ID: 358573
Sample Name: 2021-02-18 Fivoor - Overleg - Kwartaaloverleg.docx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 21:39:51
Date: 25/02/2021
Version: 31.0.0 Emerald

Table of Contents

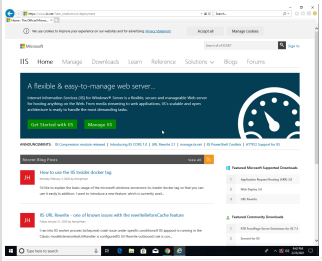
Analysis Report 2021-02-18 Fivoor - Overleg - Kwartaalo…

Overview

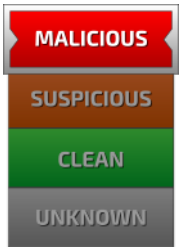
General Information

Sample Name:	2021-02-18 Fivoor - Overleg - Kwartaaloverleg.docx
Analysis ID:	358573
MD5:	14b364f395dd53f..
SHA1:	0b97138df21f05c..
SHA256:	1f39fb321c3902a..
Infos:	

Most interesting Screenshot:



Detection

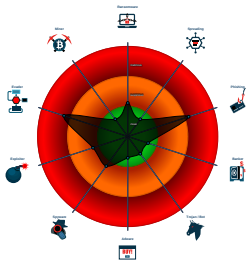


Score:	52
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Contains an external reference to an…
- Phishing site detected (based on log…
- Allocates a big amount of memory (p…
- IP address seen in connection with o…
- JA3 SSL client fingerprint seen in co…
- Monitors certain registry keys / valu…
- Queries the volume information (nam…
- Tries to load missing DLLs

Classification



Startup

- **System is w10x64**
- WINWORD.EXE (PID: 6368 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE' /Automation -Embedding MD5: 0B9AB9B9C4DE429473D6450D4297A123)
  - MSOSYNC.EXE (PID: 6552 cmdline: C:\Program Files (x86)\Microsoft Office\Office16\MsoSync.exe MD5: EA19F4A0D18162BE3A0C8DAD249ADE8C)
  - MSOSYNC.EXE (PID: 6568 cmdline: C:\Program Files (x86)\Microsoft Office\Office16\MsoSync.exe MD5: EA19F4A0D18162BE3A0C8DAD249ADE8C)
- iexplore.exe (PID: 6732 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6816 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6732 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

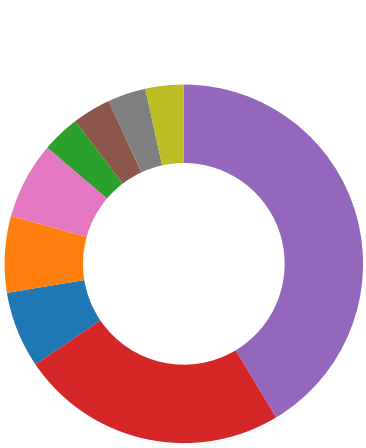
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

Phishing:

Phishing site detected (based on logo template match)

Compliance:

Uses new MSVCR Dlls

Uses secure TLS version for HTTPS connections

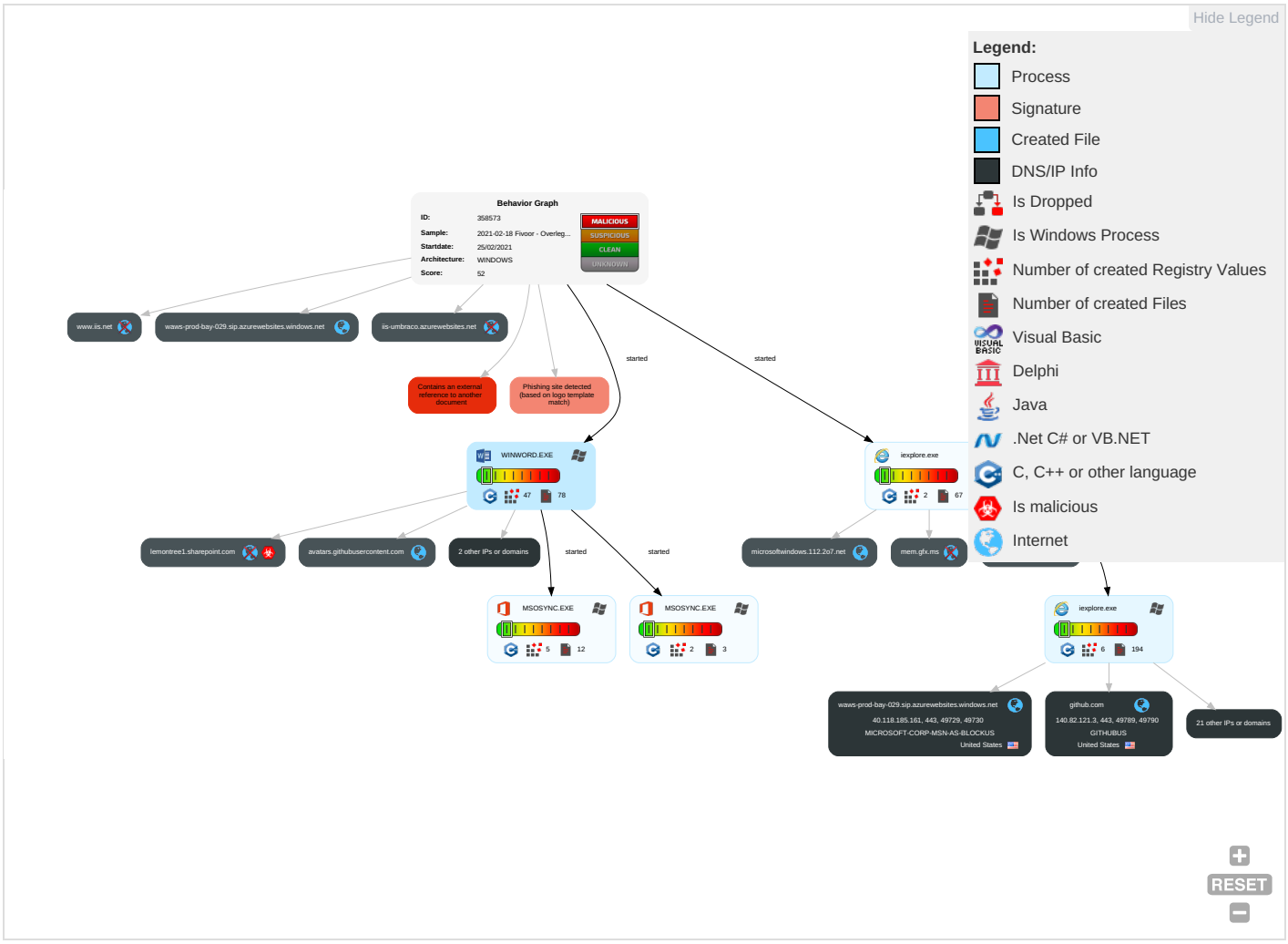
Persistence and Installation Behavior:

Contains an external reference to another document

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
Valid Accounts	Windows Management Instrumentation	DLL Side-Loading 1	Process Injection 1	Masquerading 1	OS Credential Dumping	Query Registry 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
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Process Injection 1	LSASS Memory	Security Software 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
Domain Accounts	At (Linux)	Logon Script (Windows)	Extra Window Memory Injection 1	DLL Side-Loading 1	Security Account Manager	File and Directory Discovery 2	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
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Extra Window Memory Injection 1	NTDS	System Information Discovery 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	

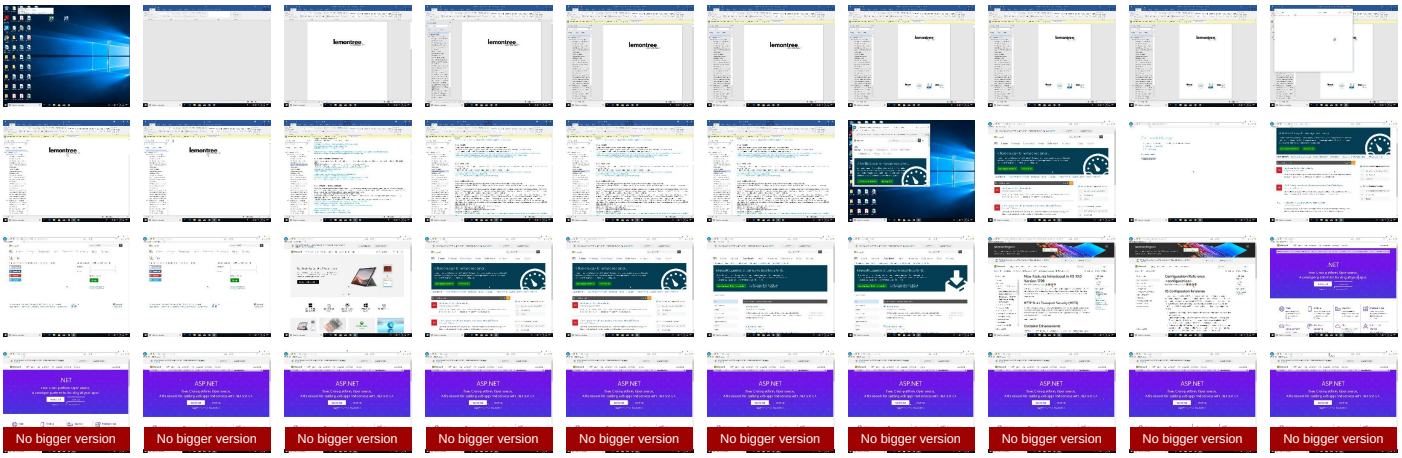
Behavior Graph

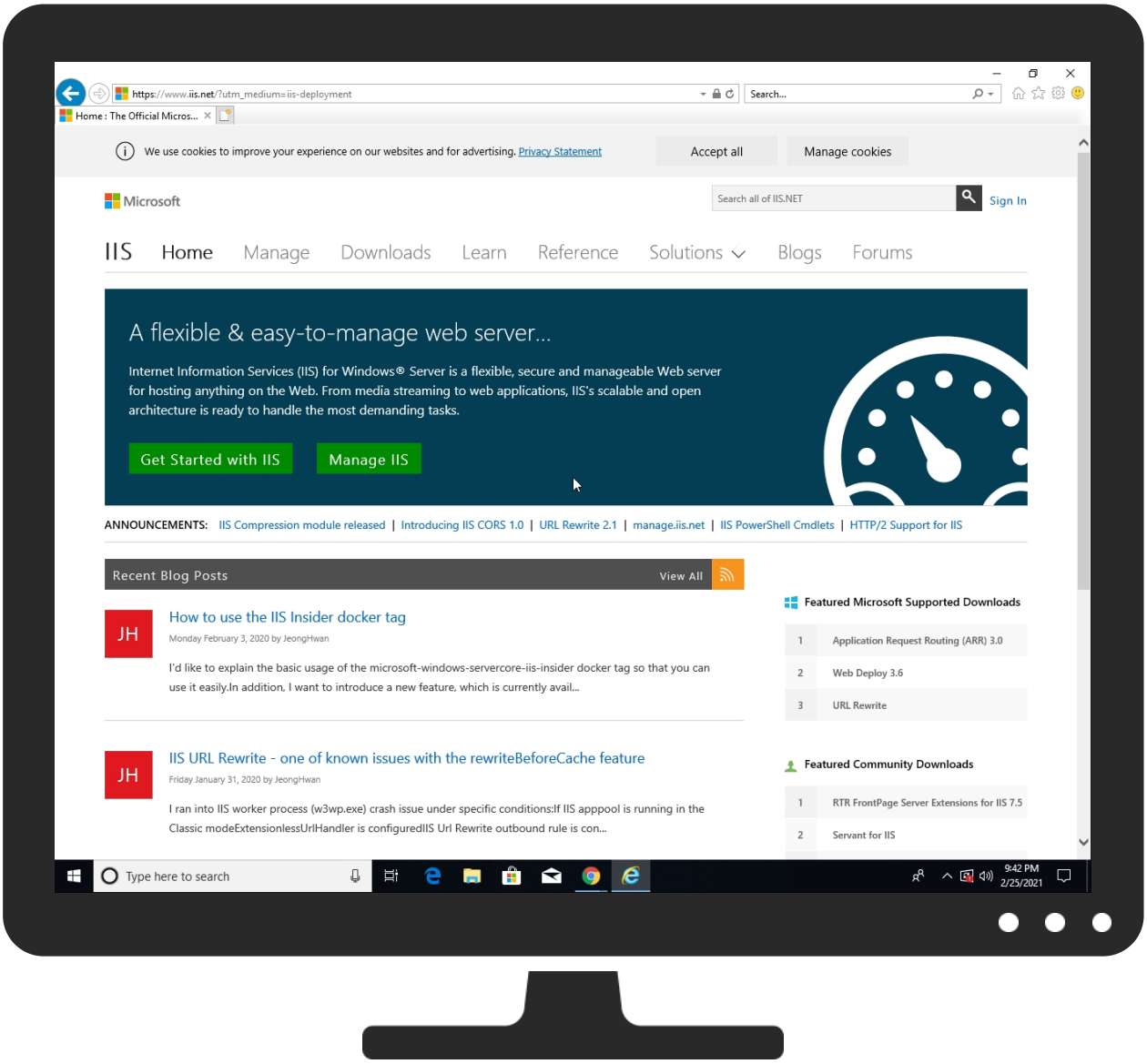


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://assets.onestore.ms	0%	URL Reputation	safe	
http://https://assets.onestore.ms	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://assets.onestore.ms	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://sn.webrootcloudav.com/oudav.com/	0%	Avira URL Cloud	safe	
http://https://skyversion.webrootcloudav.com	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	Avira URL Cloud	safe	
http://https://www.microsoftstore.com.cn/checkout	0%	URL Reputation	safe	
http://https://www.microsoftstore.com.cn/checkout	0%	URL Reputation	safe	
http://https://www.microsoftstore.com.cn/checkout	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://www.microsoftstore.com.cn/cart	0%	URL Reputation	safe	
http://https://www.microsoftstore.com.cn/cart	0%	URL Reputation	safe	
http://https://www.microsoftstore.com.cn/cart	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.microsoftstore.com.cn/software/microsoft-365	0%	Avira URL Cloud	safe	
http://fontello.comIcon	0%	URL Reputation	safe	
http://fontello.comIcon	0%	URL Reputation	safe	
http://fontello.comIcon	0%	URL Reputation	safe	
http://gambit.ph	0%	Avira URL Cloud	safe	
http://https://dotnet.microso	0%	Avira URL Cloud	safe	
http://https://g59.p4.webrootcloudav.com	0%	Avira URL Cloud	safe	
http://https://www.microsoft.	0%	URL Reputation	safe	
http://https://www.microsoft.	0%	URL Reputation	safe	
http://https://www.microsoft.	0%	URL Reputation	safe	
http://https://www.microsoftstore.com.cn/microsoft-365/microsoft-365	0%	Avira URL Cloud	safe	
http://https://www.clarity.ms/tag/	0%	Avira URL Cloud	safe	
http://https://sn.webrootcloudav.com/	0%	Avira URL Cloud	safe	
http://https://www.microsoftstore.com.cn/hardware/surface	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
sni1gl.wpc.gammacdn.net	152.199.21.175	true	false		unknown
avatars.githubusercontent.com	185.199.108.133	true	false		unknown
microsoftwindows.112.2o7.net	15.237.136.106	true	false		high
github.com	140.82.121.3	true	false		high
asp.net	40.118.185.161	true	false		high
cs1227.wpc.alphacdn.net	192.229.221.185	true	false		unknown
liveperson.map.fastly.net	151.101.1.192	true	false		unknown
waws-prod-bay-029.sip.azurewebsites.windows.net	40.118.185.161	true	false		high
sn.webrootcloudav.com	34.253.10.100	true	false		unknown
logincdn.msauth.net	unknown	unknown	false		unknown
www.asp.net	unknown	unknown	false		high
login.iis.net	unknown	unknown	false		high
assets.onestore.ms	unknown	unknown	false		unknown

Name	IP	Active	Malicious	Antivirus Detection	Reputation
lemontree1.sharepoint.com	unknown	unknown	true		unknown
mem.gfx.ms	unknown	unknown	false		unknown
www.iis.net	unknown	unknown	false		high
publisher.liveperson.net	unknown	unknown	false		high
dc.services.visualstudio.com	unknown	unknown	false		high
consentdeliveryfd.azurefd.net	unknown	unknown	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://www.iis.net/?utm_medium=iis-deployment	false		high
http://https://login.iis.net/account/login?ReturnUrl=https://www.iis.net/	false		high

