30.568414927 CET	443	49773	162.241.67.195	192.168.2.6
Nov 20, 2020 15:41:30.568435907 CET	443	49773	162.241.67.195	192.168.2.6
Nov 20, 2020 15:41:30.568439960 CET	49773	443	192.168.2.6	162.241.67.195
Nov 20, 2020 15:41:30.568451881 CET	443	49773	162.241.67.195	192.168.2.6
Nov 20, 2020 15:41:30.568510056 CET	49773	443	192.168.2.6	162.241.67.195
Nov 20, 2020 15:41:30.568536043 CET	443	49772	162.241.67.195	192.168.2.6
Nov 20, 2020 15:41:30.568586111 CET	443	49772	162.241.67.195	192.168.2.6
Nov 20, 2020 15:41:30.568586111 CET	49772	443	192.168.2.6	162.241.67.195
Nov 20, 2020 15:41:30.568624020 CET	443	49772	162.241.67.195	192.168.2.6
Nov 20, 2020 15:41:30.568629026 CET	49772	443	192.168.2.6	162.241.67.195
Nov 20, 2020 15:41:30.568653107 CET	443	49772	162.241.67.195	192.168.2.6
Nov 20, 2020 15:41:30.568660975 CET	49772	443	192.168.2.6	162.241.67.195
Nov 20, 2020 15:41:30.568669081 CET	443	49772	162.241.67.195	192.168.2.6
Nov 20, 2020 15:41:30.568685055 CET	443	49772	162.241.67.195	192.168.2.6
Nov 20, 2020 15:41:30.568692923 CET	49772	443	192.168.2.6	162.241.67.195
Nov 20, 2020 15:41:30.568700075 CET	443	49772	162.241.67.195	192.168.2.6
Nov 20, 2020 15:41:30.568715096 CET	443	49772	162.241.67.195	192.168.2.6
Nov 20, 2020 15:41:30.568726063 CET	49772	443	192.168.2.6	162.241.67.195
Nov 20, 2020 15:41:30.568730116 CET	443	49772	162.241.67.195	192.168.2.6
Nov 20, 2020 15:41:30.568747997 CET	443	49772	162.241.67.195	192.168.2.6
Nov 20, 2020 15:41:30.568764925 CET	443	49772	162.241.67.195	192.168.2.6
Nov 20, 2020 15:41:30.568772078 CET	49772	443	192.168.2.6	162.241.67.195
Nov 20, 2020 15:41:30.568779945 CET	443	49772	162.241.67.195	192.168.2.6
Nov 20, 2020 15:41:30.568793058 CET	443	49772	162.241.67.195	192.168.2.6
Nov 20, 2020 15:41:30.568800926 CET	49772	443	192.168.2.6	162.241.67.195
Nov 20, 2020 15:41:30.568830967 CET	49772	443	192.168.2.6	162.241.67.195
Nov 20, 2020 15:41:30.569346905 CET	443	49772	162.241.67.195	192.168.2.6
Nov 20, 2020 15:41:30.569413900 CET	49772	443	192.168.2.6	162.241.67.195
Nov 20, 2020 15:41:30.570816040 CET	443	49774	162.241.67.195	192.168.2.6
Nov 20, 2020 15:41:30.570914030 CET	49774	443	192.168.2.6	162.241.67.195
Nov 20, 2020 15:41:30.572676897 CET	49773	443	192.168.2.6	162.241.67.195
Nov 20, 2020 15:41:30.573545933 CET	49774	443	192.168.2.6	162.241.67.195
Nov 20, 2020 15:41:30.625161886 CET	49777	443	192.168.2.6	162.241.67.195
Nov 20, 2020 15:41:30.626641035 CET	49778	443	192.168.2.6	162.241.67.195
Nov 20, 2020 15:41:30.632239103 CET	49779	443	192.168.2.6	162.241.67.195
Nov 20, 2020 15:41:30.703531981 CET	443	49772	162.241.67.195	192.168.2.6
Nov 20, 2020 15:41:30.703603029 CET	443	49772	162.241.67.195	192.168.2.6
Nov 20, 2020 15:41:30.703615904 CET	49772	443	192.168.2.6	162.241.67.195
Nov 20, 2020 15:41:30.703620911 CET	443	49772	162.241.67.195	192.168.2.6
Nov 20, 2020 15:41:30.703645945 CET	443	49772	162.241.67.195	192.168.2.6
Nov 20, 2020 15:41:30.703653097 CET	49772	443	192.168.2.6	162.241.67.195