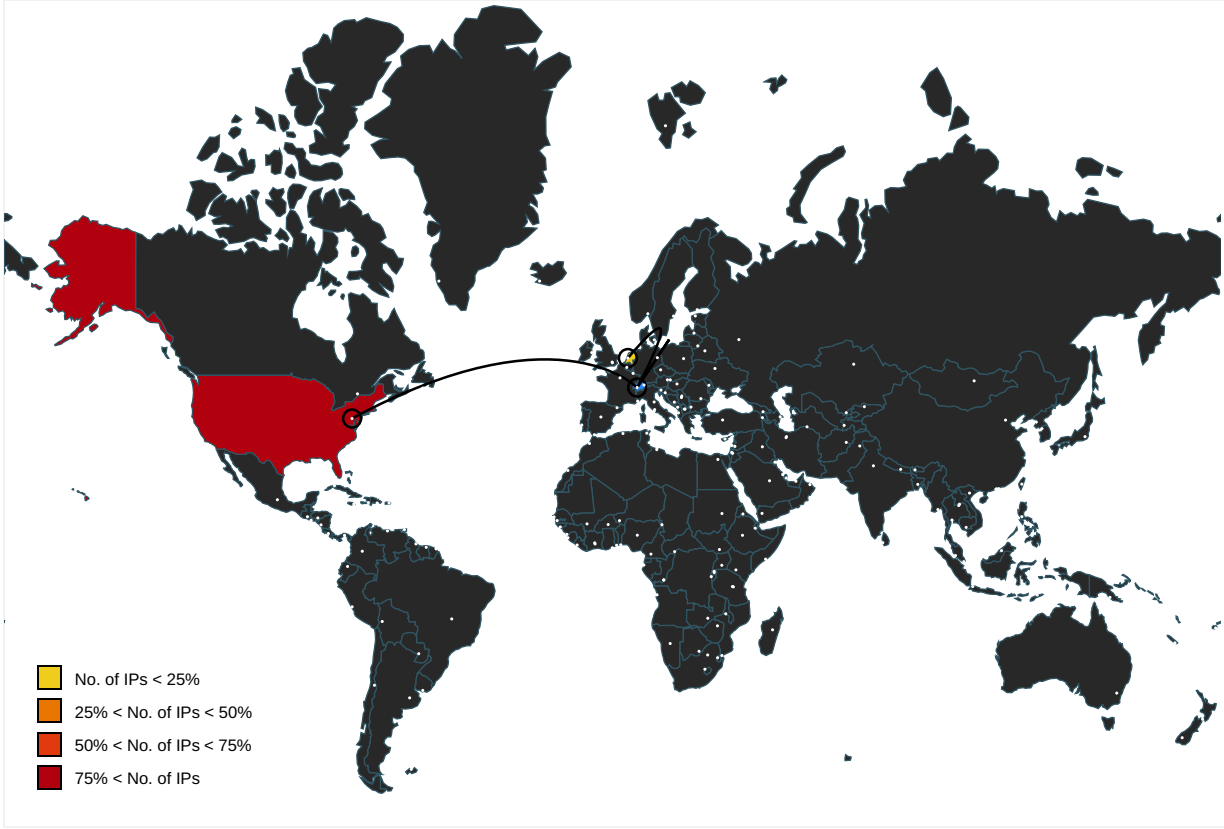
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://outlook.live.com/owa/	de-ch[1].htm.13.dr	false		high
http://https://shell.suite.office.com:1443	C35D0C9B-162A-4BE1-BAF9-F09B9C11FBF9.0.dr	false		high
http://https://www.iis.net/?utm_medium=iis-deploymentLHome	~DF3D8F722CCD3B64D6.TMP.12.dr	false		high
http://https://www.iis.net/downloadsus/IIS-Administration/	~DF3D8F722CCD3B64D6.TMP.12.dr	false		high
http://https://autodiscover-s.outlook.com/	C35D0C9B-162A-4BE1-BAF9-F09B9C11FBF9.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	C35D0C9B-162A-4BE1-BAF9-F09B9C11FBF9.0.dr	false		high
http://https://cdn.entity.	C35D0C9B-162A-4BE1-BAF9-F09B9C11FBF9.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://products.office.com/de-ch/academic/compare-office-365-education-plans	de-ch[1].htm.13.dr	false		high
http://https://assets.onestore.ms	de-ch[1].htm.13.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://github.com/MicrosoftDocs/IIS.Administration-docs/blob/live/IIS-Administration/index.md	IIS-Administration[1].htm.13.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	C35D0C9B-162A-4BE1-BAF9-F09B9C11FBF9.0.dr	false		high
http://https://login.iis.net/favicon.ico	imagestore.dat.13.dr	false		high
http://https://tools.ietf.org/html/rfc6797	new-features-introduced-in-iis-10-1709[1].htm.13.dr	false		high
http://https://rpsticket.partnerservices.getmicrosoftkey.com	C35D0C9B-162A-4BE1-BAF9-F09B9C11FBF9.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	C35D0C9B-162A-4BE1-BAF9-F09B9C11FBF9.0.dr	false		high
http://https://github.com/MicrosoftDocs/iis-docs/blob/live/iis/configuration/index.md	configuration[1].htm.13.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	C35D0C9B-162A-4BE1-BAF9-F09B9C11FBF9.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	C35D0C9B-162A-4BE1-BAF9-F09B9C11FBF9.0.dr	false		high
http://https://api.aadrm.com/	C35D0C9B-162A-4BE1-BAF9-F09B9C11FBF9.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://forums.asp.net/	aspnet[1].htm.13.dr	false		high
http://https://forums.iis.net/members/saucecontrol.aspx	downloads[1].htm.13.dr	false		high
http://https://www.twitter.com/inetsrv/	downloads[1].htm.13.dr	false		high
http://https://github.com/twbs/bootstrap/graphs/contributors)	general.min[1].js.13.dr	false		high
http://https://sn.webrootcloudav.com/oudav.com/	~DF3D8F722CCD3B64D6.TMP.12.dr	false	• Avira URL Cloud: safe	unknown
http://https://github.com/nschonni.png?size=32	new-features-introduced-in-iis-10-1709[1].htm.13.dr	false		high
http://https://blogs.iis.net/iisteam/introducing-iis-cors-1-0	6RJ6ZB23.htm.13.dr	false		high
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	C35D0C9B-162A-4BE1-BAF9-F09B9C11FBF9.0.dr	false		high
http://https://api.microsoftstream.com/api/	C35D0C9B-162A-4BE1-BAF9-F09B9C11FBF9.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	C35D0C9B-162A-4BE1-BAF9-F09B9C11FBF9.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://cr.office.com	C35D0C9B-162A-4BE1-BAF9-F09B9C11FBF9.0.dr	false		high
http://https://publisher.liveperson.net/iframe-le-tag/iframe.html?lpsite=60270350&lpsection=store-sales-de-	~DF3D8F722CCD3B64D6.TMP.12.dr	false		high
http://https://stats.g.doubleclick.net/j/collect	analytics[1].js.13.dr	false		high
http://https://www.iis.net/favicon.ico	imagestore.dat.13.dr	false		high
http://https://skyversion.webrootcloudav.com	~WRS{31CB24EF-1DEB-4C38-BB46-32AB8B1362AD}.tmp.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://manage.iis.net	IIS-Administration[1].htm.13.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	C35D0C9B-162A-4BE1-BAF9-F09B9C11FBF9.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	C35D0C9B-162A-4BE1-BAF9-F09B9C11FBF9.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	C35D0C9B-162A-4BE1-BAF9-F09B9C11FBF9.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.microsoftstore.com.cn/checkout	iframe[1].htm.13.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://store.office.cn/addinstemplate	C35D0C9B-162A-4BE1-BAF9-F09B9C11FBF9.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://wus2-000.pagecontentsync.	C35D0C9B-162A-4BE1-BAF9-F09B9C11FBF9.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.microsoftstore.com.cn/cart	iframe[1].htm.13.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://forums.iis.net/members/$	downloads[1].htm.13.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	C35D0C9B-162A-4BE1-BAF9-F09B9C11FBF9.0.dr	false		high
http://https://www.odwebp.svc.ms	C35D0C9B-162A-4BE1-BAF9-F09B9C11FBF9.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.microsoftstore.com.cn/software/microsoft-365	iframe[1].htm.13.dr	false	• Avira URL Cloud: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	C35D0C9B-162A-4BE1-BAF9-F09B9C11FBF9.0.dr	false		high
http://https://web.microsoftstream.com/video/	C35D0C9B-162A-4BE1-BAF9-F09B9C11FBF9.0.dr	false		high
http://fontello.comIcon	docons.225ca470[1].eot.13.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net	C35D0C9B-162A-4BE1-BAF9-F09B9C11FBF9.0.dr	false		high
http://https://github.com/shirhatti	IIS-Administration[1].htm.13.dr	false		high
http://github.com/jquery/jquery-tmpl	downloadshome[1].js.13.dr	false		high
http://https://www.surveymonkey.com/r/netcoresupport_dotnetwebsite	BOWGV9MI.htm.13.dr	false		high
http://https://blogs.iis.net/	downloads[1].htm.13.dr, 6RJ6ZB23.htm.13.dr	false		high
http://https://lpcdn.lpsnmedia.net/le_unified_window/9.12.0.19-release_4769/resources/loader_on_warmGray5_7	iframe[1].htm.13.dr	false		high
http://https://jquery.com/	general.min[1].js.13.dr	false		high
http://gambit.ph	main.min[1].js.13.dr	false	• Avira URL Cloud: safe	unknown
http://https://dotnet.microso	{3A9550E0-77F5-11EB-90E4-ECF4BB862DED}.dat.12.dr	false	• Avira URL Cloud: safe	unknown
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	C35D0C9B-162A-4BE1-BAF9-F09B9C11FBF9.0.dr	false		high
http://https://g59.p4.webrootcloudav.com	~WRS{31CB24EF-1DEB-4C38-BB46-32AB8B1362AD}.tmp.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://github.com/MicrosoftDocs/iis-docs/blob/live/iis/get-started/whats-new-in-iis-10-version-1709	new-features-introduced-in-iis-10-1709[1].htm.13.dr	false		high
http://https://www.microsoft.	{3A9550E0-77F5-11EB-90E4-ECF4BB862DED}.dat.12.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://github.com/js-cookie/js-cookie	main.min[1].js.13.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	C35D0C9B-162A-4BE1-BAF9-F09B9C11FBF9.0.dr	false		high
http://github.com/aFarkas/lazysizes	de-ch[1].htm.13.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://weather.service.msn.com/data.aspx	C35D0C9B-162A-4BE1-BAF9-F09B9C11FBF9.0.dr	false		high
http://https://github.com/Rich-Lang.png?size=32	new-features-introduced-in-iis-10-1709[1].htm.13.dr	false		high
http://https://sizzlejs.com/	general.min[1].js.13.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	C35D0C9B-162A-4BE1-BAF9-F09B9C11FBF9.0.dr	false		high
http://https://www.iis.net/configreference	downloads[1].htm.13.dr, login[1].htm.13.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	C35D0C9B-162A-4BE1-BAF9-F09B9C11FBF9.0.dr	false		high
http://https://www.microsoftstore.com.cn/microsoft-365/microsoft-365	iframe[1].htm.13.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.iis.net/downloads	~DF3D8F722CCD3B64D6.TMP.12.dr, login[1].htm.13.dr	false		high
http://https://www.iis.net/?utm_medium=iis-deployment#hero	~DF3D8F722CCD3B64D6.TMP.12.dr	false		high
http://schema.org/BreadcrumbList	configuration[1].htm.13.dr	false		high
http://https://blogs.iis.net/adminapi	6RJ6ZB23.htm.13.dr	false		high
http://https://github.com/MicrosoftDocs/iis-docs/blob/22f8c6108ea9ed9330333ede82568276a3162b34/iis/configur	configuration[1].htm.13.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	C35D0C9B-162A-4BE1-BAF9-F09B9C11FBF9.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	C35D0C9B-162A-4BE1-BAF9-F09B9C11FBF9.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	C35D0C9B-162A-4BE1-BAF9-F09B9C11FBF9.0.dr	false		high
http://https://www.skype.com/de/	de-ch[1].htm.13.dr	false		high
http://https://clients.config.office.net/user/v1.0/android/policies	C35D0C9B-162A-4BE1-BAF9-F09B9C11FBF9.0.dr	false		high
http://https://entitlement.diagnostics.office.com	C35D0C9B-162A-4BE1-BAF9-F09B9C11FBF9.0.dr	false		high
http://https://www.clarity.ms/tag/	aspnet[1].htm.13.dr	false	• Avira URL Cloud: safe	unknown
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	C35D0C9B-162A-4BE1-BAF9-F09B9C11FBF9.0.dr	false		high
http://https://outlook.office.com/	C35D0C9B-162A-4BE1-BAF9-F09B9C11FBF9.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	C35D0C9B-162A-4BE1-BAF9-F09B9C11FBF9.0.dr	false		high
http://https://sn.webrootcloudav.com/	~DF3D8F722CCD3B64D6.TMP.12.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.iis.net/com/de-ch/n?ReturnUrl=https://www.iis.net/	~DF3D8F722CCD3B64D6.TMP.12.dr	false		high
http://https://github.com/	8c3bc838.index-docs[1].js.13.dr	false		high
http://https://www.iis.net	login[1].htm.13.dr	false		high
http://https://www.microsoftstore.com.cn/hardware/surface	iframe[1].htm.13.dr	false	• Avira URL Cloud: safe	unknown
http://https://blogs.iis.net/iisteam/url-rewrite-v2-1	6RJ6ZB23.htm.13.dr	false		high
http://https://forums.iis.net/1080.aspx	downloads[1].htm.13.dr	false		high
http://https://www.iis.net/?utm_medium=iis-deployment#herojH	~DF3D8F722CCD3B64D6.TMP.12.dr	false		high
http://https://graph.windows.net/	C35D0C9B-162A-4BE1-BAF9-F09B9C11FBF9.0.dr	false		high
http://https://devnull.onenote.com	C35D0C9B-162A-4BE1-BAF9-F09B9C11FBF9.0.dr	false		high
http://https://messaging.office.com/	C35D0C9B-162A-4BE1-BAF9-F09B9C11FBF9.0.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
40.118.185.161	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
151.101.1.192	unknown	United States		54113	FASTLYUS	false
140.82.121.3	unknown	United States		36459	GITHUBUS	false
34.253.10.100	unknown	United States		16509	AMAZON-02US	false
192.229.221.185	unknown	United States		15133	EDGECASTUS	false
185.199.108.133	unknown	Netherlands		54113	FASTLYUS	false
152.199.21.175	unknown	United States		15133	EDGECASTUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	358573
Start date:	25.02.2021
Start time:	21:39:51
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 3s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	2021-02-18 Fivoor - Overleg - Kwartaaloverleg.docx
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Potential for more IOCs and behavior
Number of analysed new started processes analysed:	36
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0

Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal52.phis.evad.winDOCX@8/188@16/7
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .docx • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Browse link: https://sn.webrootcloudav.com/ • Scroll down • Close Viewer • Browsing link: https://go.microsoft.com/fwlink/?LinkId=521839 • Browsing link: https://www.iis.net/?utm_medium=iis-deployment#hero • Browsing link: https://login.iis.net/login/signin.aspx?ReturnUrl=https://www.iis.net/ • Browsing link: https://www.microsoft.com/ • Browsing link: https://www.iis.net/ • Browsing link: https://docs.microsoft.com/en-us/IIS-Administration/ • Browsing link: https://www.iis.net/downloads • Browsing link: https://www.iis.net/learn • Browsing link: https://www.iis.net/configreference • Browsing link: https://www.microsoft.com/net • Browsing link: https://www.asp.net/
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, ielowutil.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.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): 51.104.139.180, 40.88.32.150, 13.64.90.137, 168.61.161.212, 23.54.113.53, 52.109.32.63, 52.109.88.37, 52.109.88.39, 13.107.136.9, 52.109.8.22, 52.109.12.24, 52.109.8.24, 52.109.88.38, 52.109.76.36, 52.255.188.83, 104.43.139.144, 184.30.20.56, 88.221.62.148, 152.199.19.161, 13.107.253.19, 8.248.145.254, 8.238.36.254, 8.241.126.249, 8.248.91.254, 8.238.27.126, 20.54.26.129, 51.104.144.132, 92.122.213.247, 92.122.213.194, 23.54.112.217, 13.107.246.19, 13.107.213.19, 65.55.44.109, 84.53.167.109, 2.20.209.184, 152.199.19.160, 184.30.21.171, 40.126.31.8, 40.126.31.139, 40.126.31.4, 40.126.31.137, 40.126.31.141, 40.126.31.143, 20.190.159.138, 20.190.159.134, 23.50.102.187, 92.122.213.219, 92.122.213.200, 142.250.185.238, 51.107.59.180, 52.155.217.156 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, assets.onestore.ms.edgekey.net, e13678.dscb.akamaiedge.net, www.tm.lg.prod.aadmsa.akadns.net, publisher.livepersonk.akadns.net, fs-wildcard.microsoft.com.edgekey.net, www.tm.a.prd.aadg.trafficmanager.net, e11290.dspg.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, www.microsoft.com-c-3.edgekey.net, star-azurefd-prod.trafficmanager.net, login.live.com, audownload.windowsupdate.nsatc.net, officeclient.microsoft.com, watson.telemetry.microsoft.com, au-bg-shim.trafficmanager.net, a1778.g2.akamai.net, www.google-analytics.com, e10583.dspg.akamaiedge.net, fs.microsoft.com, www-iis.azureedge.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, lgincdnvzeuno.ec.azureedge.net, skypedataprdcolcus17.cloudapp.net, swn-breeziest-in.cloudapp.net, skypedataprdcolcus16.cloudapp.net, statics-marketingsites-wcus-ms-com.akamaized.net, assets.onestore.ms.akadns.net, web.vortex.data.trafficmanager.net, c-

s.cms.ms.akadns.net, az416426.vo.msecnd.net, ris.api.iris.microsoft.com, e55.dspb.akamaiedge.net, store-images.s-microsoft.com, lgincdn.trafficmanager.net, t-0009.t-msedge.net, cdn.account.microsoft.com.akadns.net, blobcollector.events.data.trafficmanager.net, t-0009.fb-t-msedge.net, c.s-microsoft.com-c.edgekey.net, dotnet.microsoft.com, dub2.next.a.prd.aadg.trafficmanager.net, europe.configsvc1.live.com.akadns.net, spo-0004.spo-msedge.net, cs9.wpc.v0cdn.net, www-iis.ec.azureedge.net, prod-w.nexus.live.com.akadns.net, docs.microsoft.com-c.edgekey.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, www.microsoft.com-c-3.edgekey.net.globalredir.akadns.net, iecvlist.microsoft.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, go.microsoft.com, dual.t-0009.t-msedge.net, nexus.officeapps.live.com, displaycatalog.mp.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, docs.microsoft.com-c.edgekey.net.globalredir.akadns.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, www-google-analytics.l.google.com, ie9comview.vo.msecnd.net, cs22.wpc.v0cdn.net, prod.configsvc1.live.com.akadns.net, 187105-ipv4.farm.dprodmgd104.aa-rt.sharepoint.com.spo-0004.spo-msedge.net, mem.gfx.ms.edgekey.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, 187105-ipv4e.farm.dprodmgd104.sharepointonline.com.akadns.net, login-iis.azureedge.net, e13630.dscb.akamaiedge.net, login.msa.msidentity.com, web.vortex.data.microsoft.com, lgincdnvzeuno.azureedge.net, login-iis.ec.azureedge.net, skypedataprdcoleus17.cloudapp.net, c.s-microsoft.com, config.officeapps.live.com, go.microsoft.com.edgekey.net, dc.trafficmanager.net, dc.applicationinsights.microsoft.com, e13678.dscg.akamaiedge.net, az725175.vo.msecnd.net, www.microsoft.com, displaycatalog-rp.md.mp.microsoft.com.akadns.net, wcpstatic.microsoft.com, docs.microsoft.com

- Report size exceeded maximum capacity and may have missing behavior information.
- 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 NtQueryAttributesFile calls found.
- Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
40.118.185.161	http://www.servos.it/gr/guiide/aruba/	Get hash	malicious	Browse	• www.iis.net/default.aspx?tabid=2&subtabid=25&i=969&p=1
	http%3a%2f%2fwww.ctmsds.com%2fuploads%2fallimg%2f160128%2f1-16012PT31N47.png%c2%a0	Get hash	malicious	Browse	• www.iis.net/default.aspx?tabid=2&subtabid=25&i=969&p=1
140.82.121.3	Funded.jar	Get hash	malicious	Browse	
	Covid19_Vacine_Investment_Proposals_1st_Quarter2021 pdf.jar	Get hash	malicious	Browse	
	Covid19_Vacine_Investment_Proposals_1st_Quarter2021 pdf.jar	Get hash	malicious	Browse	
	Unterlagen PDF.exe	Get hash	malicious	Browse	
	f1a14e6352036833f1c109e1bb2934f2.exe	Get hash	malicious	Browse	
	d88e07467ddcf9e3b19fa972b9f000d1.exe	Get hash	malicious	Browse	
	password.doc	Get hash	malicious	Browse	
	Pastebin.docm	Get hash	malicious	Browse	
	index_2021-02-18-00_38.exe	Get hash	malicious	Browse	
	executable.908.exe	Get hash	malicious	Browse	
	executable.908.exe	Get hash	malicious	Browse	
	MT0128.jar	Get hash	malicious	Browse	
	executable.908.exe	Get hash	malicious	Browse	
	executable.908.exe	Get hash	malicious	Browse	
	executable.908.exe	Get hash	malicious	Browse	
	executable.908.exe	Get hash	malicious	Browse	
	executable.908.exe	Get hash	malicious	Browse	
	executable.908.exe	Get hash	malicious	Browse	
	executable.908.exe	Get hash	malicious	Browse	
	PO 20191003.exe	Get hash	malicious	Browse	
151.101.1.192	Farie PO.doc	Get hash	malicious	Browse	
	Cerere de pret NUM003112 09-02-2021.doc	Get hash	malicious	Browse	
	Notice_Admin_Johnstoncompanies_8578.htm	Get hash	malicious	Browse	
	http://https://donkoontzdds-my.sharepoint.com:443/:o:/p/paula/EpkEAfrMo1VPgFsywG5EnMwBbr42_dHD8h4N6RCWcat9eA?e=5%3a3JiMMt&at=9	Get hash	malicious	Browse	
	http://https://omoolowo001.github.io/myfirstrepo/YWNjb3VudHNfbG9nindex.html?scriptID=35662936635352205&cookies=MC4xOTUyNjY0OTg0MzM0NTQ0NQ&token=81117470799998&email=jeaton@nlcmutual.com	Get hash	malicious	Browse	
	http://https://kingkorefitness.com/Inc-Corp/RD-FITT	Get hash	malicious	Browse	
	http://https://kingkorefitness.com/Inc-Corp/RD-FITT	Get hash	malicious	Browse	
	http://https://rzh09.github.io/kirapzoxda/adiuew.html?bbre=as83wsdcx	Get hash	malicious	Browse	
	http://https://linkprotect.cudasvc.com/url?a=https%3a%2f%2fseacoccs.github.io%2fvivapdeltoozx%2fsorirw.html%3fbbre%3dod948reids&c=E,1,vSy_DaxVlhDKTU_DAd4XDQRKFbpEz58IBL3G2ibxtXxy4isfCn6tn5y2D7KvyG8o1RL3a--vpSQ8W1tCBVf3nGFmVP0O8Zl4kUultyRSb1120A,,&typo=1	Get hash	malicious	Browse	
	http://https://app.box.com/s/o2w7bicj17iez9hkgk744e23wl6qiw9m	Get hash	malicious	Browse	
	http://https://judithjamm.github.io/vaopstarndupx/ifus.html?bbre=dsi8243er	Get hash	malicious	Browse	
	http://https://joeboeboe.com/wertghfg/sdfgrhtjytf/	Get hash	malicious	Browse	
	http://https://criswellauto-my.sharepoint.com/:b:/p/jtan/EU06P7jwOKFJoP-tIPrljMMBEG3gKDGg6TlM9-QtbrOOKg?e=N4aC2p	Get hash	malicious	Browse	
	http://https://sanfetaappdevmaozi-noisy-cassowary-es.mybluemix.net/roietri/ipz.php?bbre=gfh565rtdf&d=DwMFAw	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://ewretrytukhjghfgdfsf.azurewebsites.net/5gqxbb/suuyF/tryhfdg.php?bbre=1b077f6510087ea39a88e7c61636c339	Get hash	malicious	Browse	
	http://https://www.canva.com/design/DAEPFQpVQOg/UPJfT3H38FpnoN0B2vprRA/view?utm_content=DAEPFQpVQOg&utm_campaign=designshare&utm_medium=link&utm_source=sharebutton	Get hash	malicious	Browse	
	2tsY1gtYQe.exe	Get hash	malicious	Browse	
	http://https://34.75.2o2.lol/XYWNc0aW9uPWwNsaWNrJngVybD1ovndHRwnczovL3NleY3wVyZWQtbG9naW4ubmV0nL3BhZ2VzLzQyY2FkNTJhZmU3YSZyZWNpcGllbnRfaWQ9NzM2OTg3ODg4JmNhbXBhaWduX3J1bl9pZD0zOTM3OTcz	Get hash	malicious	Browse	
	http://https://flyboyfurnishings.com/firstam/RD-FITT	Get hash	malicious	Browse	
	http://https://aterapeutica.com.br/link	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
sni1gl.wpc.gammacdn.net	http://https://www.canva.com/design/DAESYWKuLHs/avvDNRvDuj_tk82H9Q45ZQ/view?utm_content=DAESYWKuLHs&utm_campaign=designshare&utm_medium=link&utm_source=sharebutton	Get hash	malicious	Browse	• 152.199.21.175
	http://y.novobanco.opengateautospray.com/674616e69612e726f7361406e6f766f62616e636f2e7074	Get hash	malicious	Browse	• 152.199.21.175
	http://https://www.canva.com/design/DAEQ9wWiiI4/xe_9LxFtkmjBa9UV_tvT3Q/view?utm_content=DAEQ9wWiiI4&utm_campaign=designshare&utm_medium=link&utm_source=publishshsharelink	Get hash	malicious	Browse	• 152.199.21.175
	http://www.almbrandbk.com	Get hash	malicious	Browse	• 152.199.21.175
	http://https://www.canva.com/design/DAEQZtuJBHQ/-KqHZHDeeo0Ff-f1vALKQQ/view?utm_content=DAEQZtuJBHQ&utm_campaign=designshare&utm_medium=link&utm_source=publishshsharelink	Get hash	malicious	Browse	• 152.199.21.175
	http://https://www.canva.com/design/DAEP8Lslefs/1QHXKjNU7Rc-vcFi3qKqEA/view?utm_content=DAEP8Lslefs&utm_campaign=designshare&utm_medium=link&utm_source=sharebutton	Get hash	malicious	Browse	• 152.199.21.175
	http://https://www.canva.com/design/DAEPXu2qGvw/k5VLbFVATM5hEHHOGOOwNA/view?utm_content=DAEPXu2qGvw&utm_campaign=designshare&utm_medium=link&utm_source=publishshsharelink	Get hash	malicious	Browse	• 152.199.21.175
	http://https://www.canva.com/design/DAEPYcksizk/0MRkCRv3o_LJBVKhQRIOLQ/view?utm_content=DAEPYcksizk&utm_campaign=designshare&utm_medium=link&utm_source=sharebutton	Get hash	malicious	Browse	• 152.199.21.175
	http://https://dryblush.cf	Get hash	malicious	Browse	• 152.199.21.175
	http://https://www.canva.com/design/DAEPWILyBiI/ZnP1WTHl7xNwOB76L4gORw/view?utm_content=DAEPWILyBiI&utm_campaign=designshare&utm_medium=link&utm_source=publishshsharelink	Get hash	malicious	Browse	• 152.199.21.175
	http://https://www.canva.com/design/DAEPD5F7x4w/nI8qoCkPV-p6ew3evzbyTw/view?utm_content=DAEPD5F7x4w&utm_campaign=designshare&utm_medium=link&utm_source=sharebutton	Get hash	malicious	Browse	• 152.199.21.175
	http://https://www.canva.com/design/DAEOhhihuRE/ilbmdiYYv4SZabsnRUealQ/view?utm_content=DAEOhhihuRE&utm_campaign=designshare&utm_medium=link&utm_source=sharebutton	Get hash	malicious	Browse	• 152.199.21.175
	http://https://www.canva.com/design/DAEN9RlD8Vk/acBvt6UoL-DafjXmQk38pA/view?utm_content=DAEN9RlD8Vk&utm_campaign=designshare&utm_medium=link&utm_source=publishshsharelink	Get hash	malicious	Browse	• 152.199.21.175
	http://https://www.canva.com/design/DAEN3YdYVHw/zaVHWoDx-9G9l20JXWSBtg/view?utm_content=DAEN3YdYVHw&utm_campaign=designshare&utm_medium=link&utm_source=sharebutton	Get hash	malicious	Browse	• 152.199.21.175

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://www.canva.com/design/DAENqED8UzU/0m_RcAQIILTwa79MyPG8KA/view?utm_content=DAENqED8UzU&utm_campaign=designshare&utm_medium=link&utm_source=sharebutton	Get hash	malicious	Browse	• 152.199.21.175
	http://https://www.canva.com/design/DAENr9VVSBY/j0BB1RmEldachKWw-1swmQ/view?utm_content=DAENr9VVSBY&utm_campaign=designshare&utm_medium=link&utm_source=publishshare link	Get hash	malicious	Browse	• 152.199.21.175
	http://https://www.canva.com/design/DAENVYOHvFA/QhSvoOcZFDz8qgW3A0jWDQ/view?utm_content=DAENVYOHvFA&utm_campaign=designshare&utm_medium=link&utm_source=sharebutton	Get hash	malicious	Browse	• 152.199.21.175
	http://https://www.canva.com/design/DAENNkaW0Y8/5kCPSDWLGORxHG5wxCeq1A/view?utm_content=DAENNkaW0Y8&utm_campaign=designshare&utm_medium=link&utm_source=sharebutton	Get hash	malicious	Browse	• 152.199.21.175
	http://https://www.canva.com/design/DAEL583ir78/-CJG7ikE36AULbESHNtnfQ/view?utm_content=DAEL583ir78&utm_campaign=designshare&utm_medium=link&utm_source=publishshare link	Get hash	malicious	Browse	• 152.199.21.175
	http://https://www.canva.com/design/DAEMXlzyBJo/VT_PJS9miMeLf1BsAVFwFA/view?utm_content=DAEMXlzyBJo&utm_campaign=designshare&utm_medium=link&utm_source=sharebutton	Get hash	malicious	Browse	• 152.199.21.175
avatars.githubusercontent.com	1d46a419ae040e2c284ce365d66c8971.exe	Get hash	malicious	Browse	• 185.199.111.133
	TxvR Order.exe	Get hash	malicious	Browse	• 185.199.108.133
	5293ea9467ea45e928620a5ed74440f5.exe	Get hash	malicious	Browse	• 185.199.108.133
	Unterlagen PDF.exe	Get hash	malicious	Browse	• 185.199.108.133
	f1a14e6352036833f1c109e1bb2934f2.exe	Get hash	malicious	Browse	• 185.199.108.133
	d88e07467ddcf9e3b19fa972b9f000d1.exe	Get hash	malicious	Browse	• 185.199.108.133
	index_2021-02-18-00_38.exe	Get hash	malicious	Browse	• 185.199.108.133
	571e42f6394e3fe9d63239315df13631.exe	Get hash	malicious	Browse	• 185.199.108.133
	executable.908.exe	Get hash	malicious	Browse	• 185.199.109.133
	executable.908.exe	Get hash	malicious	Browse	• 185.199.111.133
	executable.908.exe	Get hash	malicious	Browse	• 185.199.108.133
	executable.908.exe	Get hash	malicious	Browse	• 185.199.111.133
	executable.908.exe	Get hash	malicious	Browse	• 185.199.111.133
	executable.908.exe	Get hash	malicious	Browse	• 185.199.111.133
	executable.908.exe	Get hash	malicious	Browse	• 185.199.111.133
	executable.908.exe	Get hash	malicious	Browse	• 185.199.108.133
	executable.908.exe	Get hash	malicious	Browse	• 185.199.108.133
	executable.908.exe	Get hash	malicious	Browse	• 185.199.108.133
	executable.908.exe	Get hash	malicious	Browse	• 185.199.108.133
	executable.908.exe	Get hash	malicious	Browse	• 185.199.108.133
microsoftwindows.112.2o7.net	Farie PO.doc	Get hash	malicious	Browse	• 15.237.136.106
	Cerere de pret NUM003112 09-02-2021.doc	Get hash	malicious	Browse	• 15.237.76.117
	Notice_Admin_Johnstoncompanies_8578.htm	Get hash	malicious	Browse	• 15.237.76.117
	http://https://hartdistrict-my.sharepoint.com/:w:/g/personal/mdizon_hartdistrict_org/EcmmCdfu1mtEoYBuvYtOs90BEgUjrpXzZM-WsUQSD4k2RQ?e=4%3aWZv5NT&at=9	Get hash	malicious	Browse	• 15.237.76.117

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://donkoontzdds-my.sharepoint.com:443/:o:/p/paula/EpkEAfrMo1VPgFsywG5EnMwBbr42_dHD8h4N6RCWcat9eA?e=5%3a3JiMMt&at=9	Get hash	malicious	Browse	• 35.181.18.61
	http://https://omoolowo001.github.io/myfirstrepo/YWNjb3VudHNfbG9nindex.html?scriptID=35662936635352205&cookies=MC4xOTUyNjY0OTg0MzM0NTQ0NQ&token=81117470799998&email=jeaton@nlcmutual.com	Get hash	malicious	Browse	• 15.237.76.117
	http://https://kingkorefitness.com/Inc-Corp/RD-FITT	Get hash	malicious	Browse	• 15.237.136.106
	http://https://kingkorefitness.com/Inc-Corp/RD-FITT	Get hash	malicious	Browse	• 15.237.136.106
	http://https://rzh09.github.io/kirapzoxda/adiuew.html?bbre=as83wsdcx	Get hash	malicious	Browse	• 15.237.136.106
	http://https://linkprotect.cudasvc.com/url?a=https%3a%2f%2fseacoccs.github.io%2fvivapdeltoozx%2fsorirw.html%3fbbre%3dod948reids&c=E,1,vSy_DaxVlhDKTU_DAd4XDQRKFbpEz58IBL3G2ibxtXxy4isfCn6tn5y2D7KvyG8o1RL3a--vpSQ8W1tCBVf3nGFmVP0O8Zl4kUultyRSb1120A,,&typo=1	Get hash	malicious	Browse	• 35.181.18.61
	http://https://app.box.com/s/o2w7bicj17iez9hkgk744e23wl6qiw9m	Get hash	malicious	Browse	• 35.181.18.61
	http://https://u920579.ct.sendgrid.net/ls/click?upn=Cq4RbLQjlFZUayowJ9tEN6gixmb7UKhyXAXCvMsmbICjFD5DhJprkszpFOyNbgNmq7-2Bq9gyOkpQCauiiQYtKUuzuhRkDdVY3iYQlbf85PPIex1qg1iCLXLRCmn62egy7Kd2WI-2FZe6QjrykO-2BkxUIwg-3D-3Da0Ze_tSu-2BgbrFGsICLGVaAGPqAvBa4uzmGUZNhZ55boO3KRTzNu4GGZepxUqpMzDNq41wULstJA35t6JtnVf2vFtHlmz2-2B31tSDfiBobK3sk93ifRCie1NHPaL2KnBxyzl2a1K3xUYPE-2FZxt6LXV-2FOq7Qf7BGwhC5mooDbh2JB86GzKa1gkvDcq2SJ7XHDp7jJpNK-2FgzsQi2DReRUeTh8TNbzxPb03EO0c0GUBrVxC04FuSc-3D	Get hash	malicious	Browse	• 15.237.136.106
	http://https://t.yesware.com/tt/ae9851ab7b578dad1289f08bbf450624f7ae3a45/2ee42987f58d2f32bb36ff11a00dd921/2f4e7e35c28c3b7f4958904f5584a915/joom.ag/2VFC	Get hash	malicious	Browse	• 35.181.18.61
	http://https://joom.ag/3wFC	Get hash	malicious	Browse	• 35.181.18.61
	http://https://judithjamm.github.io/vaopstarndupx/ifus.html?bbre=dsi8243er	Get hash	malicious	Browse	• 15.237.76.117
	http://https://criswellauto-my.sharepoint.com/:b:/p/jtan/EU06P7jwOKFJoP-tIPrljMMBEG3gKDGg6TlM9-QtbrOOKg?e=N4aC2p	Get hash	malicious	Browse	• 15.237.76.117
	http://https://sanfetaappdevmaozi-noisy-cassowary-es.mybluemix.net/roietri/ipz.php?bbre=gfh565rtdf&d=DwMFAw	Get hash	malicious	Browse	• 35.181.18.61
	http://https://ewretrytukhjghfgdfsf.azurewebsites.net/5gqxbb/suuyF/tryhfdg.php?bbre=1b077f6510087ea39a88e7c61636c339	Get hash	malicious	Browse	• 35.181.18.61
	http://https://www.canva.com/design/DAEPFQpVQOg/UPJfT3H38FpnoN0B2vprRA/view?utm_content=DAEPFQpVQOg&utm_campaign=designshare&utm_medium=link&utm_source=sharebutton	Get hash	malicious	Browse	• 15.237.136.106
	http://https://thelomacompanies1174-my.sharepoint.com/:b:/g/personal/john_lomamp_com/EfPUPKym1fxAikFwNeaYbrcBiKvlWxqL0hSx6Q33Il8jig?e=4%3aM00aXU&at=9	Get hash	malicious	Browse	• 35.181.18.61

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
MICROSOFT-CORP-MSN-AS-BLOCKUS	Payment.html	Get hash	malicious	Browse	• 52.97.250.194
	Remittance advice.htm	Get hash	malicious	Browse	• 52.97.200.130
	rtofwqxq.exe	Get hash	malicious	Browse	• 104.47.54.36
	26F3.bat	Get hash	malicious	Browse	• 23.98.155.192
	u2KV7KzveH.exe	Get hash	malicious	Browse	• 51.103.66.128
	k.doc	Get hash	malicious	Browse	• 51.103.66.128
	Information.pdf.vbs	Get hash	malicious	Browse	• 51.103.66.128
	moog_invoice_Wednesday 02242021._xslx.hTML	Get hash	malicious	Browse	• 52.97.201.210
	530000.exe	Get hash	malicious	Browse	• 40.113.109.14
	GOKmBGKJCL.docm	Get hash	malicious	Browse	• 13.78.149.8
	fecRZG3xtP.exe	Get hash	malicious	Browse	• 40.88.32.150
	PO.exe	Get hash	malicious	Browse	• 65.52.145.87

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	bhfVDmWu.exe	Get hash	malicious	Browse	• 23.102.129.234
	networkmanager	Get hash	malicious	Browse	• 21.64.178.127
	f_0008a8.exe	Get hash	malicious	Browse	• 20.38.109.132
	wildix-collaboration-mobile.apk	Get hash	malicious	Browse	• 104.45.180.93
	wildix-collaboration-mobile.apk	Get hash	malicious	Browse	• 104.45.180.93
	tS9P6wPz9x.exe	Get hash	malicious	Browse	• 13.74.136.93
	ransomware.exe	Get hash	malicious	Browse	• 13.74.136.93
	Gremian7.exe	Get hash	malicious	Browse	• 13.107.42.13
GITHUBUS	Funded.jar	Get hash	malicious	Browse	• 140.82.121.4
	Funded.jar	Get hash	malicious	Browse	• 140.82.121.3
	1d46a419ae040e2c284ce365d66c8971.exe	Get hash	malicious	Browse	• 140.82.121.4
	a.exe	Get hash	malicious	Browse	• 140.82.121.10
	Covid19_Vacine_Investment_Proposals_1st_Quarter2021 pdf.jar	Get hash	malicious	Browse	• 140.82.121.3
	Covid19_Vacine_Investment_Proposals_1st_Quarter2021 pdf.jar	Get hash	malicious	Browse	• 140.82.121.3
	TxvR Order.exe	Get hash	malicious	Browse	• 140.82.121.4
	5293ea9467ea45e928620a5ed74440f5.exe	Get hash	malicious	Browse	• 140.82.121.4
	Unterlagen PDF.exe	Get hash	malicious	Browse	• 140.82.121.3
	rufus-3.13.exe	Get hash	malicious	Browse	• 140.82.121.4
	f1a14e6352036833f1c109e1bb2934f2.exe	Get hash	malicious	Browse	• 140.82.121.4
	d88e07467ddcf9e3b19fa972b9f000d1.exe	Get hash	malicious	Browse	• 140.82.121.3
	Invoice467972.jar	Get hash	malicious	Browse	• 140.82.121.4
	Invoice467972.jar	Get hash	malicious	Browse	• 140.82.121.4
	password.doc	Get hash	malicious	Browse	• 140.82.121.4
	password.doc	Get hash	malicious	Browse	• 140.82.121.3
	Pastebin.docm	Get hash	malicious	Browse	• 140.82.121.4
	password.doc	Get hash	malicious	Browse	• 140.82.121.4
	Pastebin.docm	Get hash	malicious	Browse	• 140.82.121.4
	Pastebin.docm	Get hash	malicious	Browse	• 140.82.121.3
FASTLYUS	SecuriteInfo.com.Variant.Bulz.362300.21634.dll	Get hash	malicious	Browse	• 151.101.1.44
	44252636284259300000.dat.dll	Get hash	malicious	Browse	• 151.101.1.44
	DTN Basis AWS Basis Main.xlsm	Get hash	malicious	Browse	• 151.101.112.84
	Xeros from condor.htm	Get hash	malicious	Browse	• 104.244.43.131
	RFQ.xlsx	Get hash	malicious	Browse	• 151.101.65.195
	RFQ.xlsx	Get hash	malicious	Browse	• 151.101.1.195
	DTN Basis AWS Basis Main.xlsm	Get hash	malicious	Browse	• 151.101.13 0.109
	DTN Basis AWS Basis Main.xlsm	Get hash	malicious	Browse	• 151.101.12.84
	counters.dll	Get hash	malicious	Browse	• 151.101.1.44
	BL.html	Get hash	malicious	Browse	• 151.101.12.193
	Funded.jar	Get hash	malicious	Browse	• 185.199.11 0.154
	Funded.jar	Get hash	malicious	Browse	• 185.199.11 0.154
	gQcKVtx6h0.dll	Get hash	malicious	Browse	• 151.101.1.44
	qt1dVk6hrj.dll	Get hash	malicious	Browse	• 151.101.1.44
	PnzVGXpv4C.dll	Get hash	malicious	Browse	• 151.101.1.44
	TcNpJ6Lerr.dll	Get hash	malicious	Browse	• 151.101.1.44
	doTCeuxsZh.dll	Get hash	malicious	Browse	• 151.101.1.44
	P1ON2FMKtb.dll	Get hash	malicious	Browse	• 151.101.1.44
	83dLkz7iFE.dll	Get hash	malicious	Browse	• 151.101.1.44
	iyLA8EXSBg.dll	Get hash	malicious	Browse	• 151.101.1.44

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
9e10692f1b7f78228b2d4e424db3a98c	SecuriteInfo.com.Variant.Bulz.362300.21634.dll	Get hash	malicious	Browse	• 34.253.10.100 • 192.229.22 1.185 • 185.199.10 8.133 • 152.199.21.175 • 140.82.121.3 • 151.101.1.192

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	44252636284259300000.dat.dll	Get hash	malicious	Browse	• 34.253.10.100 • 192.229.221.185 • 185.199.108.133 • 152.199.21.175 • 140.82.121.3 • 151.101.1.192
	RFQ.xlsx	Get hash	malicious	Browse	• 34.253.10.100 • 192.229.221.185 • 185.199.108.133 • 152.199.21.175 • 140.82.121.3 • 151.101.1.192
	counters.dll	Get hash	malicious	Browse	• 34.253.10.100 • 192.229.221.185 • 185.199.108.133 • 152.199.21.175 • 140.82.121.3 • 151.101.1.192
	mferreira@itpros.us.com.pff.HTM	Get hash	malicious	Browse	• 34.253.10.100 • 192.229.221.185 • 185.199.108.133 • 152.199.21.175 • 140.82.121.3 • 151.101.1.192
	Xero from mashreqbank.htm	Get hash	malicious	Browse	• 34.253.10.100 • 192.229.221.185 • 185.199.108.133 • 152.199.21.175 • 140.82.121.3 • 151.101.1.192
	Sprint Note tod.friedman@americansignaturefurniture.com 81454 AM .html	Get hash	malicious	Browse	• 34.253.10.100 • 192.229.221.185 • 185.199.108.133 • 152.199.21.175 • 140.82.121.3 • 151.101.1.192
	Outllook_Membership_Update.html	Get hash	malicious	Browse	• 34.253.10.100 • 192.229.221.185 • 185.199.108.133 • 152.199.21.175 • 140.82.121.3 • 151.101.1.192
	Payment.html	Get hash	malicious	Browse	• 34.253.10.100 • 192.229.221.185 • 185.199.108.133 • 152.199.21.175 • 140.82.121.3 • 151.101.1.192
	vmail_6512365134_7863.html	Get hash	malicious	Browse	• 34.253.10.100 • 192.229.221.185 • 185.199.108.133 • 152.199.21.175 • 140.82.121.3 • 151.101.1.192
	Remittance advice.htm	Get hash	malicious	Browse	• 34.253.10.100 • 192.229.221.185 • 185.199.108.133 • 152.199.21.175 • 140.82.121.3 • 151.101.1.192

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	gQcKVtx6h0.dll	Get hash	malicious	Browse	• 34.253.10.100 • 192.229.221.185 • 185.199.108.133 • 152.199.21.175 • 140.82.121.3 • 151.101.1.192
	qt1dVk6hrj.dll	Get hash	malicious	Browse	• 34.253.10.100 • 192.229.221.185 • 185.199.108.133 • 152.199.21.175 • 140.82.121.3 • 151.101.1.192
	PnzVGXpv4C.dll	Get hash	malicious	Browse	• 34.253.10.100 • 192.229.221.185 • 185.199.108.133 • 152.199.21.175 • 140.82.121.3 • 151.101.1.192
	TcNpJ6Lerr.dll	Get hash	malicious	Browse	• 34.253.10.100 • 192.229.221.185 • 185.199.108.133 • 152.199.21.175 • 140.82.121.3 • 151.101.1.192
	doTCeuxsZh.dll	Get hash	malicious	Browse	• 34.253.10.100 • 192.229.221.185 • 185.199.108.133 • 152.199.21.175 • 140.82.121.3 • 151.101.1.192
	P1ON2FMKtb.dll	Get hash	malicious	Browse	• 34.253.10.100 • 192.229.221.185 • 185.199.108.133 • 152.199.21.175 • 140.82.121.3 • 151.101.1.192
	83dLkz7iFE.dll	Get hash	malicious	Browse	• 34.253.10.100 • 192.229.221.185 • 185.199.108.133 • 152.199.21.175 • 140.82.121.3 • 151.101.1.192
	Zh9kAls1Tz.dll	Get hash	malicious	Browse	• 34.253.10.100 • 192.229.221.185 • 185.199.108.133 • 152.199.21.175 • 140.82.121.3 • 151.101.1.192
	iyLA8EXSBg.dll	Get hash	malicious	Browse	• 34.253.10.100 • 192.229.221.185 • 185.199.108.133 • 152.199.21.175 • 140.82.121.3 • 151.101.1.192