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 15:40:37.688582897 CET	56023	53	192.168.2.6	8.8.8.8
Nov 20, 2020 15:40:37.715837002 CET	53	56023	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 15:40:39.716182947 CET	58384	53	192.168.2.6	8.8.8.8
Nov 20, 2020 15:40:39.743355989 CET	53	58384	8.8.8.8	192.168.2.6
Nov 20, 2020 15:40:40.711205006 CET	60261	53	192.168.2.6	8.8.8.8
Nov 20, 2020 15:40:40.738306046 CET	53	60261	8.8.8.8	192.168.2.6
Nov 20, 2020 15:40:41.428394079 CET	56061	53	192.168.2.6	8.8.8.8
Nov 20, 2020 15:40:41.459526062 CET	53	56061	8.8.8.8	192.168.2.6
Nov 20, 2020 15:40:42.024358988 CET	58336	53	192.168.2.6	8.8.8.8
Nov 20, 2020 15:40:42.063370943 CET	53	58336	8.8.8.8	192.168.2.6
Nov 20, 2020 15:40:42.743578911 CET	53781	53	192.168.2.6	8.8.8.8
Nov 20, 2020 15:40:42.770651102 CET	53	53781	8.8.8.8	192.168.2.6
Nov 20, 2020 15:40:43.229830980 CET	54064	53	192.168.2.6	8.8.8.8
Nov 20, 2020 15:40:43.342001915 CET	53	54064	8.8.8.8	192.168.2.6
Nov 20, 2020 15:40:44.775362968 CET	52811	53	192.168.2.6	8.8.8.8
Nov 20, 2020 15:40:44.824069977 CET	53	52811	8.8.8.8	192.168.2.6
Nov 20, 2020 15:40:44.914254904 CET	55299	53	192.168.2.6	8.8.8.8
Nov 20, 2020 15:40:44.951581001 CET	53	55299	8.8.8.8	192.168.2.6
Nov 20, 2020 15:40:45.641248941 CET	63745	53	192.168.2.6	8.8.8.8
Nov 20, 2020 15:40:45.687294006 CET	53	63745	8.8.8.8	192.168.2.6
Nov 20, 2020 15:40:46.015185118 CET	50055	53	192.168.2.6	8.8.8.8
Nov 20, 2020 15:40:46.050515890 CET	53	50055	8.8.8.8	192.168.2.6
Nov 20, 2020 15:40:46.587654114 CET	61374	53	192.168.2.6	8.8.8.8
Nov 20, 2020 15:40:46.614497900 CET	53	61374	8.8.8.8	192.168.2.6
Nov 20, 2020 15:40:47.535528898 CET	50339	53	192.168.2.6	8.8.8.8
Nov 20, 2020 15:40:47.573852062 CET	53	50339	8.8.8.8	192.168.2.6
Nov 20, 2020 15:40:49.185460091 CET	63307	53	192.168.2.6	8.8.8.8
Nov 20, 2020 15:40:49.309264898 CET	53	63307	8.8.8.8	192.168.2.6
Nov 20, 2020 15:40:53.724229097 CET	49694	53	192.168.2.6	8.8.8.8
Nov 20, 2020 15:40:53.772994995 CET	53	49694	8.8.8.8	192.168.2.6
Nov 20, 2020 15:40:53.932842970 CET	54982	53	192.168.2.6	8.8.8.8
Nov 20, 2020 15:40:53.977441072 CET	53	54982	8.8.8.8	192.168.2.6
Nov 20, 2020 15:40:54.287468910 CET	50010	53	192.168.2.6	8.8.8.8
Nov 20, 2020 15:40:54.324628115 CET	53	50010	8.8.8.8	192.168.2.6
Nov 20, 2020 15:40:54.709362984 CET	63718	53	192.168.2.6	8.8.8.8
Nov 20, 2020 15:40:54.736495972 CET	53	63718	8.8.8.8	192.168.2.6
Nov 20, 2020 15:40:55.568557024 CET	62116	53	192.168.2.6	8.8.8.8
Nov 20, 2020 15:40:55.595587969 CET	53	62116	8.8.8.8	192.168.2.6
Nov 20, 2020 15:41:01.127976894 CET	63816	53	192.168.2.6	8.8.8.8
Nov 20, 2020 15:41:01.155123949 CET	53	63816	8.8.8.8	192.168.2.6
Nov 20, 2020 15:41:02.243783951 CET	55014	53	192.168.2.6	8.8.8.8
Nov 20, 2020 15:41:02.289330959 CET	53	55014	8.8.8.8	192.168.2.6