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\NY1GEO55\dotnet.microsoft[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):	565
Entropy (8bit):	5.080150069925342
Encrypted:	false
SSDEEP:	12:JsrsrsrUqY0MIcY0MOkuQ7rsrUq/MIc/MOW4Q7rsrUivq+fUUOUUDW4QV:W00U3cOPQv0UdGOjQv0UaUUOUUDjQV
MD5:	B7EFDE44CD76CC3985D2DFEB4285A86E
SHA1:	9BFF123D65BF54D5F488BE9C8AE2BF6A1FE2F872
SHA-256:	3CC84E83FD09C63E1E57A5D89AE2824A87947BB7C1C1D20BB27D9BF8A2F94100
SHA-512:	FD5E44910AC17B572A88A631E2138F2D4C72E4F41F02EC3D129EADE0561DC24E62F80BF84C956D1EB078C4F80DC1C2A71BDAB6A01E09E384A0934F3D4D071B1
Malicious:	false
Reputation:	low
Preview:	<root></root><root></root><root></root><root><item name="Thu Feb 25 2021 21:42:49 GMT-0800 (Pacific Standard Time)" value="Thu Feb 25 2021 21:42:49 GMT-0800 (Pacific Standard Time)" ltime="933733120" htime="30870530" /></root><root></root><root><item name="Thu Feb 25 2021 21:42:50 GMT-0800 (Pacific Standard Time)" value="Thu Feb 25 2021 21:42:50 GMT-0800 (Pacific Standard Time)" ltime="940083120" htime="30870530" /></root><root></root><root><item name="ai_session" value="XndcP|1614318169383.0151|1614318169383.0151" ltime="940083120" htime="30870530" /></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\OFGISG8J\docs.microsoft[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	13
Entropy (8bit):	2.469670487371862
Encrypted:	false
SSDEEP:	3:D90aKb:JFKb
MD5:	C1DDEA3EF6BBEF3E7060A1A9AD89E4C5
SHA1:	35E3224FCBD3E1AF306F2B6A2C6BBEA9B0867966
SHA-256:	B71E4D17274636B97179BA2D97C742735B6510EB54F22893D3A2DAFF2CEB28DB
SHA-512:	6BE8CEC7C862AFAE5B37AA32DC5BB45912881A3276606DA41BF808A4EF92C318B355E616BF45A257B995520D72B7C08752C0BE445DCEADE5CF79F73480910FED
Malicious:	false
Reputation:	high, very likely benign file
Preview:	<root></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{3A9550DE-77F5-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	33368
Entropy (8bit):	1.8734094527377816
Encrypted:	false
SSDEEP:	96:rhZSTZZ2zlWEatEzfEcxMEYEWELEgtEni3:rhZSTZZ2JWvtKfPxMTt0dtli3
MD5:	DA42E17901D4F59892BA24D83C9F6FB2
SHA1:	18F1620818DC4409BA9EB509B4DA37CFA0D072B9
SHA-256:	21DAD4B72C3AE6675021C9CA989AF2B1ECB307B75AAE28A63B26BC5603C1ECAB
SHA-512:	7365E709F62BF856529F9DC0035CDF50D03320677C558169BD5731E4796E0883F49E1F12DD6B71B3CF53B7E483080D485DF26AD00078A6FE8A8FC03666344A6C
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\{3A9550E0-77F5-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	210030
Entropy (8bit):	2.5623768876478197
Encrypted:	false
SSDEEP:	768:4ol42tEsG2t9n1QAdQCduWTVeFyDnqdcV+C+:7cV+C+
MD5:	091E5F0B878B77636098A41DDDABC63D

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{3A9550E0-77F5-11EB-90E4-ECF4BB862DED}.dat	
SHA1:	7552A6356F7A6732DC180F80AAEA5C2F6EB6637D
SHA-256:	6F59B640D2BEBBF432A690924C07DDB2F746C0381891B6EAA771190E9536815D
SHA-512:	D50F5CE1AD03CB2E246B5D332F85EC22B8E6462779B09D41943E7727C5E7A87E03B13CCD0C830A2749E3C4C2EDDC4382FC095E7FC0983AFE78228EBE56792F7
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\{518F19A3-77F5-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5622985739662052
Encrypted:	false
SSDEEP:	48:Iw6Gcpr5ZGwpaCG4pQKGrapbSFGQpKHG7HpRdTGIpG:r+Z5TQy68BSvAmTbA
MD5:	514BD392357381B5D63966370012EE57
SHA1:	75DDC3D2CA62C2410E263C012B8C88D67465FDCC
SHA-256:	16FED22ADD2BA8C7C972C0A36FEEF71EB4E1081B2D08D278B550EA7990D819A0
SHA-512:	720D7E43DF713015FDA401CF56462CEBE3BBE19CBD20010726219E75966A7EC858CE1DDD36B020CB7DD0C7876DBD6293FEA2573BEB98D504C2ACF44176B537D
Malicious:	false
Reputation:	low
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\ynfz0jx\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	118640
Entropy (8bit):	3.9350149257023963
Encrypted:	false
SSDEEP:	3072:VJ222wlJJx22D4k9SvhFQIIbMiiiszIIIzjiiipa6UrrrrurrrryZJ222wlJJxV:VJ222wlJJx22D4k9SvhFQIIbMiiiszII
MD5:	B37A9A80B6C57047EFF2C4377B96FDF5
SHA1:	D61D682988389DB859E5A8A591AD41A4C9FC7663
SHA-256:	2B8A86D9952F60A794821F7AB98F6107DC68FBA0C7642D89271FC83CC2D27EC3
SHA-512:	0E9EF90C940CBE46DE6C50A1A69721C60F827E249E1B59EF19E2EFCF3C285BDDFABFA57494074D5132B497152A8CC4C25A1D2DEF06FB912E90A95BF74ECFCA5
Malicious:	false
Reputation:	low
Preview:	..h.t.t.p.s.:././.w.w.w...i.i.s...n.e.t./.f.a.v.i.c.o.n...i.c.o..... ....(... ...@..... .....}..... .....

C:\Users\user\AppData\Local\Microsoft\Office\16.0\OfficeFileCache\CentralTable.accdb	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	626709
Entropy (8bit):	0.5037784262049757
Encrypted:	false
SSDEEP:	384:rhyJCmZ8SFMjfZ0jGB4tm2WvwtZ1IGK+hVZO4FdgWanGTHi5O:dCCmZHMTZuURv/427GTH+O
MD5:	097C1D465D48D13B42D34BAB76834997
SHA1:	D2D1A7DD2ECF364FD3450A2A910D889DC60332EB
SHA-256:	D60723EA30EC277BF43D3523BBAC26B0A1FD116493490FAB555AD7B125967517
SHA-512:	47E298A235524020A85DE1742625FAC0311BF0EBA3409072D0EDE9FB3FE6C728CA6BE3FCFF960493E06F136634C240D90A749CA23C1CFB226A9B7058D6C1215
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Office\16.0\OfficeFileCache\CentralTable.accdb	
Preview:	.....Standard ACE DB.....n.b`..U.gr@?..~.....1.y..0...c...F...NZW.7.....(....`.8{6)...X.C...3..y[N.|*..|.....^..s.f_...$.g..'D...e....F.x....-b.T...4.0..... ....

C:\Users\user\AppData\Local\Microsoft\Office\16.0\OfficeFileCache\CentralTable.ini	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	36
Entropy (8bit):	2.730660070105504
Encrypted:	false
SSDEEP:	3:5NixJlElGUR:WrEcUR
MD5:	1F830B53CA33A1207A86CE43177016FA
SHA1:	BDF230E1F33AFBA5C9D5A039986C6505E8B09665
SHA-256:	EAF9CDC741596275E106DDDCF8ABA61240368A8C7B0B58B08F74450D162337EF
SHA-512:	502248E893FCFB179A50863D7AC1866B5A466C9D5781499EBC1D02DF4F6D3E07B9E99E0812E747D76734274BD605DAD6535178D6CE06F08F1A02AB60335DE06
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	C.e.n.t.r.a.l.T.a.b.l.e...a.c.c.d.b.

C:\Users\user\AppData\Local\Microsoft\Office\16.0\OfficeFileCache\CentralTable.laccdb	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\MSOSYNC.EXE
File Type:	data
Category:	modified
Size (bytes):	64
Entropy (8bit):	1.3860360556164644
Encrypted:	false
SSDEEP:	3:ulXHaV:uNu
MD5:	334DB8E86457CD1A976CA2A0E56AB93C
SHA1:	533C32C7E721C1742FBBEA46D50B4EC6BDA19733
SHA-256:	4FB2CE4D568A646BE624CFD303E2B09958AC724B3C78FC5F88D36D2781F19F38
SHA-512:	19178D6A265883E64F27A189A7E1E1A64ABFE57485E06DC3A28C0BD3AD41A8D2921ECA4478B95F97AA47D04C7F61F1AD08F24D002826C718AE1CB73A596BBF67
Malicious:	false
Reputation:	low
Preview:	642294. Admin.

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\C35D0C9B-162A-4BE1-BAF9-F09B9C11FBF9	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	132891
Entropy (8bit):	5.375865444417352
Encrypted:	false
SSDEEP:	1536:PcQceNquBXA3gBwJpQ9DQW+zA9H34ZldpKWXboOilXNErLdzEh:/cQ9DQW+z0XiK
MD5:	D5B4A3C64EEB3DB11ACC322CEEAD3774
SHA1:	BB6CB73F13780E5C23BE2561572935F52583A7B1
SHA-256:	120F4251A02B0440E5D965F9FD02CA1C9DAA4C37E4BD44B9D71EAB63C47EF0CD
SHA-512:	BDA6ABF25EF3B905CE82750508A72BC6B14CADFC7FDD9B42B24F9612374218E9FEB843978F44C03ABBE27B7F3DAEE492289B154F60488068FCD92BEB52E73C4
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2021-02-25T20:40:39">.. Build: 16.0.13822.30525-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:url>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\25299F9C.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	PNG image data, 654 x 923, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	59420

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\25299F9C.png	
Entropy (8bit):	7.694210587234906
Encrypted:	false
SSDEEP:	1536:mhrLMxx+G6n5eddv+kA7zqimZdoL/Cc3GYQB43yf:8MT+F5edQjPGZdoL/C8GY64if
MD5:	AAADF2047AF16BD04A41CAB98F82E761
SHA1:	762BF191613A013A7B4CCB6182105CD3BA1FA7A5
SHA-256:	721E916EA29C97983B62594E5AF95ACBC970BD5F1B2FCAA5B416888A271EF83F
SHA-512:	8D6B8580F15C9C8B76483A8B6DA400FB4D5BBDD7C1AA4889FC8C1B84F287A99BD1B4042CFF04AF256681EE4152626B351DB442B3662DF56F71E93157270BE2C
Malicious:	false
Preview:	.PNG........IHDR..............b.|....sRGB.........pHYs..........+......tEXtSoftware.Microsoft Office..5q...IDATx^.......Ov7...!.I...w-.-R...R...".H[.8.>(.R....I .....7.....oC.7..m..7o....7.s.9.... ...@...... P....>.Q.. ...@...... P...c1........ ...@...t..@...... ....F.... ...@...G... ...@....@Q...Eab#.@...... ...#}...... ...@.(...0... ...@......>...@...... P...cQ........ ...@..H.... ...@...(... (Ll...@...... .p..@...... ....E..X.&6... ...@...@8.. ...@.......".p,...A...... ... .@..E.@8.... ...@...........@...... ....F.... ...@...G... ...@....@Q...Eab#.@...... ...#}...... ...@.(...0... ...@......>...@...... P...cQ........ ...@..H.... ...@...(...(Ll...@...... .p..@...... ....E..X.&6... ...@...@8.. ...@.......".p,...A...... ... .@..E.@8.... ...@...........@...... ....F.... ...@.. .G... ...@....@Q...Eab#.@...... ...#}...... ...@.(...0... ...@......>...@...... P...cQ........ ...@..H.... ...@...(...(Ll...@...... .p..@...... ....E..X.&6... ...@.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\6C0FD40A.jpeg	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 72x72, segment length 16, baseline, precision 8, 1024x224, frames 3
Category:	dropped
Size (bytes):	23216
Entropy (8bit):	7.701916157227709
Encrypted:	false
SSDEEP:	384:JOikMVV2vtRWXNqYhsd7WVVqW3ITGHntrnKB8RvKKU3LM8kq9s6MUb:JOikW21EqpZGqW33ntzKB8Rvo3Z9sLo
MD5:	AE39BFE7DE7DDED0C1AA8BCA56F65243
SHA1:	FD4BA003C5021E4FF86F6A995F7154A5B6776488
SHA-256:	2F7F131B2A19EADA069565BA37C790D0544BAFB794B65B397114C803EC4DF4A5
SHA-512:	E84D34DB8D60243DECEEC8A5FEE102030B339CC04A23B8624DF53606492E0C2A328ADF1CA563F2BE1DCA67F24D6952C6367E3938E93244D12DAFB0CD82CF66 A
Malicious:	false
Preview:	......JFIF.....H.H.....C.................................. $.' ",#..(7),01444.'9=82<.342...C...........2!.!22222222222222222222222222222222222222222222222222...........".................... ....}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz... ....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.. ....?._...\|U.O...7.Ej.F.Z.s.2y"...^.=.......G..7...*7......^a@.............H....^.=.......G....P.....Q....m...$.B.H.,a...........I......k.h...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(... (...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\EF142ED.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	PNG image data, 175 x 81, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	3055
Entropy (8bit):	7.910645684698364
Encrypted:	false
SSDEEP:	48:s7YMm70M2QvcNnLLvFXTMAh5vsX3pfRLUBu0NScpY0ysb4fHO3LL4fOw1A68l0RD:0L+vMnLLRTM8BsHPQu0PY0ysb6HO3LK7
MD5:	AF50F17E5B9F20A042975CDE3BD730EC
SHA1:	E96496E5E33C3885752D4190A669B84D1F985FE7
SHA-256:	08CD77CA53547E80C24B95CD4BA6A7D17991F97FB8B387C280680DC12EC0D9CA
SHA-512:	76246B49A1488A6E75D6023AF8CB0A4A154625F222836891A85AE67AB0302C2E0D51E8AF44C7A42A85F8E676B5B48A41E05A86AF2D70BB45FF70E5AA4BBC634E
Malicious:	false
Preview:	.PNG........IHDR.......Q.....+haK....sRGB.........IDATx^.\...........r....r-(.. h@B..P"I......!.ME.1...!`..A.K..Ac@..XQ.eAV.S.....WN%_o....s..og^..^m.7........_.9.O.&C.....f.`8 8`.`.`q...... .`...F7.\..`0`t...?..Na.bv....S.....`@...n..T6.3h..)..A.S...!....F..]NeC;..l......t9...r....I._N..t.......C.l.G.kL.4|v.V.-T....2epg..(...;.....z..:7...`C.9Q..<#f4<..rF...........].H*.....=....O....s.g .4D..X+...8....~$.0.!......W-..<..j.......\|#.(8...~...k....O.gD.`.....f7l..U.\|...@i<h.WF0!.un..-...zz...].....@<h...........5..Z...Sh.4z.....EX...Y1`..5.v'.8`..}..+5.9...6H..n..d2^F.l.......97...8b..` .dtCxY.........y.C....."....[.j.....oo.U.M.7.......$../..#.p..1.....K..`..Q<....1....O.Y|[r....vp.$=..~...ri..J:.....>.}t.D.......,......#.....(....??Booe.O.. .,."..!`...i.^f6.,.._.=?....[...O..k.&|}...(..Px... ..i..j_...R.7.Q...{.h.....:D;g.g.c.v.........K...YP..y.......;..=0P..V4w-.{.....u......^/..?....f..b]...S(.'.y...A..........9V..0..,.v....@.j.#

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{31CB24EF-1DEB-4C38-BB46-32AB8B1362AD}.tmp	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	195870
Entropy (8bit):	4.159826208565377
Encrypted:	false
SSDEEP:	3072:FWiFN+btsA9YHoKceEIm2HhSa56t44wCAMevR+ptk/Ho0ly4Rzca0xzLPJ51VaSy:ip7PTv1LaaBBg
MD5:	378AA1B4F1EF115C1ACBAA4FE1B9FD21
SHA1:	EE604F9E2F20D5810D6D3A41306A7800B96A396E
SHA-256:	71D681AFF0429342EE4DBA13FE46ECE2716E6E6039B7E159C2CA1F3442B9C612
SHA-512:	22A508D5B3AAC904FC50042EFA7B5470384A497B8B5286F4F491C9A4CD9245987F4F7CC4B022613594CB850E55C87E032DD5ACA94EF07B9F83DDB2779A22F30
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{31CB24EF-1DEB-4C38-BB46-32AB8B1362AD}.tmp	
Preview:	..... .!."#.$.%.&.'.(.).*.+.,.-.../.0.1.2.3.4.5.6.7.8.9.:.;.<.=.>...../.....F.i.v.o.o.r. .. .O.v.e.r.l.e.g. . v.e.r.b.e.t.e.r.i.n.g.e.n. .o.m.g.e.v.i.n.g...../..... .A.D.V.A.N.C.E. . .\.y. .6.5.0. .....D.a.t.u.m...:...1.8.-.0.2.-.2.0.2.1.....O.n.d.e.r.w.e.r.p. ...:. ..F.i.v.o.o.r. .. .O.v.e.r.l.e.g. .v.e.r.b.e.t.e.r.i.n.g.e.n..... .....%.....(..gd.u.....gd.u.....gd.sF...%.gd6c....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{A3851AEE-AECA-436C-8A5A-BC14FD1EA042}.tmp	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.1215386864328073
Encrypted:	false
SSDEEP:	3:JlXll/lGNWtWlxlG:ANyiC
MD5:	6D00E84E5EDAA43E119EA03CE5ECAA4F
SHA1:	9FA7D5D09FED0A7C1F8392022EAAA24B66F4E77B
SHA-256:	957DA89085D8855135307E641A71C5EA2284BE478C115D7A6C3E9C095E83D407
SHA-512:	9DD9AD771F98A2AA72A238FCFE2F34AE181059A55A214A0B3EF7238916E9494B7BE5510DF0884B1CB1D357578E27F0E9B13F5CB7A1002E4583DBF428D3BBA0BE
Malicious:	false
Preview:	D...D.d..... .....D..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{D5993233-DA6C-4F31-A159-3A5C447B0181}.tmp	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	1.368237040785311
Encrypted:	false
SSDEEP:	3:IiiiiiiiiVeldI43lnl/bl//l/fl/9vvvvvvvvvvFl/l/lAqsDNjPl3lldHzlbP:Iiiiiiiii8l+4cc8++lwG3qi/
MD5:	CDE38F27CD0333B17A403AC06B2A7316
SHA1:	5CF656B8F36F3DDB631E310A68CB696118A5FD2C
SHA-256:	6241AEC10B55E87042A55E2FFD37A1B4A2F86E502EDE6490A9CFA83B5BC05325
SHA-512:	9A7033DF637BCB370600EF4AA64B20927D48CCA9F663CC20DC6B49E78CD351939C4E41C553A1A8E99DB55964D71FD0EE3A95A364A480E339896EA3BB9B189EAC
Malicious:	false
Preview:	..(...(...(...(...(...(...(...(...(...(...(...p.r.a.t.e.s.h...p..... ...."...&...*.....>...B..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{F7D58E8D-739A-48B6-B99E-11D35D7AABFB}.tmp	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28BA4
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\12971179[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, baseline, precision 8, 32x32, frames 3

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\12971179[1].jpg	
Category:	downloaded
Size (bytes):	883
Entropy (8bit):	7.348077838863208
Encrypted:	false
SSDEEP:	24:Q9YMa6M0XxDuLHeOWXG427DAJuLHenX3Xr3n3PJiOsZN4:Q9YMabuETA1vJ+N4
MD5:	FA5ED0745DF0FA66411F182875FD60F8
SHA1:	1BB4A3A894979E13D561A2CBFB57B24922077491
SHA-256:	F25AF592C4DD3E83E25BA380D17B6F9DB40FA3600D47B4E88247FC2146902676
SHA-512:	2531D85AA9124632E03251069E2B15A5FF92A38D72F017F9AB6E82B553FB54AE38A2C8F1C5BC1F052443283E1C6F712A520A4635576E94F14442D78D3009C12B
Malicious:	false
IE Cache URL:	http://https://avatars.githubusercontent.com/u/12971179?s=32&v=4
Preview:	..... $.' ",#..(7),01444.'9=82<.342.....2!.!22222222222222222222222222222222222222222222222..... . .."..... ....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... ..w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..T...0\._.c.T...yuz.. .s$.2w.Mk^.....l.zg..+.y.E'...6.#.F=..j.c..MI]..,4.t.]c.....{.....Z.....Vut.C....<~5.].~.....4.M..U....b.....${.V.-~.Wf.2..V..)]..)=.C\.....T.>....`..>.....N....Vuu...y8.Ck_Swg.....G.a.;.(n a....&...h<.....$[B@...P.....x.!...Dt..q.?.*.P.....g..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\17-f90ef1[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	134136
Entropy (8bit):	5.224428921008954
Encrypted:	false
SSDEEP:	3072:1f/HuFVppxvIeq0i9d1EwgXA95Ki5DCE4t:1f/Hu/FIhRwt
MD5:	D567746F6D3BABF05ACF7A63730AC2CB
SHA1:	DDB8B9E24115D9653C432C1C2A3C57E0F881AFEB
SHA-256:	F4DF01A10175F31D0620AE8AA24854DF0D8DCB0C752E8465376B2ED3DEF62DE0
SHA-512:	3F9F18CD40F4CDCDA4F55174AC02766F4F511A61797296D59F1F216E2A51FC9068981E0C41C998ECB05053495BD7971FEA56A032F5438438A224CCA1A33F7189
Malicious:	false
IE Cache URL:	http://https://www.microsoft.com/onerfstatics/marketingsites-wcus-prod/shell/_scrf/js/themes=default/54-af9f9f/c0-247156/de-099401/e1-a50eee/e7-954872/d8-97d509/f0-251fe2/46-be1318/77-04a268/11-240c7b/63-077520/a4-34de62/bb-d7480b/db-bc0148/dc-7e9864/6d-c07ea1/29-1ec5a9/f6-aa5278/cd-23d3b0/6d-1e7ed0/b7-cadaa7/c4-898cf2/ca-40b7b0/4e-ee3a55/3e-f5c39b/c3-6454d7/f9-7592d3/92-10345d/79-499886/7e-cda2d3/69-13871c/e5-08f1c0/e0-3c9860/91-97a04f/1f-100dea/33-abe4df/17-f90ef1?ver=2.0&iife=1
Preview:	(function(){/**. * @license almond 0.3.3 Copyright jQuery Foundation and other contributors.. * Released under MIT license, http://github.com/requirejs/almond/LICENSE. */ .var requirejs,require,define,__extends;(function(n){function r(n,t){return w.call(n,t)}function s(n,t){var o,s,f,e,h,p,c,b,r,l,w,k,u=t&&t.split("/"),a=i.map,y=a&&a["*"]||{};if(n){ for(n=n.split("/"),h=n.length-1,i.nodeIdCompat&&v.test(n[h])&&(n[h]=n[h].replace(v,"")),n[0].charAt(0)==="."&&u&&(k=u.slice(0,u.length-1),n=k.concat(n)),r=0;r<n.length;r+ +)if(w=n[r],w===".")n.splice(r,1),r-=1;else if(w===".."){if(r===0||r===1&&n[2]===".."||n[r-1]==="..")continue;else r>0&&(n.splice(r-1,2),r-=2);n=n.join("/")}if((u||y)&&a){ for(o=n.split("/"),r=o.length;r>0;r-=1){if(s=o.slice(0,r).join("/"),u)for(l=u.length;l>0;l-=1)if(f=a[u.slice(0,l).join("/")],f&&(f=f[s],f)){e=f;p=r;break}if(e)break;!c&&y&&y[s]&&(c =y[s],b=r)}!e&&c&&(e=c,p=b);e&&(o.splice(0,p,e),n=o.join("/"))}return n}function y(t,i){return function(){var r=b.call(arguments,0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\1x1clear[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	downloaded
Size (bytes):	43
Entropy (8bit):	3.122191481864228
Encrypted:	false
SSDEEP:	3:CUTxls/1h/:7lU/
MD5:	F8614595FBA50D96389708A4135776E4
SHA1:	D456164972B508172CEE9D1CC06D1EA35CA15C21
SHA-256:	7122DE322879A654121EA250AEAC94BD9993F914909F786C98988ADBD0A25D5D
SHA-512:	299A7712B27C726C681E42A8246F8116205133DBE15D549F8419049DF3FCFDAB143E9A29212A2615F73E31A1EF34D1F6CE0EC093ECEAD037083FA40A075819D2
Malicious:	false
IE Cache URL:	http://https://www.microsoft.com/onerfstatics/marketingsites-neu-prod/_h/9be151e5/coreui.statics/images/1x1clear.gif
Preview:	GIF89a.....!.....,.....D..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\21000428[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, baseline, precision 8, 32x32, frames 3
Category:	downloaded
Size (bytes):	985
Entropy (8bit):	7.431193290888644
Encrypted:	false
SSDEEP:	24:Q9YMa6M0XxDuLHeOWXG427DAJuLHenX3tabWqwJrRljJ4eFpd:Q9YMabuETArXdJr2eTd
MD5:	F11BEBD3272BE79E45889ABAA70C84AB

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\21000428[1].jpg	
SHA1:	4B02180FC34E82AA88B1F0D3A3F1CDF6097C9B2C
SHA-256:	7EB62B514CA774F8041AFCC896CDEBBDD4C6D18C89BFCCE10500D1971B7BDB86
SHA-512:	A994BBA2455300A30CFA9D2DBA423367C675CADBD5065C5EB92F6AA56AC3DEA06DB835E260F86F51999437501C389543746B7863D03ADC8413A02EFF064742E
Malicious:	false
IE Cache URL:	http://https://avatars.githubusercontent.com/u/21000428?s=32&v=4
Preview:	..... $.' '',#..(7),01444.'9=82<.342.....2!.!2222222222222222222222222222222222222222222222222..... . ..''..... ....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... ..w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?.....].+.F.d...X.q. y.`g'..9....i:...o.....~..Ns....4?._..wM.E..0N.....w.....&.9....+.8-..k....C...2.s....#.....<.3..G.Y...R8.F.9....O..P....R..<. .....9...i.Ky{4`.$)...(G$.PN1...Q...oRjQ\.dy".v%W.5...$...H .LwK&....0.C..4.zM...h.a..B.o&..a...~j.m..,n...V.U.2...Ez.*Zl.z...z....@.PZ_E*.xf.YT6@.G.=...x.u.....q.....z.J.MGW.....F.c.G....."..xY.{...."..*.xJU-..qU#v...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\4734691[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, baseline, precision 8, 32x32, frames 3
Category:	downloaded
Size (bytes):	922
Entropy (8bit):	7.355655975810304
Encrypted:	false
SSDEEP:	24:Q9YMa6M0XxDuLHeOWXG427DAJuLHenX3m3m8bAQCyw3v8f:Q9YMabuETAw9A7K
MD5:	3C13AD93A4CD187712A66C033FFFBC4F
SHA1:	27C9752FAB3480F1E2B2D8982F3F2991469AC231
SHA-256:	1EC2934BFE523E1413C666A20AC54769B96F3308B6F7D21C2BEA669966A905B0
SHA-512:	01EDB01B4F8D298883F702D74375D880FE1805B9917C1445FAF80EA5F55AFA75DF5A934F225EB23D11AB367BA7F175018BC64E0CE60E6C912A5255BDD6C65F1
Malicious:	false
IE Cache URL:	http://https://avatars.githubusercontent.com/u/4734691?s=32&v=4
Preview:	..... $.' '',#..(7),01444.'9=82<.342.....2!.!2222222222222222222222222222222222222222222222222..... . ..''..... ....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... ..w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..4=.V5.k.6v.V.\\..... .p....i1..'.T~"ZGy...f)..v.....8..+..v..a.O.k...M.b..+...8.=@.Z.....r.QG.t.....rE%.6j...|d....sW..6.ji.SF...l....-.....Fz._....y4.m..5..0.W.....(.r2k..5..+.P..9....MDj7..6..R.....U..8 .u.F..Gt.....i...X...Z.....y<{..J...R.".)ev.&d ....{.....?.....&.bP.G.)...Di(u.....U.U..w.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\65-478888[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines
Category:	downloaded
Size (bytes):	97357
Entropy (8bit):	5.0726211220968676
Encrypted:	false
SSDEEP:	1536:Q2zddgKHPbn/hLOfbv3DlFeEqyf5Y6FtgAJL55OGHlkzmnez1ZluUbMpmiRhJYJt:Q2zddgKHPbn/hLOfbv3DlFeEqyf5Y6F6
MD5:	3812F46E315F4671CED364915282F27B
SHA1:	5B1D1868DF93F0802B5F3FD2988CCA6853ECBD22
SHA-256:	03CF0734BDE04D5C95941DFE38CFF0561EC117137DF82C8412A590804F08F6A6
SHA-512:	D7A2D59F2F3ABE38F9FED4FE8AF03DAC0373FCA2385FECBAFDB9E44CC897A88913E3563AD7C141F1380A256B10E89DADC8B3EDD52965A4B5F954FBAA1AD33 79A
Malicious:	false
IE Cache URL:	http://https://www.microsoft.com/onerfstatics/marketingsites-neu-prod/west-european/mscomhp/_scrf/css/themes=default.device=uplevel_web_pc_ie/8b-18f8a3/57-7b1339/37-e29aca/21-7d6c87/5a-e79275/b5-6bb6f8/65-478888?ver=2.0
Preview:	..x-hidden-none-mobile-vp{display:none !important}@media screen and (-ms-high-contrast: active){.c-uhfh button,.c-uhfh .glyph-shopping-cart,.c-me .msame_Header{ border:none !important}.c-logo{margin-right:1px;border:none !important;outline:none !important}.c-logo.c-cat-logo:focus>span:before,.c-logo.c-cat-logo:hover>spa n:before{background:WindowText}.c-uhf-nav-link{border:none !important}.c-uhf-nav-link:hover{text-decoration:underline !important}#search{background:Window;color :WindowText}#search span{vertical-align:top}.c-uhfh.c-sgl-stck .c-uhf-menu button:focus,.c-uhfh.c-sgl-stck .c-uhf-menu a:focus,.c-uhfh.c-sgl-stck .c-uhf-nav-link:focus,.c- uhfh.c-sgl-stck .c-logo.c-sgl-stk-uhfLogo:focus,.c-uhfh.c-sgl-stck .c-logo.c-cat-logo:focus,.c-uhfh.c-sgl-stck .c-search #search:focus,.c-uhfh.c-sgl-stck .glyph-shopping- cart:focus,.c-uhfh.c-sgl-stck .glyph-global-nav-button:focus,.c-uhfh.c-sgl-stck .glyph-shopping-bag:focus{outline:2px solid WindowText !important}.c-uhfh.c-sgl-stck .c-uhfh- acti

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\RE4DRie[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 1259 x 472, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	277144
Entropy (8bit):	7.982509692680286
Encrypted:	false
SSDEEP:	6144:FoEUxdsSZjJmkW56vwynyup2RrK3Z0WjggJNERI19SW:I7jjYZ564U3grKZ0WjgQR1P
MD5:	58135C6FDFD079ED2BE729D4BF943B86
SHA1:	A0678A36EB16EFC56AD03B2FF12464EEBC5B8CB0
SHA-256:	F543C6CC2E453F353271F88323750E721C347AF3EEE77766C0929D3DFAF7F6C1
SHA-512:	F574997ABD555A27F857389CE71B4F9B5A08A059CB8EB38D0D714783FE9B004FA2F51D08DE29D91DD0B478054AA1257FA1A024A5C461983EE849850A0B605B4E

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\RE4DRie[1].png	
Malicious:	false
IE Cache URL:	http://https://img-prod-cms-rt-microsoft-com.akamaized.net/cms/api/am/imageFileData/RE4DRie?ver=f61d&q=0&m=8&h=472&w=1259&b=%23FFFFFFFF&l=f&x=0&y=0&s=1898&d=712&aim=true
Preview:	.PNG.....IHDR.....Jl.....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...|dIv.~.-.....Wuuw..vcz.p..f$J...\|..(....4\..I..R.V..J.(q%r...Z.8.....=3.].B.....{.....@.Lwu. .W]..'"ND\...a.KKK](..(..(..(..z.....EQ.EQ.EQ.EQ.Ey.Q.NQ.EQ.EQ.EQ.EQn.T.S.EQ.EQ.EQ.EQ.....EQ.EQ.EQ.EQ..6A.:EQ.EQ.EQ.EQ.E.MP.NQ.EQ.EQ.EQ.EQn.T.S.EQ .EQ.EQ.EQ.....EQ.EQ.EQ.EQ..6A.:EQ.EQ.EQ.EQ.E.MP.NQ.EQ.EQ.EQ.EQn.T.S.EQ.EQ.EQ.EQ.....EQ.EQ.EQ.EQ..6A.:EQ.EQ.EQ.EQ...nw.u+.W.ku.C?.@ ..).... ..y..EQ.EQ.EQ.EQns....~l...-....Tx....u..(..(..(..\|.@a.....k..S.EQ.EQ.EQ....~.....T....V.s..m.rS.u..(..(..(....".0...^..w?..m..U=..P.NQ.EQ.EQ.EQ....E.....+L.8.....\|. ....=..n.+.....)7....EQ.EQ.EQ.E.-..O.._:/.~i....O?;.eq..~;..6(..a.a...-....l.r.X.(..(..(..(..k..~.]~.....n6.-g....4{w.....[....B.qE...=,.L.l[.?N.~T.S.EQ.EQ.EQ....s^o\..F.M7..... .=.VQ.EQ.EQ.EQ...z....$..b.....A...._/.../.F.....oP.4XEQ.EQ.EQ.EQ....cn. .g..^K_v.V.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\RE4pkvE[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 40 x 40, 8-bit gray+alpha, non-interlaced
Category:	downloaded
Size (bytes):	247
Entropy (8bit):	6.338905999061877
Encrypted:	false
SSDEEP:	6:6v/lhPnMtksR+g5gmlUkBNdMSwul9Kx+2lPpgt+SgU2KmiZUup:6v/7Pq+g5gSUkBDkSox+2VPSgU0iqc
MD5:	F855792BD5B8D24E932D25F20D748485
SHA1:	EAAAA94DF42272C945C2330A2A205446F7F71740
SHA-256:	19EA1ED1BC38169EFE6E32AED430D45A2FDACF49A2D6A7DCA1B5F5CD75F83CF1
SHA-512:	D9DAD59EF5FEDE9DD0337A47610018AB6E4A9D3B1E80FC4FF9E6CC660D0B7420A866BB7740AAC759C2632264AD705DB9B0F798209077BA1475D4A5DA5713BDF
Malicious:	false
IE Cache URL:	http://https://img-prod-cms-rt-microsoft-com.akamaized.net/cms/api/am/imageFileData/RE4pkvE?ver=d8fc&q=90&m=6&h=40&w=40&b=%23FFFFFFFF&l=f&o=t&aim=true
Preview:	.PNG.....IHDR...(...(.....&.p.....orNT..w.....sRGB.....IDATH.c`.t@...!...a=.~.....4..h.~..@#P!...hD..#.4.bD?.3 ...1X.t`...1...=.....D7...a ~.....8j.P1../T..f.AZ...p4..8j..0..#.....jK ...b6tA..j..Yjbk=R` ...~...1.w....N.aG.@.z....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\RE4pxBu[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 40 x 40, 8-bit gray+alpha, non-interlaced
Category:	downloaded
Size (bytes):	605
Entropy (8bit):	7.5199699153609325
Encrypted:	false
SSDEEP:	12:6v/7PqXuMxRUHNV7ROerL/EmNsgF8wUy+cghBZ+QXe0q1cg+SR:+RM7cbUen/d8BZxcKg1R
MD5:	2DCF76D4D92B70117E41CC5BE6B686A0
SHA1:	C18F5F4CF898EA6394098EE5C7DFB501E6385DEA
SHA-256:	148606900BB9E626F0C3EB03C5E258E219B5E32BACE51C574169A9A123D64189
SHA-512:	F03609219E9B2AF5F584D6D25E1EC6E053F43DDB26E037AC2491AF305AB6ECFDDEA610DEAC852728DA1918844C1AA030733B14EA62A9092EC2A95F9CB86104AB
Malicious:	false
IE Cache URL:	http://https://img-prod-cms-rt-microsoft-com.akamaized.net/cms/api/am/imageFileData/RE4pxBu?ver=eae5&q=90&m=6&h=40&w=40&b=%23FFFFFFFF&l=f&o=t&aim=true
Preview:	.PNG.....IHDR...(...(.....&.p.....orNT..w.....sRGB.....IDATH.V].. ...D0...@.#...D ...@."........^x.x.qwf.....a.q`.?.....l...Gxh..{.....`,.l...E2..B,.....SF.c|T0.x.5c..."..[A..l..... 2.^_...jz.>.....<..m...|A.8..H._f..;[....I..CN...$d...n..J...pGFfST..\|..4...5..9...?Q#2..f'.W;... .....a.^.[2i..4..c... >."$....i.g.).+V.....d.x...h.l|ta3...\...R..OQ....l...T.|..C.*....].;..>..c.. P.z.V...r....zbmB.....(.|..e-.?..0Yr.h.....p..w.>+/....e.... JS....U...H...l..?...E.4.};....M.c.{....'9..!8.DOA."(..Q.q....- ..Q5....kO75m..Wn...w.U.....r.....,D.z.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\RE4rriw[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 40 x 40, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	546
Entropy (8bit):	6.67436138738567
Encrypted:	false
SSDEEP:	12:6v/7cIaddcY0rdwfbgihih12ovMSvA1jsKi3Xr+gijQ5Wk7R:rIadeHrdAbghr2p49+gEQ5WkF
MD5:	303D29F63674D6C75DE78CCE52660968
SHA1:	37753DAA92E464CE71C6EBA767B77DA227600C2C
SHA-256:	0850AA4CB7CF87C5059C0F503CFED9DABEDECF303C62B3827B70C63B82FA54AA
SHA-512:	264FFD8FE525CC96B9DB58CEFEBB6836C2A1B38EF9736C29844CDF3E10A5BAB282A13CCCC9C16D2DE9BA2EB25F1338315DA1CA95BEC6939425344BE8A4402CB1
Malicious:	false
IE Cache URL:	http://https://img-prod-cms-rt-microsoft-com.akamaized.net/cms/api/am/imageFileData/RE4rriw?ver=b2d5&q=90&m=6&h=40&w=40&b=%23FFFFFFFF&l=f&o=t&aim=true
Preview:	.PNG.....IHDR...(...(..... H_....PLTE.....*....1tRNS.r.....0a`:h.....@..P... <.;..>..+ .!..b(...V.....orNT..w.....sRGB.....IDAT8.....0...;FQP..*...?gl$.%da..V..]0.9!.....Kw.R.%)..TXAU.UT4.&.....E.....lY.h.g.67H.....:.2..>..N.s...<.:\ B.ok.`v.w.G...3 cn.....Oaj.....u.....}..5.1...h!.....z9.3.....;...f.....+T...s.....~.3.;...cf.....;..;4.Un.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\RE4sQDc[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 40 x 40, 2-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	163
Entropy (8bit):	5.471990178621621
Encrypted:	false
SSDEEP:	3:yionv//thPlVXnblpNgpBhV0iMVEeo+kMlsLtsWsoHdaRr3dO07I6F7CXjp:6v/lhPDCdV0TeksRlsSdUtO07IOCTp
MD5:	B2E9EB438C6B233684822F9CFD7D6499
SHA1:	F3F213AE98CF6890DA39692815349DA6FC2B70CD
SHA-256:	821EBFBAD9774A7B858E9A73134E6EECD63EA6CC25B53E7163FA48F4276419C3
SHA-512:	711F9F9CD7E04096FC632B8CE678AE67718E5AD4D46981F7A2A462AAF1EED4F461BF0852D6C1EE7046E3AB4F4F74FAF30B503A04C243DD2CD199FD6FC4CA04BD
Malicious:	false
IE Cache URL:	http://https://img-prod-cms-rt-microsoft-com.akamaized.net/cms/api/am/imageFileData/RE4sQDc?ver=30c2&q=90&m=6&h=40&w=40&b=%23FFFFFFFF&l=f&o=t&aim=true
Preview:	.PNG.....IHDR...(...(.....P.....PLTE.....tRNS...9.....orNT..w.....sRGB.....)IDAT..c`.....E.H|..L.....U ...?.....0G.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\SegoeUI-Roman-VF_web[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 149700, version 1.66
Category:	downloaded
Size (bytes):	149700
Entropy (8bit):	**7.993887132159728**
Encrypted:	**true**
SSDEEP:	3072:/eh+XVusFs5ZuQmbVt4yk0y6UILFw+99pbzU4xYC1u6i9:/eYXVusFUAfJ7k0y67t99pXR1u68
MD5:	9681CE357BA1F36C1857C537E836C731
SHA1:	5016DE608A6454AF21DD7C83AC1BF6DBEECDB902
SHA-256:	F12BF457762D19A0AF14283A631BC2A6FD9182FC29860B2BE5DBB247936056A1
SHA-512:	6915DB2D90C585F8BC572AEF58830AB918D36B7CDDB95344045953DFDF0786945BF9830F94CFF5D2A8C6ACCF42410A012BA2CF8151CAB18B0013C712702F07A
Malicious:	false
IE Cache URL:	http://https://docs.microsoft.com/static/third-party/SegoeUIWeb/1.01.206/SegoeUI-Roman-VF_web.woff
Preview:	wOFF.....H.....(....B.....GDEF...|.....F".lGPOS...p...o..M6'FNpGSUB..._....:.....=..HVAR..g.....W..%.OS/2...`...Z...`m..uSTAT..q....l...b~.r.avar..r.....cmap..D.....cvt .....4..ifpgm...L.....uo..fvar..r$...@...L.3i.gasp...p.....glyf....,..4.....mS.gvar..rd...`....i.f.head.....6...6....hhea.....!...$....hmtx.....wqloca.....p...p.'.maxp...@... ... ...Xname...`.....2cc.post...\..... .Q.wprep...X.....1;HR-.....BQ..^_.<.....<.....^.R.....x.c`d`.X.....'.m..c.. .....R...^...../.....e.u....x.c`aqe.....:....Q.B3_dHc.b``.feb.B&.....L.P.....@F^.ELL....Ar,.....3.1..h..x..W}h.U.....%js...l.3..k."iS,6.r[e..\.....].QS..f..5.,uN...D.FD.:!..."&...).GH.....s..z.M...9.}.9..s^3.M8.8..S..a.>.,..6....%..:..."....,..*t.Z1B..Rez..?.....#....b..(!....5U.t9G....p#..H...h..1.l&.V.VS..ghu..S....=Z.9.v..n...O.s_>.t.F.7...BF.....D92t...G.J.:H.Q..UL..XgP.}hR{.....D.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\ZSQPH9MF.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with CRLF, LF line terminators
Category:	downloaded
Size (bytes):	21839
Entropy (8bit):	5.122549966099536
Encrypted:	false
SSDEEP:	384:gqENBz3DB9jcxvxRmusLQCAy3An7oKCAgeQrEabbSm5d0+BVdmea:QkRvzsMJ+4oNeQwabb30+H6
MD5:	F82DD0CC20A8BBE1A5350FCB4B1D6B47
SHA1:	EDF69416AC765B7BA9382D79CA24BAB900BF6DC6
SHA-256:	85CF1A285D66BCE2A03CA458C1BE1909DBDCC4B29B8EB640E8FBCF4732FB8E1D
SHA-512:	F10F46BA08CB0D0C46738797B3538908D3DDCEACF4704E2A9F157D4467E52F881A5F45FC9B8E3BEF1E19D8C4589F111B23DE5FA58656750CF351484C651722C
Malicious:	false
IE Cache URL:	http://https://www.iis.net/
Preview:	.....<!DOCTYPE HTML>.. [if IE 7]><html class="ie7" lang="en"><![endif]-->.. [if IE 8]><html class="ie8" lang="en"><![endif]-->.. [if gt IE 8]> >..<html lang="en">.. <![endif]-->..<head>.. build date: Mon, 22 Feb 2021 06:29:04 GMT -->.. <meta charset="UTF-8">.. <meta http-equiv="X-UA-Compatible" content="IE=10,chrome=1" />.. <meta name="viewport" content="width=device-width, initial-scale=1.0" />.. <title>.. Home.. :.. The Official Microsoft IIS Site.. </title>.. [if IE]><script src='https://www-iis.azureedge.net/v-2021-01-05-01/scripts-bundle/html5.js'></script><![endif]-->.. ..<meta name="description" content="Learn, download, & discuss IIS7 and more on the official Microsoft IIS site for the IIS.NET development community." />.. .. <link rel="shortcut icon" type="image/ico" href="/favicon.ico">.. <link rel="apple-touch-icon-precomposed" href="/touch-icon-iphone-precomposed.png" />.. <link rel="apple-