Nov 20, 2020 15:41:03.721600056 CET	62208	53	192.168.2.6	8.8.8.8
Nov 20, 2020 15:41:03.726068020 CET	57574	53	192.168.2.6	8.8.8.8
Nov 20, 2020 15:41:03.758452892 CET	53	62208	8.8.8.8	192.168.2.6
Nov 20, 2020 15:41:03.761540890 CET	53	57574	8.8.8.8	192.168.2.6
Nov 20, 2020 15:41:03.878170967 CET	51818	53	192.168.2.6	8.8.8.8
Nov 20, 2020 15:41:03.915357113 CET	53	51818	8.8.8.8	192.168.2.6
Nov 20, 2020 15:41:05.086304903 CET	56628	53	192.168.2.6	8.8.8.8
Nov 20, 2020 15:41:05.123240948 CET	53	56628	8.8.8.8	192.168.2.6
Nov 20, 2020 15:41:05.243177891 CET	60778	53	192.168.2.6	8.8.8.8
Nov 20, 2020 15:41:05.270267963 CET	53	60778	8.8.8.8	192.168.2.6
Nov 20, 2020 15:41:06.441771030 CET	53799	53	192.168.2.6	8.8.8.8
Nov 20, 2020 15:41:06.468797922 CET	53	53799	8.8.8.8	192.168.2.6
Nov 20, 2020 15:41:07.314277887 CET	54683	53	192.168.2.6	8.8.8.8
Nov 20, 2020 15:41:07.341130972 CET	53	54683	8.8.8.8	192.168.2.6
Nov 20, 2020 15:41:07.484074116 CET	59329	53	192.168.2.6	8.8.8.8
Nov 20, 2020 15:41:07.511059046 CET	53	59329	8.8.8.8	192.168.2.6
Nov 20, 2020 15:41:08.134674072 CET	64021	53	192.168.2.6	8.8.8.8
Nov 20, 2020 15:41:08.161815882 CET	53	64021	8.8.8.8	192.168.2.6
Nov 20, 2020 15:41:08.805767059 CET	56129	53	192.168.2.6	8.8.8.8
Nov 20, 2020 15:41:08.832926989 CET	53	56129	8.8.8.8	192.168.2.6
Nov 20, 2020 15:41:10.674499989 CET	58177	53	192.168.2.6	8.8.8.8
Nov 20, 2020 15:41:10.701625109 CET	53	58177	8.8.8.8	192.168.2.6
Nov 20, 2020 15:41:12.017580032 CET	50700	53	192.168.2.6	8.8.8.8
Nov 20, 2020 15:41:12.044830084 CET	53	50700	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 15:41:12.637804031 CET	54069	53	192.168.2.6	8.8.8.8
Nov 20, 2020 15:41:12.673556089 CET	53	54069	8.8.8.8	192.168.2.6
Nov 20, 2020 15:41:12.801131964 CET	61178	53	192.168.2.6	8.8.8.8
Nov 20, 2020 15:41:12.828290939 CET	53	61178	8.8.8.8	192.168.2.6
Nov 20, 2020 15:41:13.030180931 CET	50700	53	192.168.2.6	8.8.8.8
Nov 20, 2020 15:41:13.057356119 CET	53	50700	8.8.8.8	192.168.2.6
Nov 20, 2020 15:41:13.805995941 CET	61178	53	192.168.2.6	8.8.8.8
Nov 20, 2020 15:41:13.841516972 CET	53	61178	8.8.8.8	192.168.2.6
Nov 20, 2020 15:41:14.025134087 CET	50700	53	192.168.2.6	8.8.8.8
Nov 20, 2020 15:41:14.052205086 CET	53	50700	8.8.8.8	192.168.2.6
Nov 20, 2020 15:41:14.740499020 CET	57017	53	192.168.2.6	8.8.8.8
Nov 20, 2020 15:41:14.767612934 CET	53	57017	8.8.8.8	192.168.2.6
Nov 20, 2020 15:41:14.815766096 CET	61178	53	192.168.2.6	8.8.8.8
Nov 20, 2020 15:41:14.842837095 CET	53	61178	8.8.8.8	192.168.2.6
Nov 20, 2020 15:41:16.031301975 CET	50700	53	192.168.2.6	8.8.8.8
Nov 20, 2020 15:41:16.058422089 CET	53	50700	8.8.8.8	192.168.2.6
Nov 20, 2020 15:41:16.817890882 CET	61178	53	192.168.2.6	8.8.8.8
Nov 20, 2020 15:41:16.845141888 CET	53	61178	8.8.8.8	192.168.2.6