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\bootstrap-custom.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines
Category:	downloaded
Size (bytes):	194898
Entropy (8bit):	5.128603866235674
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\bootstrap-custom.min[1].css	
SSDEEP:	3072:fc3q8gK1CfXyj1H0DNv6kNB6w4c0JJFuqNnUuwrdYHE+:fca8gK1CfXyj1H0DNv6kNB6w4c0JJFfd
MD5:	F16344A1180589735E678A8DBC191D0D
SHA1:	AAC7DBD1B45252EFAA76DA11D349F4B1672DB9BE
SHA-256:	FA7D84DA16B986DC1BD6455760DE9FEA00CFB4F67C6E218F12201C6DAEEADD54
SHA-512:	C3F97A2FD06802530DCC6BAD9F79AE01795FC84EA67E933A2FDD39E07B1FF67D203E1CE071CB337E0AE8D961F88C4673B66908B19951DE043A9BED02D6F6AFD
Malicious:	false
IE Cache URL:	http://https://dotnet.microsoft.com/static/css/bootstrap-custom.min.css?v=zUFFfZQtjzfrV0BMRToNsOqlIOMLoV3OQiUTACfEFPs
Preview:	./*!. * Bootstrap v4.6.0 (https://getbootstrap.com/). * Copyright 2011-2021 The Bootstrap Authors. * Copyright 2011-2021 Twitter, Inc.. * Licensed under MIT (https://github.com/twbs/bootstrap/blob/main/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:#512bd4;--secondary:#6c757d;--success:#107c10;--info:#0078d4;--warning:#ffc107;--danger:#e81123;--light:#f8f9fa;--dark:#343a40;--breakpoint-xs:0;--breakpoint-sm:576px;--breakpoint-md:768px;--breakpoint-lg:992px;--breakpoint-xl:1200px;--font-family-sans-serif:"Segoe UI",Helvetica,Arial,sans-serif;--font-family-monospace:Menlo,Monaco,Consolas,"Courier New",monospace;}*,*::before,*::after{box-sizing:border-box;}html{font-family:sans-serif;line-height:1.15;-webkit-text-size-adjust:100%;-webkit-tap-highlight-color:transparent;}article,aside,figcaption,figure,f

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\common[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	20820
Entropy (8bit):	5.282254356180202
Encrypted:	false
SSDEEP:	384:qXioxqE157H96t3KCslCT12Yss2uNc6mR9:qXio0E1PXIT1xY
MD5:	7DDEB37E9EEFDF8CD2D96F6BF861F11C
SHA1:	2BA67DC64C5C8050A98B2F8C13F1227877776C72
SHA-256:	176F4FFF5A724D160D373EFDC51DD5ECEAF039F397884049247598E9FAD91A9C
SHA-512:	471FA249FDE409A8A528D564E21645B7FFE2B949890B6AFAABC72BA2F3FDAAAC2C1F2D90949348A296C2B3859953641535D8F4AF8F104E3F09DB4F95B75F7B2
Malicious:	false
IE Cache URL:	http://https://login-iis.azureedge.net/resources/v-2021-01-05-001/iis/style/css-bundle/common.css
Preview:	html,body,div,span,applet,object,iframe,h1,h2,h3,h4,h5,h6,p,blockquote,pre,a,abbr,acronym,address,big,cite,code,del,dfn,em,img,ins,kbd,q,s,samp,small,strike,strong,sub,sup,tt,var,b,u,i,center,dl,dt,dd,ol,ul,li,fieldset,form,label,legend,table,caption,tbody,tfoot,thead,tr,th,td,article,aside,canvas,details,embed,figure,figcaption,footer,header,hgroup,menu,nav,output,ruby,section,summary,time,mark,audio,video{margin:0;padding:0;border:0;font-size:100%;font:inherit;vertical-align:baseline;background:transparent}body{line-height:20px;height:100%}ol,ul{list-style:none}table{border-collapse:collapse;border-spacing:0}caption,th,td{text-align:left;font-weight:normal;vertical-align:middle}q,blockquote{quotes:none}q:before,q:after,blockquote:before,blockquote:after{content:"";content:none}a img{border:none}article,aside,details,figcaption,figure,footer,header,hgroup,menu,nav,section,summary{display:block}html{height:100%;overflow-y:scroll}body{background:#fff;font:14px/24px 'Segoe UI',Tahoma,Ari

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\configuration[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with CRLF, LF line terminators
Category:	downloaded
Size (bytes):	38647
Entropy (8bit):	5.026580697576986
Encrypted:	false
SSDEEP:	384:42HrFakOnTGzfEoCJSkKEm6733d9NtC9ISp3NJCJUoLgEEpG3GcsGbGt4ElWpKoS:9HrQ6CnDXzaovM2fxhyMaAaPGhyMaAa5
MD5:	1D8211914D5908D7094D1D5E8E642DA5
SHA1:	3991CD9DDA2B136E730D33B252B39DB79DCD73F1
SHA-256:	6499F5797B6AB8C7B737A9930DC7ADAF888212845AF986549506B6E1A6913470
SHA-512:	E17B303AC9C16886AA26F7A2DC65DD4FAF1BCD0284D92780729F994CD28518018DAE2F016EF12CB8BDD706B02FBFAAFB86A0104299455C3E8A973ED89DCCE557
Malicious:	false
IE Cache URL:	http://https://docs.microsoft.com/en-us/iis/configuration/
Preview:	<!DOCTYPE html>.....<html class="hasSidebar hasPageActions hasBreadcrumb conceptual has-default-focus theme-light" lang="en-us" dir="ltr" data-css-variable-support="true" data-authenticated="false" data-auth-status-determined="false" data-target="docs" x-ms-format-detection="none">....<head>...<meta charset="utf-8" />...<meta name="viewport" content="width=device-width, initial-scale=1.0" />...<meta property="og:title" content="Configuration Reference <configuration>" />...<meta property="og:type" content="website" />...<meta property="og:url" content="https://docs.microsoft.com/en-us/iis/configuration/" />.....<meta property="og:description" content="IIS Configuration Reference Internet Information Services (IIS) 7 and later use an XML-based configuration system for storing IIS settings which replaces the..." />....<meta property="og:image" content="https://docs.microsoft.com/en-

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\customers-godaddy[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 637 x 177, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	16969
Entropy (8bit):	7.9470667897009495
Encrypted:	false
SSDEEP:	384:+NvlTdfVSd6ClGXKEFP80j0X1PjqYYwPP4lQZ596:+XXSUvHl80jYSyokX6
MD5:	357A2E5A8D0504FCD230C0D7F6CED70F

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\customers-godaddy[1].png	
SHA1:	883005B1C08BD9A5C789778DBABCBACD9CC05377
SHA-256:	1925BAF3426C413E7382F8CD94AD2DAD61356DE08BB0B6547387C15DCD168242
SHA-512:	75273B7A937115BC183746316E912FDB7548DACD135608B012FB4180045E92C2A81B4984E65CD8272EDF691832112FEE7AF4413DA8454B6B63116448BCABABCD
Malicious:	false
IE Cache URL:	http://https://dotnet.microsoft.com/static/images/redesign/customers-godaddy.png?v=GSW680JsQT5zgvjNlK0trWE1beCLsLZUc4fBXc0WgkI
Preview:	.PNG.....IHDR...}.....+..B.IDATx.....\...tg.m.-.tgv.m..l.m..;.7..^T..$..*.]%.....sz.....<.....m{^.....U.$.%.....,...3...%w.)....U.....tFo..k.S.....F..<3i.:]...g.....w.e.{.[m.K...Q.;.6,...../gn.g....+.8F.....1..O.m.K/....1i..~.\.[....(T.*..{.o...0.z.g....[.....q6}...a.Zu..SM..<SO.b.6.9.>.Bb..-....co.G.....FY.(.CV.....w)K.|_n...*.+g.27.G.n.....&~..B..k.i.....HK.}...m].....&wn..(.*_|...R.sF.....}....F....3|.....3[.p..%...j.|. .3...g...B9.~...0.FV?.Y}..y....U...7....I.z.....,=.[...M....8..k....{...S>9.!....D.A....?W..g.V...f...?.A.....".F.v.....]'....]}..`...h..z.v^.T.....[.B..~Z..M..F=.&..S.F.....B?..".'...d...U...>G.}.Z.g..h+U:...g...#...V.*...M.=.m].....%.>o..B_.}C..S}.{sg.zi.#.....y....~.>.. .....2.....2d..o...L..7.v.....=9.U...8....&.....}U.?...j.M.j;...$M....C.H..ZY...z.&.....I...-Z1.y.=m..+...?../...g:..]..... .4.z@2&..s...g.f.S.6.U.}.t..7xH..|".}.....\..'.+...Xup...W..x..n.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\customers-ups[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	3012
Entropy (8bit):	4.532536234099354
Encrypted:	false
SSDEEP:	48:2DPQWGCuwzkTM/0w+5tcJCW/uKXlI5PAjpcAHcAQyAHYaKYlBPVoboEnVGjv:KPQFCOc0w+5tJW2K1MPAjOA97A41YlEc
MD5:	0AAA5877DFA41D2BB342757D2AB3B57B
SHA1:	8A16F47887C310347CA5C51D1ED94D9C9A5E4968
SHA-256:	8C6B12D5A09FB80C9BD7F42B10D50C0B6A55291E1F6841F17C0BAFC12E8C5B85
SHA-512:	CDAC3BC8178AB34DC1D108F85B4E78DE1E7071C44FCEA49CE7FED9D6CD00C85687C9CC6A4297CCA1700F5A88819D4F8D167FD1416E125CBF048D13D4D2E951
Malicious:	false
IE Cache URL:	http://https://dotnet.microsoft.com/static/images/redesign/customers-ups.svg?v=jGsS1aCfuAyb1_QrENUMC2pVKR4faEHxfAuvwS6MW4U
Preview:	<svg viewBox="0 0 51 60" version="1.1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink">..<title>UPS-logo</title>..<desc>Created using Figma</desc>..<g id="Canvas" transform="translate(-380 -1898)">..<g id="UPS-logo">..<g id="Vector">..<use xlink:href="#path0_fill" transform="matrix(1.25 0 0 -1.25 381.31 1956.37)" fill="#301506"/>..</g>..<g id="Vector">..<use xlink:href="#path1_fill" transform="translate(380 1898)" fill="#FAB80A"/>..</g>..</g>..</g>..<defs>..<path id="path0_fill" fill-rule="evenodd" d="M 1.77162e-06 32.3779L 0.174541 12.5672L 4.6254 7.06904L 17.9785 2.27729e-05L 34.3857 8.02908L 37.7894 16.1454L 37.4403 42.4147L 25.0475 42.7638L 12.1313 40.6693L 0.349605 33.8621L 1.77162e-06 32.3779Z"/>..<path id="path1_fill" d="M 25.2076 0.000491971C 15.4853 0.000491971 7.00468 1.88277 0 5.5947L 0 35.2704C 0 41.5147 2.34621 46.7363 6.78379 50.3739C 10.904 53.7537 23.6466 59.3235 25.2081 60C 26.6889 59.3555 39.5825 53.6996 43.6373 50.3739C 48.0725 46.7382 5

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\downloadshome[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF, LF line terminators
Category:	downloaded
Size (bytes):	44412
Entropy (8bit):	5.400829221268768
Encrypted:	false
SSDEEP:	768:6YBBgYvld1LGW2MdRi8S2n02Z+xwKLhBJRWVK3UokB/kdkNW7Hbr:6YBBgYvldRHdljn0gmhBJRV3ULiKOr
MD5:	0E4378F78480BF4E91C53C0C8BD7EE7D
SHA1:	60D18E93A7244C1EA8C502FC37A8A3A4C874CDB6
SHA-256:	B6C9939B85DD7444A670E01724644575A2BB6C086359838B8DBB7AE8D3A424F4
SHA-512:	72E088BF372EC8871A7EC130250F8E42FED509ED56C01686C41A02B316BA3892F483B515785A237E114AD817EAB45C2D8A39C16AA4311C6BCCB24C7F617A68C
Malicious:	false
IE Cache URL:	http://https://www-iis.azureedge.net/v-2021-01-05-01/scripts-bundle/downloadshome.js
Preview:	../* Minification Error ..(40,83-84): run-time error JS1195: Expected expression: > ..(51,6-7): run-time error JS1195: Expected expression:) ..(53,70-71): run-time error JS1195: Expected expression: > ..(64,5-6): run-time error JS1002: Syntax error: } ..(71,5-6): run-time error JS1002: Syntax error: } ..(78,5-6): run-time error JS1002: Syntax error: } ..(80,7-15): run-time error JS1197: Too many errors. The file might not be a JavaScript file: document.. Minification Error */....$(document).ready(function () {.... $('#btn-search-submit').click(function () {.. var q = $('#txt-search').val();.. if (q.length) { window.location = searchDomain + '/search?searchterm=' + encodeURIComponent(q); }.. });.... $('#txt-search').keypress(function (e) {.. var keycode = (e.keyCode ? e.keyCode : e.which);.. if (keycode == '13') {.. e.preventDefault();.. $('#btn-search-submit').click();.. }.. });.... $(".user-profile a").on("click"

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\facebook[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 32 x 32, 8-bit/color RGB, non-interlaced
Category:	downloaded
Size (bytes):	265
Entropy (8bit):	6.681697500155679
Encrypted:	false
SSDEEP:	6:6v/lhP1RnDsp9ULc5k6sc+7IhXxXA1MiyphxiDw66yVUjqIbp:6v/79GCc5kAhqMpph8UyWq6
MD5:	352637E02A377A29073AA9F65B1FBA22
SHA1:	E5E2B07F777F47DCF158120B11D0B6BDEB0BC878
SHA-256:	C77873C0C4A8499BA493832E950D41CBAEE43020D5C99D702A1E9DEBBAF0DB32

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\facebook[1].png	
SHA-512:	DFDF4B94AC252B67E6D255C708505845AD427CEC4155D4C2796B84AC49658D6D140CC3744A5BA7A2F4F7AE989EC89D1F13271AAAC44ADF15D8553F45BBF447 A
Malicious:	false
IE Cache URL:	http://https://www.microsoft.com/onerfstatics/marketingsites-neu-prod/_h/85288795/coreui.statics/images/social/facebook.png
Preview:	.PNG........IHDR... ... .tEXtSoftware.Adobe ImageReadyq.e<....IDATx.bt.].@K..@c0j.A.B....Vey......T...X:>PKYN.Y.9n5u,...m..a.dG..6..C...].O.=..V....D.>8.)0z1.) D....@....H...(..........0.^..J.8x.......W......-.G-..`0V.....8........@2..M....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\favicon[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 6 icons, 128x128, 16 colors, 72x72, 16 colors
Category:	downloaded
Size (bytes):	17174
Entropy (8bit):	2.9129715116732746
Encrypted:	false
SSDEEP:	24:QSNTmTFxg4lyyyyyyyyyyyyyio7eeeeeeeeekzgsLsLsLsLsLsQZp:nfgyyyyyyyyyyyyynzQQQQQO
MD5:	12E3DAC858061D088023B2BD48E2FA96
SHA1:	E08CE1A144ECEAE0C3C2EA7A9D6FBC5658F24CE5
SHA-256:	90CDAF487716184E4034000935C605D1633926D348116D198F355A98B8C6CD21
SHA-512:	C5030C55A855E7A9E20E22F4C70BF1E0F3C558A9B7D501CFAB6992AC2656AE5E41B050CCAC541EFA55F9603E0D349B247EB4912EE169D44044271789C719CD0
Malicious:	false
IE Cache URL:	http://https://dotnet.microsoft.com/favicon.ico
Preview:	.............h(..f...HH..........(..00......h....6.. ....=..............@..........(....A..(...................(.................................."P......................................"""""""""""""""""""""""""""""""""""" ...3 333333333333333333333333333333"""""""""""""""""""""""""""""""""""" ...333333333333333333333333333333"""""""""""""""""""""""""""""""""""" ...333333333333333333333333333333"""" """""""""""""""""""""""""""""""" ...333333333333333333333333333333"""""""""""""""""""""""""""""""""""" ...333333333333333333333333333333"""""""""""""""""""""""""""""""""""" ...33333333333 3333333333333333333"""""""""""""""""""""""""""""""""""" ...333333333333333333333333333333"""""""""""""""""""""""""""""""""""" ...333333333333333333333333333333"""""""""""""""""""""""""""""" """""""" ...333333333333333333333333333333"""""""""""""""""""""""""""""""""""" ...333333333333333333333333333333"""""""""""""""""""""""""""""""""""" ...3333333333333333333333 333333333"""""""""""""""""""""""""""""""""""" ...333333333333333333333333333333""""""""""""""""""""""""""""""""

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\home-hero-bg[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	39993
Entropy (8bit):	4.0685196750676305
Encrypted:	false
SSDEEP:	768:kjkSKx5vspoJhh1LXOVm5bazxW2fp8Qd5Ca48Z/fDT:5SKTx1LTj2b9P
MD5:	151DB21C2E4C2C163F30276469152F0B
SHA1:	9561B63C99C963871DA1A447BCA8A801B2E5027F
SHA-256:	7E7F55FD1D6A0AC778DECA4E11CCB740337A27F36909968C55BD3CFEC431D1B6
SHA-512:	0416EFFF719E486519A22F5DFDDC62F174D5948A03026E9E521992AAE55411362FAFA014445E830D1F2821F3818314F9D02DD5EC9B3C3CDB78201D8DAED9C1C
Malicious:	false
IE Cache URL:	http://https://dotnet.microsoft.com/static/images/redesign/home-hero-bg.svg
Preview:	<svg width="800" height="100" viewBox="0 0 800 100" version="1.1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink">..<title>Tile</title>.. <desc>Created using Figma</desc>..<g id="Canvas" transform="translate(-64 1126)" opacity=".07">..<clipPath id="clip-0" clip-rule="evenodd">..<path d="M 64 -1126L 8 64 -1126L 864 -1026L 64 -1026L 64 -1126Z" fill="#FFFFFF"/>..</clipPath>..<g id="Tile" clip-path="url(#clip-0)">..<g id="Group">..<g id="Vector">..<use xlink:hre f="#path0_fill" transform="translate(78 -1116)" fill="#FFFFFF"/>..</g>..</g>..<g id="Group">..<g id="Vector">..<use xlink:href="#path1_fill" transform="translate(374 -1116)" fill="#FFFFFF"/>..</g>..</g>..<g id="Group">..<g id="Vector">..<use xlink:href="#path2_fill" transform="translate(176 -1116)" fill="#FFFFFF"/>..</g>..</g>..<g id="Gro up">..<g id="Vector">..<use xlink:href="#path3_fill" transform="translate(280 -1116)" fill="#FFFFFF"/>..</g>..</g>..<g id="Group">..<g id="Vector">..<use xlink:href="#pat

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\home.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):	541
Entropy (8bit):	4.993219052734672
Encrypted:	false
SSDEEP:	12:wQ7vamY0CRFXRLXSZYK+CPhUvO2X9MUSeKqKSr0zMsHtiFj3:B7amYNRFXJXtXwhCX9MxeKqJ4btiFT
MD5:	7772ADC543163860614852CF46FD75FE
SHA1:	38C92575FC84058A863BD74011AE974E0BB4E476
SHA-256:	ED3E30DFDB49657BE1D74047AF0D54E65B3A777EBEC10CD9FAC4C508859F2C6A
SHA-512:	5A59D66F0882DE0C021B63284134EC4DA60D6CE9F0BEB6C95A2CEC317D6480C9B2A8FB46610BB1150E8E9CDF2DF2DB6C92836628693968D68E83BF71AB05E7 E
Malicious:	false
IE Cache URL:	http://https://dotnet.microsoft.com/static/js/home.min.js?v=gyCwryoVznJoQ0qrJPkCUl2d0uo8E-dIqE9WoqSYYJo

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\home.min[1].js	
Preview:	$(function(){$(window).width()<992||($(".tagline").addClass("typing"),setTimeout(function(){function i(t,r,u){r<t.length?(n.show().html(t.substring(0,r+1)),setTimeout(function(){i(t,r+1,u)},100)):typeof u=="function"&&setTimeout(u,2e3)}function r(t,i){t>0?(n.html(n.html().substring(0,t-1)),setTimeout(function(){r(t-1,i)},100)):typeof i=="function"&&setTimeout(i,100)}function u(f){r(n.html().length,function(){i(t[f],0,function(){u((f+1)%t.length)})})}var t=["web","mobile","desktop","game","IoT","all your"],n=$(".tagline");u(0)},3e3))});

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\httpErrorPagesScripts[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	12105
Entropy (8bit):	5.451485481468043
Encrypted:	false
SSDEEP:	192:x20iniOciwd1BtvjrG8tAGGGVWnvyJVUrUiki3ayimi5ezLCvJG1gwm3z:xPini/i+1Btvjy815ZVUwiki3ayimi5f
MD5:	9234071287E637F85D721463C488704C
SHA1:	CCA09B1E0FBA38BA29D3972ED8DCECEFDEF8C152
SHA-256:	65CC039890C7CEB927CE40F6F199D74E49B8058C3F8A6E22E8F916AD90EA8649
SHA-512:	87D691987E7A2F69AD8605F35F94241AB7E68AD4F55AD384F1F0D40DC59FFD1432C758123661EE39443D624C881B01DCD228A67AFB8700FE5E66FC794A6C0384
Malicious:	false
IE Cache URL:	res://ieframe.dll/httpErrorPagesScripts.js
Preview:	...function isExternalUrlSafeForNavigation(urlStr)..{..var regEx = new RegExp("^(http(s?)|ftp|file)://", "i");..return regEx.exec(urlStr);..}..function clickRefresh()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..window.location.replace(location.substring(poundIndex+1));..}..}..function navCancelInit()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..var bElement = document.createElement("A");..bElement.innerText = L_REFRESH_TEXT;..bElement.href = 'javascript:clickRefresh()';..navCancelContainer.appendChild(bElement);..}..else..{..var textNode = document.createTextNode(L_RELOAD_TEXT);..navCancelContainer.appendChild(textNode);..}..}..function getDisplayValue(elem

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\iis-new-logo[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 94 x 70, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	1715
Entropy (8bit):	6.079695372617734
Encrypted:	false
SSDEEP:	24:SF1h8yxQumhpBt2BfWwQMGdlIa4HPddikAm5NJIBB7DLO:SLhDtMB/1MGdl14FqGvIBNDLO
MD5:	0456E8EAC54EDA32F6674DE66A81175D
SHA1:	60B4AF4696CF5CA16088811795A5A61B3CD985B4
SHA-256:	B3D431B09ABCF901FFC40EE7DE5EC9183DAC26B66EE0BBB8306824A858A8178C
SHA-512:	716F999A835206814228E8C77217DB4EDDC3D58772C11C0536DC429747E494456C3CCF40D89E460BE0324CBF5410B5125B118CC4BDB111E02CA99AB9007870B
Malicious:	false
IE Cache URL:	http://https://www-iis.azureedge.net/v-2021-01-05-01/images/iis-new-logo.png
Preview:	.PNG........IHDR...^...F.....r.....mPLTE......sss333ssssssssssssssss333sss333sss333333ssssss333ssssss333ssssssssssss333333sssssssssssssssssssssssssssssssssssssss333sss333ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss333ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss333sssssssssssssssssssssssssss333ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss333ssssssssssss333sss....P"......q.......tRNS...@Q...`.... ....p0W..0.."M...L..P.!....9.8.......^./..R...1.....E.....P,..).....>....A..k....%[.?=...w..U.......]..G.b..V.. .SN..J......o$CY....O*T...5.B..:Fi.K.(.;.I{&....#.r.H5....,IDATx^...o....a.@CHh ...P..B...K.....&......?.2.;....v.2.v...9W....\|.&..M...M..TC..5.LU!..~..Y^Z....f.6......p$.!.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\jsll-4[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):	56291
Entropy (8bit):	5.402726813102013
Encrypted:	false
SSDEEP:	768:0tgoOjNcc6rCDBjPSeAaKU7rD8kc7HhAHZcllEiKjkT3dgD4GD1hrTd8PuWCF9IS:0tV81ICDVRQnhAiUinxgDRQ7wYv6p
MD5:	CAF5C715307CB80BD4B30E2DA8E95C37
SHA1:	961579FB71954E027DD519058F6E2DA3D83EB7C2
SHA-256:	E246EFF2F6AE3E255A06EB561E6FC93AE3BEF2CCE22C5E0124D713C15F80567C
SHA-512:	DAB733460AFF828BBC696B159D8B0B3877E648FD4E3E59A913865C676032816B4599D5390326C7EFE652C5636C5B4F56B9D78413EB19AD19E5616D049BC775B0
Malicious:	false
IE Cache URL:	http://https://az725175.vo.msecnd.net/scripts/jsll-4.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\jsll-4[1].js	
Preview:	var awa=awa||{},behaviorKey;awa.isInitialized=!1;awa.verbosityLevels={NONE:0,ERROR:1,WARNING:2,INFORMATION:3};awa.behavior={UNDEFINED:0,NAVIGATIONBACK:1,NAVIGATION:2,NAVIGATIONFORWARD:3,APPLY:4,REMOVE:5,SORT:6,EXPAND:7,REDUCE:8,CONTEXTMENU:9,TAB:10,COPY:11,EXPERIMENTATION:12,PRINT:13,SHOW:14,HIDE:15,MAXIMIZE:16,MINIMIZE:17,BACKBUTTON:18,STARTPROCESS:20,PROCESSCHECKPOINT:21,COMPLETEPROCESS:22,SCENARIOCANCEL:23,DOWNLOADCOMMIT:40,DOWNLOAD:41,SEARCHAUTOCOMPLETE:60,SEARCH:61,SEARCHINITIATE:62,TEXTBOXINPUT:63,PURCHASE:80,ADDTOCART:81,VIEWCART:82,ADDWISHLIST:83,FINDSTORE:84,CHECKOUT:85,REMOVEFROMCART:86,PURCHASECOMPLETE:87,VIEWCHECKOUTPAGE:88,VIEWCARTPAGE:89,VIEWPDP:90,UPDATEITEMQUANTITY:91,INTENTTOBUY:92,PUSHTOINSTALL:93,SIGNIN:100,SIGNOUT:101,SOCIALSHARE:120,SOCIALLIKE:121,SOCIALREPLY:122,CALL:123,EMAIL:124,COMMUNITY:125,SOCIALFOLLOW:126,VOTE:140,SURVEYINITIATE:141,SURVEYCOMPLETE:142,REPORTAPPLICATION:143,REPORTREVIEW:144,SURVEYCHECKPOINT:145,CONTACT:160,REGISTRATIONINITIATE:161,REGISTRATIO

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\microsoft-logo2[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 89 x 19, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	1152
Entropy (8bit):	7.755397690287432
Encrypted:	false
SSDEEP:	24:9HuefFHH8rU+B+V8WUBgcjDt8CmSIgYiOo+DJdc:ZXfFHHLV985jWlSROo+DJdc
MD5:	A9B90F3D5C63149938FDB40A76C135C2
SHA1:	E55DDEC6D81066452FA8D68FB27E6AA6AA397FF3
SHA-256:	254251FD421ABFD7966A41EC0251D5B6796C99362C7CF90C8E286A9D457543F1
SHA-512:	C5F7318B4EB3885E34A2C933E71B8667F1A6530ADAE689852B3A752538C619DD89AF668E2BEF21E716913F47AB095DF413984BB6CEB2B0790DCF49BC18277E38
Malicious:	false
IE Cache URL:	http://https://www-iis.azureedge.net/v-2021-01-05-01/images/microsoft-logo2.png
Preview:	.PNG.....IHDR...Y.....GIDATX...h.U...j.....&..RT....XF..[w,A.A..i.....%.[..(.m...[...F.i..:4s.....o|.7...<..<.....~.....a:.g..!.#....5.D.:.+++.O\-.....61H.t.....(.V"...l...X.~...;[.;.~..^.Ipt.8#Z...*...Y,p.x.?..Z1P..$Wv....Gp.x*..E.k.BT...=Y,r/.,#... .?.H.....st&...D...0!.Y..O.Gm.\|h.s...x.-.S...;...E...u.f..?.Blc..N\|.....g.>26./\|)..D~G.....n..i.F.....\|3.L.U..\|L.pND>L.M...]....8!..s..''&Qn....;..y.$...2yOf.-8Z..o.I<.m1b..3.5Q.By.e[..b...!.....p..V.X+.....,...w.8J.Z.....A..F4[.6..!.9T.....KG.....l...l$.....R..#N...l7..m.;_.. ..fQ...L.U{....H...W\.-.....f.B...f(..rr..h....N....K).....80M.e.n...''.h....9.-.t.M.....7q..R.z1.6...'8.\|..6.<9...P.v@Hz.....K..N....I..\|....D..].I.O.=.k{?.-.'.....y....X..n'x.{\..5.K..Va.;..E\.Fd...<..F...]lscm+.....X...''\|D...x..=...O.....U...m.....$.K....o.....9&.:...c.<^.90..^..SyG.bY...{....}?../....._.{lOw.....M....0...o....Q$..n.[...o%%...@8

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\new-features-introduced-in-iis-10-1709[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with CRLF, LF line terminators
Category:	downloaded
Size (bytes):	37332
Entropy (8bit):	5.045079917185881
Encrypted:	false
SSDEEP:	384:427aCfGzfEoCJSkKEm6773d9NtC9ISp3NJCJUoLgaHGaGwGHGt4ElSl3BOjEiKhY:9X6CnfXz+I3B/hyMaAaPGhyMaAa5
MD5:	480B6D1BCD68F1B5E4EEF3A0FB07B7F3
SHA1:	8172974C45F55DC0A966162F968E8E8485A8C034
SHA-256:	71183C56331175797B0DF317A5CEC2A2E5F5EE075F1ADE437ADDA5E149CF1661
SHA-512:	9304BC13759FCCC14440B835B5D29C3DB089D34352CEB774FB189410ABDE08F94ADA3B39B97EF4ADDFDC3DD2C36B13E718F5CCDA23BB6B8ED05295376B9D9C67
Malicious:	false
IE Cache URL:	http://https://docs.microsoft.com/en-us/iis/get-started/whats-new-in-iis-10-version-1709/new-features-introduced-in-iis-10-1709
Preview:	<!DOCTYPE html>.....<html class="hasSidebar hasPageActions hasBreadcrumb conceptual has-default-focus theme-light" lang="en-us" dir="ltr" data-css-variable-support="true" data-authenticated="false" data-auth-status-determined="false" data-target="docs" x-ms-format-detection="none">....<head>...<meta charset="utf-8" />...<meta name="viewport" content="width=device-width, initial-scale=1.0" />...<meta property="og:title" content="New Features Introduced in IIS 10.0 Version 1709" />...<meta property="og:type" content="website" />...<meta property="og:url" content="https://docs.microsoft.com/en-us/iis/get-started/whats-new-in-iis-10-version-1709/new-features-introduced-in-iis-10-1709" />.....<meta property="og:description" content="The article introduces native HTTP Strict Transport Security (HSTS) support in IIS 10.0 version 1709." />....<meta property="og:image" content="https://docs.micr

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\scripts-jquery-validate[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):	26547
Entropy (8bit):	5.222838132538589
Encrypted:	false
SSDEEP:	768:ztpdABVS5ou94pzfjny+8vT3D2SZG9Pl2wHLVH7U7h:ppdAVS5ou98Lny+sD2lDHLVHs
MD5:	CF8BAF10D9875C045363E6E62AC391E3
SHA1:	F6D924EF46F1E35D30DDE6DB6627991E323C6F06
SHA-256:	4EE9FF61B491970EF9A0F904C1C1C160A96E8570DE5DF56D84DA24EB8923FED1
SHA-512:	6A85B6A52B90853224ABDA25BFAF80E93F31BE69FE6132399833EEF81EB2306ECB237E0C4DC2320CCB4BE68FBB489AAEB5D8C6C08EA52C71997BE5D93861A334
Malicious:	false
IE Cache URL:	http://https://login-iis.azureedge.net/resources/v-2021-01-05-001/scripts/scripts-bundle/scripts-jquery-validate.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\scripts-jquery-validate[1].js	
Preview:	/*! jQuery Validation Plugin - v1.13.0 - 7/1/2014. * http://jqueryvalidation.org/. * Copyright (c) 2014 J.rn Zaefferer; Licensed MIT */.!function(n){"function"==typeof define&&define.amd?define(["jquery"],n):n(jQuery)}(function(n){n.extend(n.fn,{validate:function(t){if(!this.length)return void(t&&t.debug&&window.console&&console.warn("Nothing selected, can't validate, returning nothing."));var i=n.data(this[0],"validator");return i?i:(this.attr("novalidate","novalidate"),i=new n.validator(t,this[0]),n.data(this[0],"validator",i),i.settings.onsubmit&&(this.validateDelegate(":submit","click",function(t){i.settings.submitHandler&&(i.submitButton=t.target);n(t.target).hasClass("cancel")&&(i.cancelSubmit=!0);void 0!==n(t.target).attr("formnovalidate")&&(i.cancelSubmit=!0)}),this.submit(function(t){function r(){var r;return i.settings.submitHandler?(i.submitButton&&(r=n("<input type='hidden'/>").attr("name",i.submitButton.name).val(n(i.submitButton).val()).appendTo(i.currentForm)),i.setting

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\sprite[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 140 x 540, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	5197
Entropy (8bit):	7.805675053594171
Encrypted:	false
SSDEEP:	96:HcR3DBWHO8CJ2Glhs6t1YuvFWJPq5ofKtjUI5Nu1kscExnDTp4yOwqp0d6:8RzBT8CQ1udWJ6jjUWAknExnHdrqa6
MD5:	7AC90B1A61D512D60D3C07EDF3ADF0AC
SHA1:	9E20C8ECBF5C88FD326E1B112D32DAAD5719CCDC
SHA-256:	67C411A7FEB225208D88A6BEBE2353136DF5F0A4ACA7EE447394AF9EDF7FB9BA
SHA-512:	59CD15FD361D5BC7DA460388511BDA4F03AF443B87E42D15927106360E77B280FC365487FB706782EC84760F99E88AAB6E2FA37EDB049F843C90D1DAAA3AD88
Malicious:	false
IE Cache URL:	http://https://www-iis.azureedge.net/v-2021-01-05-01/images/sprite.png
Preview:	.PNG.....IHDR.....$9FT....IDATx..._h.U...B P...BPT.@n..E%E.....BI..E...T..@M.+..jt%.X...(.:.\...J@..J....B...d'..\|w..3.f.....=.0.....33;K.Hd.....a.<.H.b..#..4.m.Y..I...,...w.....N.>Q....;0....6...'..`BX..t..c...8..,..4.~.'.n.s.*p.x....?.>Q..3..Q.@<.....".....F.....s.O.i0j..$.?.2.!3.S..J.."..h.].8..=.S.O...n...s...@..v_.]....1..C..S}.!./....3.j.L..D.._...{c..,..7.$..q.{}A.o\.....$....`(e.Y|BjW?../N..7b...z..Pz0..o.<%..TK...Mx.8..8..p.I...8-.~Oc.....Ix.i.h...V.....`(..~K]..k.....5^..K}.....i0.....i(z]}.Q.}....Su~...?.%.C|ZM...3.>7.....6:....."..n).$xpF..Ot7.3k.~.H..1.N.#..g.....m..8e.F.k...L.....0.SR..c...C.....a0.....!.C..:'.IK0.z``.%.`.K0..e.,...,n....=z...A9~..i.].et.5...L....@N..).?q...}.3..:.c..k0`.#.`..FZ.#..+.W..0\a\g.0),+.E...>..p...k.^..W...C..$....d.....`.?..0..Y(.. ..c. n5.H."i.....`....!.C...9.1."......!.C...8.|.X.Y.....{..KO..[.9?y.&6..A.....s.* .^.Ci.....`0...I../2.J.f...>..`Le....PZ0=...w.K..`..F

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\swimlane-aspnet-extends-dotnet[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	62390
Entropy (8bit):	5.444896142358859
Encrypted:	false
SSDEEP:	768:naF93b8Ih0YgCee+Bgsymb0M4Xy/bJ5loSDOQqkjDTgJYQ8TcPLHwjiBZciii:64DTEm1lloSokbA4TSLdZc+
MD5:	5F73CD60DF6801F729E623685A7165D4
SHA1:	80A688D318884FF2D6748A99F8239B3F2066C3FF
SHA-256:	1338D873F9050CB2544C343F03A2ED1196085E27737624996496829650BCD639DA
SHA-512:	6490237167114F3EC09345C8C8893EEBD5955F613709A3037AA1F1491330C1356B8EAF08656D86AECEF8C9291FAB4ECA65BA38F9960E17D32A68D5FF47B5E2A4
Malicious:	false
IE Cache URL:	http://https://dotnet.microsoft.com/static/images/illustrations/swimlane-aspnet-extends-dotnet.svg?v=EzjYc_kFDLJUTDQ_A6LtEZYIXidzdiSZZIKWULzWOdo
Preview:	<?xml version="1.0" encoding="utf-8"?>.. Generator: Adobe Illustrator 24.3.0, SVG Export Plug-In . SVG Version: 6.00 Build 0) -->..<svg version="1.1" id="Layer_1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" x="0px" y="0px"... viewBox="0 0 636 300" style="enable-background:new 0 0 636 300;" xml:space="preserve">..<style type="text/css">....st0{fill:#FBC977;}....st1{fill:#57AA9A;}....st2{fill:#F7B548;}....st3{fill:#6BA8F1;}....st4{fill:#BDD8F9;}....st5{fill:#8065E0;}....st6{fill:#FFFFFF;}....st7{fill:#1572E0;}....st8{fill:#B0D1F7;}....st9{fill:#FFD590;}....st10{fill:#7FD5CA;}....st11{fill:#D8E8FB;}....st12{fill:#C2E8E3;}....st13{fill:#FFECCD;}....st14{fill:#FEDEA7;}....st15{fill:#D1C5F4;}....st16{fill:#70D6E0;}....st17{fill:#25BACA;}....st18{fill:#1BA1B5;}....st19{fill:#8A6FE8;}....st20{fill:url(#SVGID_1_);}....st21{fill:#522CD5;}....st22{fill:url(#SVGID_2_);}....st23{fill:url(#SVGID_3_);}....st24{fill:url(#SVGID_4_);}....st25{fill:url(#SVGID_5_);}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\toc[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):	30435
Entropy (8bit):	4.645466725270606
Encrypted:	false
SSDEEP:	384:44gFFWT+jbv1UGSpxlPgaTX0HYq6vJnXe1hZII60lzNqz1Ky:44g3WT+O7pxlrTXOYq6vJnfyzNc4y
MD5:	BE7519EB455A08BA0DD716F212FFF3F7
SHA1:	0D81F993EDF96B106541762E252ABA81ACFA6E8A
SHA-256:	CC680882BBD1D0A1C99D60EDBAF09D7FB27BCDF5B1688579BE865237C51D5E13
SHA-512:	D288915E6C1ED6D23F1BAFEB99A307CAF461952FDA1B4BBF7FD73801BA55265AF6A7E5C7F04DE5EE22EDAB779C9E8F19F001998F8034EE29B80AECDE4B2F3BF2
Malicious:	false
IE Cache URL:	http://https://docs.microsoft.com/en-us/iis/configuration/toc.json

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\toc[1].json	
Preview:	{"metadata":{"pdf_absolute_path":"/iis/opbuildpdf/configuration/toc.pdf","open_to_public_contributors":true,"breadcrumb_path":"/iis/breadcrumb/toc.json","extend Breadcrumb":"true","_navPath":"/foo","_navRel":"/foo","searchScope":["IIS"],"ms.prod":"iis","ms.topic":"conceptual","author":"shirhatti","ms.author":"soshir"},"items":[{" href":"./","toc_title":"<configuration>","children":[{"href":"administrators/","toc_title":"<administrators>","children":[{"href":"administrators/managementscope/","toc_title":"<ma nagementScope>","children":[{"href":"administrators/managementscope/add","toc_title":"<add>"}]}]},{"href":"administratorsproviders/","toc_title":"<administratorsProviders >","children":[{"href":"administratorsproviders/add","toc_title":"<add>"}]},{"href":"configpaths/","toc_title":"<configPaths>","children":[{"href":"configpaths/searchresult/","toc_ title":"<searchResult>","children":[{"href":"configpaths/searchresult/section","toc_title":"<section>"}]}]},{"href":"configurationredirectio