Nov 20, 2020 15:41:20.040663958 CET	50700	53	192.168.2.6	8.8.8.8
Nov 20, 2020 15:41:20.067794085 CET	53	50700	8.8.8.8	192.168.2.6
Nov 20, 2020 15:41:21.070298910 CET	61178	53	192.168.2.6	8.8.8.8
Nov 20, 2020 15:41:21.097362041 CET	53	61178	8.8.8.8	192.168.2.6
Nov 20, 2020 15:41:28.516356945 CET	56327	53	192.168.2.6	8.8.8.8
Nov 20, 2020 15:41:28.576951981 CET	53	56327	8.8.8.8	192.168.2.6
Nov 20, 2020 15:41:29.519328117 CET	50243	53	192.168.2.6	8.8.8.8
Nov 20, 2020 15:41:29.558644056 CET	53	50243	8.8.8.8	192.168.2.6
Nov 20, 2020 15:41:30.466197014 CET	62055	53	192.168.2.6	8.8.8.8
Nov 20, 2020 15:41:30.493236065 CET	53	62055	8.8.8.8	192.168.2.6
Nov 20, 2020 15:41:30.581669092 CET	61249	53	192.168.2.6	8.8.8.8
Nov 20, 2020 15:41:30.627670050 CET	53	61249	8.8.8.8	192.168.2.6
Nov 20, 2020 15:41:30.734797955 CET	65252	53	192.168.2.6	8.8.8.8
Nov 20, 2020 15:41:30.801850080 CET	53	65252	8.8.8.8	192.168.2.6
Nov 20, 2020 15:41:31.129020929 CET	64367	53	192.168.2.6	8.8.8.8
Nov 20, 2020 15:41:31.156045914 CET	53	64367	8.8.8.8	192.168.2.6
Nov 20, 2020 15:41:31.999767065 CET	55066	53	192.168.2.6	8.8.8.8
Nov 20, 2020 15:41:32.035321951 CET	53	55066	8.8.8.8	192.168.2.6
Nov 20, 2020 15:41:35.593060017 CET	60211	53	192.168.2.6	8.8.8.8
Nov 20, 2020 15:41:35.620100021 CET	53	60211	8.8.8.8	192.168.2.6
Nov 20, 2020 15:41:42.299295902 CET	56570	53	192.168.2.6	8.8.8.8
Nov 20, 2020 15:41:42.336368084 CET	53	56570	8.8.8.8	192.168.2.6
Nov 20, 2020 15:41:47.043011904 CET	58454	53	192.168.2.6	8.8.8.8
Nov 20, 2020 15:41:47.126301050 CET	53	58454	8.8.8.8	192.168.2.6
Nov 20, 2020 15:41:59.158113003 CET	55180	53	192.168.2.6	8.8.8.8
Nov 20, 2020 15:41:59.185129881 CET	53	55180	8.8.8.8	192.168.2.6
Nov 20, 2020 15:42:00.166172028 CET	55180	53	192.168.2.6	8.8.8.8
Nov 20, 2020 15:42:00.193248987 CET	53	55180	8.8.8.8	192.168.2.6
Nov 20, 2020 15:42:01.179106951 CET	55180	53	192.168.2.6	8.8.8.8
Nov 20, 2020 15:42:01.206204891 CET	53	55180	8.8.8.8	192.168.2.6
Nov 20, 2020 15:42:03.193852901 CET	55180	53	192.168.2.6	8.8.8.8
Nov 20, 2020 15:42:03.229495049 CET	53	55180	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 20, 2020 15:40:43.229830980 CET	192.168.2.6	8.8.8.8	0xdad0	Standard query (0)	eagleeyeproduce-my.sharepoint.com	A (IP address)	IN (0x0001)
Nov 20, 2020 15:40:44.914254904 CET	192.168.2.6	8.8.8.8	0x2496	Standard query (0)	spoprod-a.akamaihd.net	A (IP address)	IN (0x0001)
Nov 20, 2020 15:40:47.535528898 CET	192.168.2.6	8.8.8.8	0x3480	Standard query (0)	onenoteonlinesync.onenote.com	A (IP address)	IN (0x0001)
Nov 20, 2020 15:40:53.724229097 CET	192.168.2.6	8.8.8.8	0x44cc	Standard query (0)	messaging.office.com	A (IP address)	IN (0x0001)
Nov 20, 2020 15:40:54.287468910 CET	192.168.2.6	8.8.8.8	0xea43	Standard query (0)	site-cdn.onenote.net	A (IP address)	IN (0x0001)

Copyright null 2020

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 20, 2020 15:41:02.243783951 CET	192.168.2.6	8.8.8.8	0x869	Standard query (0)	www.onenote.com	A (IP address)	IN (0x0001)
Nov 20, 2020 15:41:03.721600056 CET	192.168.2.6	8.8.8.8	0x232d	Standard query (0)	cdn.onenote.net	A (IP address)	IN (0x0001)
Nov 20, 2020 15:41:03.726068020 CET	192.168.2.6	8.8.8.8	0x8cdc	Standard query (0)	ajax.aspnetcdn.com	A (IP address)	IN (0x0001)
Nov 20, 2020 15:41:29.519328117 CET	192.168.2.6	8.8.8.8	0xf3ca	Standard query (0)	sbccpro.com	A (IP address)	IN (0x0001)
Nov 20, 2020 15:41:30.466197014 CET	192.168.2.6	8.8.8.8	0xd54c	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)
Nov 20, 2020 15:41:31.129020929 CET	192.168.2.6	8.8.8.8	0xadd2	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
Nov 20, 2020 15:41:31.999767065 CET	192.168.2.6	8.8.8.8	0xbdab	Standard query (0)	sbccpro.com	A (IP address)	IN (0x0001)
Nov 20, 2020 15:41:35.593060017 CET	192.168.2.6	8.8.8.8	0x409e	Standard query (0)	maxcdn.bootstrapcdn.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 20, 2020 15:40:43.342001915 CET	8.8.8.8	192.168.2.6	0xdad0	No error (0)	eagleeyeproduce-my.sharepoint.com	eagleeyeproduce.sharepoint.com		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 15:40:43.342001915 CET	8.8.8.8	192.168.2.6	0xdad0	No error (0)	eagleeyeproduce.sharepoint.com	1566-ipv4e.clump.prod.aa-rt.sharepoint.com		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 15:40:43.342001915 CET	8.8.8.8	192.168.2.6	0xdad0	No error (0)	1566-ipv4e.clump.prod.aa-rt.sharepoint.com	20536-ipv4e.farm.prod.aa-rt.sharepoint.com		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 15:40:43.342001915 CET	8.8.8.8	192.168.2.6	0xdad0	No error (0)	20536-ipv4e.farm.prod.aa-rt.sharepoint.com	20536-ipv4e.farm.prod.sharepointonline.com.akadns.net		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 15:40:44.951581001 CET	8.8.8.8	192.168.2.6	0x2496	No error (0)	spoprod-a.akamaihd.net	spoprod-a.akamaihd.net.edgesuite.net		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 15:40:47.573852062 CET	8.8.8.8	192.168.2.6	0x3480	No error (0)	onenoteonlinesync.onenote.com	prod.onenoteonlinesync-onenote.com.akadns.net		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 15:40:53.772994995 CET	8.8.8.8	192.168.2.6	0x44cc	No error (0)	messaging.office.com	omexmessaging.osi.office.net		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 15:40:54.324628115 CET	8.8.8.8	192.168.2.6	0xea43	No error (0)	site-cdn.onenote.net	site-cdn.onenote.net.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 15:41:02.289330959 CET	8.8.8.8	192.168.2.6	0x869	No error (0)	www.onenote.com	prod.reverseproxy-onenote.com.akadns.net		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 15:41:03.758452892 CET	8.8.8.8	192.168.2.6	0x232d	No error (0)	cdn.onenote.net	cdn.onenote.net.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 15:41:03.761540890 CET	8.8.8.8	192.168.2.6	0x8cdc	No error (0)	ajax.aspnetcdn.com	mscomajax.vo.msecnd.net		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 15:41:29.558644056 CET	8.8.8.8	192.168.2.6	0xf3ca	No error (0)	sbccpro.com		162.241.67.195	A (IP address)	IN (0x0001)
Nov 20, 2020 15:41:30.493236065 CET	8.8.8.8	192.168.2.6	0xd54c	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 15:41:31.156045914 CET	8.8.8.8	192.168.2.6	0xadd2	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Nov 20, 2020 15:41:31.156045914 CET	8.8.8.8	192.168.2.6	0xadd2	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Nov 20, 2020 15:41:32.035321951 CET	8.8.8.8	192.168.2.6	0xbdab	No error (0)	sbccpro.com		162.241.67.195	A (IP address)	IN (0x0001)
Nov 20, 2020 15:41:35.620100021 CET	8.8.8.8	192.168.2.6	0x409e	No error (0)	maxcdn.bootstrapcdn.com	cds.j3z9t3p6.hwcdn.net		CNAME (Canonical name)	IN (0x0001)

HTTPS Packets

Copyright null 2020

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Nov 20, 2020 15:41:29.848064899 CET	162.241.67.195	443	192.168.2.6	49772	CN=sbccpro.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	Thu Nov 19 01:00:00 CET 2020 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Thu Feb 18 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 20, 2020 15:41:29.849347115 CET	162.241.67.195	443	192.168.2.6	49773	CN=sbccpro.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	Thu Nov 19 01:00:00 CET 2020 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Thu Feb 18 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 20, 2020 15:41:31.210840940 CET	104.16.19.94	443	192.168.2.6	49789	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Oct 21 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Thu Oct 21 01:59:59 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Nov 20, 2020 15:41:31.211463928 CET	104.16.19.94	443	192.168.2.6	49788	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Oct 21 02:00:00 CEST 2020	Thu Oct 21 01:59:59 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Nov 20, 2020 15:41:32.352943897 CET	162.241.67.195	443	192.168.2.6	49790	CN=sbccpro.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	Thu Nov 19 01:00:00 CET 2020	Thu Feb 18 00:59:59 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	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		
							Mon May 18 02:00:00 CEST 2015	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2025	Mon Jan 01 00:59:59 CET 2029

Code Manipulations

Statistics

Behavior

- iexplore.exe
- iexplore.exe
- dllhost.exe
- explorer.exe
- iexplore.exe

Copyright null 2020

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 6716 Parent PID: 792

General

Start time:	15:40:41
Start date:	20/11/2020
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff721e20000
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: 6764 Parent PID: 6716

General

Start time:	15:40:41
Start date:	20/11/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6716 CREDAT:17410 /prefetch:2
Imagebase:	0xc80000
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: 5212 Parent PID: 792

General

Start time:	15:41:04
Start date:	20/11/2020
Path:	C:\Windows\System32\dllhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\DllHost.exe /Processid:{49F171DD-B51A-40D3-9A6C-52D674CC729D}
Imagebase:	0x7ff716560000
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: 3440 Parent PID: 5212

General

Start time:	15:41:06
Start date:	20/11/2020
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff6f22f0000
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: 5912 Parent PID: 6716

General

Start time:	15:41:28
Start date:	20/11/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6716 CREDAT:17432 /prefetch:2
Imagebase:	0xc80000
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

Disassembly

Code Analysis

Copyright null 2020