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\twitter[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 32 x 32, 8-bit/color RGB, non-interlaced
Category:	downloaded
Size (bytes):	532
Entropy (8bit):	7.480175935964278
Encrypted:	false
SSDEEP:	12:6v/79GsdpT04EoI/TGxLd1sjDBdqktOeUoOzQag23jEAgc:SdpfdUyxpgMb1zpg2Tpp
MD5:	B30436EB503A7EA8E77925F435DF4671
SHA1:	3313C5FDE8EC85B94547168B867EFEC0188F5987
SHA-256:	0AC4630B76827B89EBEA070A1BEB6E5175D280EADC76B67FA886CF6068368CA3
SHA-512:	CE6B7F9D8860E146CD41802FBD30AE99F205D145CCA4BBECBAB446851165BEE8316FEAABD83826FB31CA97652E911BE4815ED542F33B5BFEAABDCF71BCEF CDC8
Malicious:	false
IE Cache URL:	http://https://www.microsoft.com/onerfstatics/marketingsites-neu-prod/_h/93690392/coreui.statics/images/social/twitter.png
Preview:	.PNG.....IHDR... ... .tEXtSoftware.Adobe ImageReadyq.e<....IDATx..V=O.P.....u`.A.q...eU.....YW..q.UYHD.M.A.]:Xc4..X<.1....&..Ci.;..s.T./?bQF".q....@..G.O. .r^....q.j...4F.C.....ik.....".....r>.V..^}.H.u....g2...\t7....p.5.C...?..8.....IW...j.x._Ay-S)....bi...B..c.Yk@.....$.....$.@.F....X...B#...*9U.y.to%.m.u.2....Kp.;....b....N..@y..MkL.Fg.- %.~.....Cq.#W4J0.xP..R.+1..kdPm.kw...n.+B..d..J!.p....5..T..84..$..3..O5...m.SHmz..\.ULX._.q....r...f.....h8..g.4...0..|.o$..&....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\18338075[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, baseline, precision 8, 32x32, frames 3
Category:	downloaded
Size (bytes):	1015
Entropy (8bit):	7.449373336888139
Encrypted:	false
SSDEEP:	24:Q9YMa6M0XxDuLHeOWXG427DAJuLHenX3fAwWiLa8c5Ki7mJSFxDSJ:Q9YMabuETAtACLJclUSFxDSJ
MD5:	78A1B1B9A1B37076A5D9FB23E7701611
SHA1:	32B30651ACF4D1C9245C9F6FEFAF737EB1EA20D6
SHA-256:	AC5A17D0446DBE5FFE5983386AA11EF6F220A52B7FCF945C5B0327FB057CFA95
SHA-512:	BD6042653A74D3CA281A4020CCA696DFE394EC6AFC345F19548C28BC27162A82927B321F78A41AF3DC504BF27DCEE5595E7AC0C8F8F0E9ACD529E75D8ADAD 17
Malicious:	false
IE Cache URL:	http://https://avatars.githubusercontent.com/u/18338075?s=32&v=4
Preview:	..... $.' '',#..(7),01444.'9=82<.342.....2!.!2222222222222222222222222222222222222222222222222..... . .."..... ....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... ..w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?...u=ZO.$.S,V..*..... s....'..D..s$D.....]G.<...G3..$.....U.'R.|3...5.."R.....\.j.S.Q..-.;.t0t-O.....iq5.....O8.....Jb.!.....Q.[.>../...\.9. ..jxwQ...8.....,e.N.0..1S....x.4.n...H. ..>~?.....Z.....3..rp. l.t.* ...~.3$....I.....^_..\Yj....Qd...0.PA.0..cd....G..m..:...4.>..R.4.....e..''=...as.....v.s...e.=8.....V.!...J.L..K.*F.$.s.v.^.g.vvp.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\94-3cd1e0[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):	68375
Entropy (8bit):	5.370837839922446
Encrypted:	false
SSDEEP:	1536:gtV81ICDVRgJhAiUinqgDRQ7wYv6uxhBANIu:gv81+einqgD8Q
MD5:	53475B50CF354A3E5CCBB0740A2AE553
SHA1:	9166969D9B0D89321B6BD0A754E3DEE54C2B7B11
SHA-256:	EEA90E1F236FD6CED5D08C19B424BC7D36A1679C3B87B71C560365AED4888FF3
SHA-512:	D53A98168F82CFDCC02CEF55D73EE40D4F1D32EDB8AC85256182D88F3609FEEAB7A5186B4527BC7B5AA77CB06930E324C8A56CB49F3CC71E1A02D5B5394396 7
Malicious:	false
IE Cache URL:	http://https://www.microsoft.com/onerfstatics/marketingsites-neu-prod/mscomhp/_scrf/js/themes=default/78-6f121b/94-3cd1e0?ver=2.0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\94-3cd1e0[1].js	
Preview:	var awa,behaviorKey;define("jsllConfig",["rawJsllConfig"],function(n){return n});awa=awa||{};awa.isInitialized=!1;awa.verbosityLevels={NONE:0,ERROR:1,WARNING:2,INFORMATION:3};awa.behavior={UNDEFINED:0,NAVIGATIONBACK:1,NAVIGATION:2,NAVIGATIONFORWARD:3,APPLY:4,REMOVE:5,SORT:6,EXPAND:7,REDUCE:8,CONTEXTMENU:9,TAB:10,COPY:11,EXPERIMENTATION:12,PRINT:13,SHOW:14,HIDE:15,MAXIMIZE:16,MINIMIZE:17,BACKBUTTON:18,STARTPROCESS:20,PROCESSCHECKPOINT:21,COMPLETEPROCESS:22,SCENARIOCANCEL:23,DOWNLOADCOMMIT:40,DOWNLOAD:41,SEARCHAUTOCOMPLETE:60,SEARCH:61,SEARCHINITIATE:62,TEXTBOXINPUT:63,PURCHASE:80,ADDTOCART:81,VIEWCART:82,ADDWISHLIST:83,FINDSTORE:84,CHECKOUT:85,REMOVEFROMCART:86,PURCHASECOMPLETE:87,VIEWCHECKOUTPAGE:88,VIEWCARTPAGE:89,VIEWPDP:90,UPDATEITEMQUANTITY:91,INTENTTOBUY:92,PUSHTOINSTALL:93,SIGNIN:100,SIGNOUT:101,SOCIALSHARE:120,SOCIALLIKE:121,SOCIALREPLY:122,CALL:123,EMAIL:124,COMMUNITY:125,SOCIALFOLLOW:126,VOTE:140,SURVEYINITIATE:141,SURVEYCOMPLETE:142,REPORTAPPLICATION:143,REPORTREVIEW:144,SURV

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\97269d6d.site-ltr[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	431382
Entropy (8bit):	5.103554935637682
Encrypted:	false
SSDEEP:	1536:pY3syISLoGECJnMI8I02CN6prheetKf7AxS0EyrwkmWPI2b17Uxggvt/wNAx6VCa:pCnCeeetKfaLEfkmebfC1YLZpHMg
MD5:	7B59E6828815309A2BC59EFD694F493F
SHA1:	A8213B45F840CC5CD94B6632955874116F3CB5C0
SHA-256:	12375C8E126FDDA964F203C3E8183A5DF59E2054E1AF730DF5073024BF776D6A
SHA-512:	470BE09331B3032F17B63C1A0857D3747A0F89F8E4E65423282F4455E2B459ECB245A9F59C97B1E2C3F5673B0AF799A2C0C1C23B5BA2248D8BAA909C14DA8FA4
Malicious:	false
IE Cache URL:	http://https://docs.microsoft.com/_themes/docs.theme/master/en-us/_themes/styles/97269d6d.site-ltr.css
Preview:	/*! normalize.css v8.0.1 | MIT License | github.com/necolas/normalize.css */html{line-height:1.15;-webkit-text-size-adjust:100%}body{margin:0}main{display:block}h1{font-size:2em;margin:.67em 0}hr{box-sizing:content-box;height:0;overflow:visible}pre{font-family:monospace,monospace;font-size:1em}a{background-color:transparent}abbr[title]{border-bottom:none;text-decoration:underline;text-decoration:underline dotted}b,strong{font-weight:bolder}code,kbd,samp{font-family:monospace,monospace;font-size:1em}small{font-size:80%}sub,sup{font-size:75%;line-height:0;position:relative;vertical-align:baseline}sub{bottom:-.25em}sup{top:-.5em}img{border-style:none}button,input,optgroup,select,textarea{font-family:inherit;font-size:100%;line-height:1.15;margin:0}button,input{overflow:visible}button,select{text-transform:none}[type=button],[type=reset],[type=submit],button{-webkit-appearance:button}[type=button]::-moz-focus-inner,[type=reset]::-moz-focus-inner,[type=submit]::-moz-focus-inner,button::-moz

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\MeControl_mDEQjNo-v8fzxvfr-ss1Pw2[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):	17157
Entropy (8bit):	5.454494845618141
Encrypted:	false
SSDEEP:	384:Olj+5PpFCtfMaqMQYARsWa5hPwLkfbxc91Vn5W8fQzu1f+KxdQAz:OljEC/aghPo8O9lVT1f+Kx9z
MD5:	9831108CDA3EBFC7F3C6F7EBFACB353F
SHA1:	FD04337DE552F4E901CBC90A94154CB4979F0411
SHA-256:	54FCA076D07D891680EA1343C5526F923C9B762216F2F914FE82C5A48A1CB158
SHA-512:	B4E3955A8929166B8BC4CFFE4278973D160AFE4610CF04C8D1DAAF5106BB6FF4BA57A6F87C89777B3084F28D645B7B398429702543FA46DA4905F9A3FBBFE454
Malicious:	false
IE Cache URL:	http://https://logincdn.msauth.net/16.000/content/js/MeControl_mDEQjNo-v8fzxvfr-ss1Pw2.js
Preview:	function _iY(a){return a?true:a==0||a==false||a==""}function _Du(a,b){return _iY(a)?a:b}function _Bd(a){return a instanceof Array}function _BD(a){return "function"._g2(typeof a,true)}function _F(a){return typeof a=="string"}function _BE(a){return _iY(a)&&_F(a)&&a!=""}function strOrDefault(a,b){return _BE(a)?a:b}function _A2(a){if(!_F(a))return "";if(a.lastIndexOf(".")<0)return "";return a.toLowerCase().substr(a.lastIndexOf(".")+1,a.length)}function _A1(a){return document.getElementById(a)}var $J={_dW:false,_b:function(c,a){var d=null;if("img"._g2(c)&&_iY(a)){var g=_A2(a.src);if("png"._g2(g,true)&&!$F._mK())c="span"}var b=d;if("input"._g2(c,true)&&_iY(a)&&(a.name||a.type)){if(!$aE._i._g2(a.type)){var f=document.createElement("div");f.innerHTML='<input type="'+(a.type?a.type:"")+'" name="'+(a.name?a.name:"")+'" />';b=f.firstChild}else try{var e="<"+c;if(a.type)e+=' type="'+a.type+'"';if(a.name)e+=' name="'+a.name+'"';e+=">";b=document.createElement(e)}catch(h){b=d}if(_iY(b)){a.type=d;a.n

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\RE4qZxW[1].wdp	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG-XR
Category:	downloaded
Size (bytes):	18281
Entropy (8bit):	7.897319739476044
Encrypted:	false
SSDEEP:	384:I0s2DInUyFqiu1NM0QsOUVsaBLwybtzG7BsS5S76H0Z6kqA8XW8fKG:82DInUyFqRTM0Qc30y5eGkS7k0Z6kNDO
MD5:	15B38520FFCDE29D9CA14429F8F75C00
SHA1:	553E94DF0F843E573023E7337D4BBFE34908CF6E
SHA-256:	48BD2AE0048CB2AA05A12D39A54982363DA5FE0DBCEB87A36D2922B793381226
SHA-512:	45C5833CFB3E5CCB10ECEA0F1A593AB5634ED0F82FB672874BFA9D7D28743C4CAE377036996AD3D5D62980276EB2071ADA8B5031C431D822D9CCEAD5FC198A17
Malicious:	false
IE Cache URL:	http://https://img-prod-cms-rt-microsoft-com.akamaized.net/cms/api/am/imageFileData/RE4qZxW?ver=11cf&q=90&m=6&h=201&w=358&b=%23FFFFFFFF&l=f&o=t&aim=true

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\RE4qZxW[1].wdp	
Preview:	II.. ...$..o.N.K..=wv.....f.....$..B.....$..B.....F.....WMPHOTO..E.q.e..0....I,.6...`.....-..>.....`.I.....H ...T..=I..L...[g....\hM.E.oC.G ...'...u..x. ..\eRi.B.k.K1.ZV.1.Y.!.P.....B..r....-.)../...B..[.u...`6b..FK.1. j..(,.....Q.....6IR.m..n.U~.."....AtMa.C&^/...]E....inuI.b.i9VF..]h2.M..w.&M...P.g2\...8.J.&!t..(..0..$..]e|J.... .$....X .3D.FeM.} .3.1....6.1.S@.6\|.YKY{.y%E..z...K.9.Q..Z-5.I.PI..d...F2..ar..!.J".....K.LC..c$....JA.bzc...t.L.6J0.td..#..d..t.Z...../.....UJ....i..... ./..hz%$.(.....4X.HQ@.....q_.?.. +S.\.;i..-...J.F.....X\.Zz.{}8^.5.P.....K..@(Ey[.kicq..q.>.j.0.B...xm.j..$T..[....$..u...R"./.3.r%..n....."....."!.....`..3....(....O.....k.....$p."..t|0.Q.!z....&.a8....i..kd.....Y.....H.a.t....8CS .....H.*..4....._id7a.Vr1...u...G...$NUB*...x...e.Hjk..&...v/.. ....X.....o.X._. s..,g.....w....N.%,.g.}...D...r.q.?0V.N.@|0cF{.....U.Y.E

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\a4-539297[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):	4455
Entropy (8bit):	5.112562468544386
Encrypted:	false
SSDEEP:	96:vLyjQDkP7UnGGmabvws8hhuZAFguM86xmfkbXH/0RKZy:TyjQwjeGGmabvSPuWFguMWfkbv0RKZy
MD5:	DF1BDEC92A67C0C3554ADB2946ECF076
SHA1:	8BF9741EDAC3B1DB9816B6D6346DA8ED85C1FF99
SHA-256:	B11A0898FF527D53E543AD37065CDE4315C5DBBEC3FF7FF3ED1BE31EA4828978
SHA-512:	21E0D6C51906782ADF74BB4C2E0DD19E1B4A33B6593B399F3278F6B54E63F9D0182B67485DC0CB16ACFADBE13F6482CEFB9BA449B7C6AF7F7AED9D3FCE752 3C
Malicious:	false
IE Cache URL:	http://https://www.microsoft.com/onerfstatics/marketingsites-neu-prod/mscomhp/_scrf/js/themes=default/b7-5b4bf5/a4-539297?ver=2.0
Preview:	require(["jqReady!"],function(n){function a(n,t,i){i.setAttribute(o,"false");y();n.contentWindow.postMessage({action:"open"},t);e||(e=document.getElementById(w));e.style.display="none";e.getAttribute(o).toLowerCase()==="false"&&e.setAttribute(o,"true")}function b(){var n,r;t||(t=document.getElementById(u));i||(i=t.getAttribute(f));t||(t=document.getElementById(u));i||(i=t.getAttribute(f));n="";window._pageBITags&&window._pageBITags.pageTags&&(n=window._pageBITags.pageTags.pageName);r=t.getAttribute("data-lpcurl");t.contentWindow.postMessage({lppagename:n},i);t.contentWindow.postMessage({lpcurl:r},i)}function v(n){t||(t=document.getElementById(u));i||(i=t.getAttribute(f));t.contentWindow.postMessage({invite:n},i)}function y(){t||(t=document.getElementById(u));i||(i=t.getAttribute(f));var n=t.getAttribute("data-chatTopic");c||(c=t.getAttribute("data-isOfficeCommercial").toLowerCase()==="true"?"Office365":n?n:"Store");t.contentWindow.postMessage({action:"parentsize",Width:window.innerWidt

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\a96de1e1.conceptual[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	2758
Entropy (8bit):	5.003008557028622
Encrypted:	false
SSDEEP:	48:7ZS8Ji+rkeT9mP86VtgvaEbinJZn9aDvrfznGohoAg:48jQe3KtgPinXanLW7
MD5:	D7706CC0812D9EC240628DCBD347CC06
SHA1:	9D6BEC78AB2F62B866CD228E7F7344FF6FC4F673
SHA-256:	017C7FFA64C1935ED55F2EF613831F0E0985F95C2B8BE2297E1DC34BD3A26158
SHA-512:	19E9A6788F12C92B38E941D729DEDA7414C32BC6D754F51B19FAE48F7D9066C188CE302BBF98B8284CACB9DC72262F7A67BEF9B20C56F11976094846BFECC3 3
Malicious:	false
IE Cache URL:	http://https://docs.microsoft.com/_themes/docs.theme/master/en-us/_themes/styles/a96de1e1.conceptual.css
Preview:	audio,canvas,progress,video{display:inline-block;vertical-align:baseline}audio:not([controls]){display:none;height:0}template{display:none}small{font-size:80%}sub,sup{font-size:75%;line-height:0;position:relative;vertical-align:baseline}sup{top:-.5em}sub{bottom:-.25em}svg:not(:root){overflow:hidden}button{overflow:visible}button,html input[type=button],input[type=reset],input[type=submit]{cursor:pointer}button[disabled],html input[disabled]{cursor:default}button::-moz-focus-inner,input::-moz-focus-inner{border:0;padding:0}input{line-height:normal}input[type=checkbox],input[type=radio]{box-sizing:border-box;padding:0}input[type=number]::-webkit-inner-spin-button,input[type=number]::-webkit-outer-spin-button{height:auto}textarea{overflow:auto}optgroup{font-weight:600}a.nohref{cursor:pointer}.content .azureselector label{position:relative;float:left;height:28px;margin-right:.6em;font-size:.6em;font-weight:600;line-height:28px;text-transform:uppercase;letter-spacing:.5px;vertical-align:mid

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\ai.0[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	96705
Entropy (8bit):	5.228470338380378
Encrypted:	false
SSDEEP:	1536:EVpXOWPGHRGUvJEzxPNLgyLuG6XV3yV/QtJ+j1YeO4PFWYit:EVoWPGHRGUvJEzxOMQV3yV/ERaNWYit
MD5:	1DD63DE72CF1F702324245441844BE13
SHA1:	58A8BDCDCB398AF7DB424357DF70DF18E7B30E9D
SHA-256:	5201C813C37A4168CC5C20C701D4391FD0A55625F97EB9F263A74FB52B52FD0E
SHA-512:	532D1E907B433AB97785CF632D9637A957152BAF0BA57879C856CBAA469BFFECA22C4F99485679539944B27068D39E70F7D44282594F999142454DA57329A11B
Malicious:	false
IE Cache URL:	http://https://az416426.vo.msecnd.net/scripts/a/ai.0.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\ai.0[1].js	
Preview:	"use strict";var AI,Microsoft,__extends=this&&this.__extends||function(){var i=Object.setPrototypeOf||{__proto__:[]}instanceof Array&&function(e,t){e.__proto__=t}||function(e,t){for(var n in t)t.hasOwnProperty(n)&&(e[n]=t[n])};return function(e,t){function n(){this.constructor=e}i(e,t),e.prototype=null===t?Object.create(t):(n.prototype=t.prototype,new n)}}();function _endsWith(e,t){var n=e.length,i=n-t.length;return e.substring(0<=i?i:0,n)===t}!function(e){e.ApplicationInsights||(e.ApplicationInsights={})}(Microsoft||(Microsoft={})),function(e){var t;t=function n(){},(e.Telemetry||(e.Telemetry={})).Base=t}(Microsoft||(Microsoft={})),function(e){var t;t=function n(){this.ver=1,this.sampleRate=100,this.tags={}},(e.Telemetry||(e.Telemetry={})).Envelope=t}(Microsoft||(Microsoft={})),function(e){var t;(t=e.ApplicationInsights||(e.ApplicationInsights={}).Context||(t.Context={})}(Microsoft||(Microsoft={})),function(e){var t;(t=e.ApplicationInsights||(e.ApplicationInsights={})).Context||(t.Co

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\build-2020-background[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, 1792x300, frames 3
Category:	downloaded
Size (bytes):	86495
Entropy (8bit):	7.980072533330035
Encrypted:	false
SSDEEP:	1536:1pftTSq9wFAbpRAqHEq+IOBLHlV+ltBwqbarE6YX6Zn5atVVs7Fq/hgDZHtYTnAZ:1NtTD0IRHHQBL8irEJKfUVmBjDZHtYsZ
MD5:	C809D8089D9DD31796A30EE574D5C644
SHA1:	0B3209A6AE7DBE877C1D51991FB14D4F8F1CBD96
SHA-256:	A0B7463FB7A53B74472DF51680A6A864AA7D331766A851DE78A695576D632D96
SHA-512:	7B87ED1B86CB73AE84A0DDB991024FF45C82B4BE321935FB2609773FEF2FB4F4F85A75DA5B605483B528F170A6868B775EE28159919309215F7D2569BEE05716
Malicious:	false
IE Cache URL:	http://https://docs.microsoft.com/en-us/media/build_banner/build-2020-background.jpg?branch=main
Preview:	......JFIF......"..."*%%*424DD\....."..."*%%*424DD\....,...".....D..... {>..(q..[;...U...u..oX.b....."....."....A....#..~...V....vm.>1..A.....".Pj.."#....Q.....5.....E..~...m..w6...c4..x6...<?..{]..U@...@....@....h. ...7m.z..!..k.Z.f.ie.dq.+..@....U.j.+.21..h.A.$.W@.....;.O.....F..<...o.u9Y.,...V..g.j..4N.@@.... ....."..."..7O..@.A.....=.*NS.....(..+Z.EP..z.ET..X.&.....@.....x.....g..Z.oD.\'..V.x.^L...l.GR.tK.....<.....W/.u..D.....A...s..U..`.1\.9.:|.s..... +PPPF..4.T.h.]..r.P...@./h.B. ..d\-..C.}.O..9'...z.R..G.....KX.]}G.m..[..xG...u.>..Y.z.P..@..@.....W...LU....cj...*.....Th.....A@@PD.z*9.r5.RM..2.....u.....@..]ov....|..j.w.....g1.T..-...l.Z.tZK.b..E.....K.Z{...q.m..(.....f.u...dQ.TTF.8..\...8U..]?..x...X$.P.+UD..(.....M.....@..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\configreference[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	174
Entropy (8bit):	4.8072937684374155
Encrypted:	false
SSDEEP:	3:8ROFKGQIeNi1Xbvx9M84JxeCAIuREg7F6nmqDtptRHgDQIMf7SWFq:AYSI0MXLxu2CAIuh7FUppDHMQIC7SR
MD5:	20C479705FEA3F2DCCA48C6C2F13B04A
SHA1:	82794957E4EDC0B408A12FD4B405FE315FA25390
SHA-256:	65805B3F3D1F29A94E5F2A13EDD7628AA1A47BE6CECBCF1EC7887B7DD186F2A9
SHA-512:	E3145A055C3D6C4A14B85A84F0BF2673309B36C621E3EB2156F59FD1E1F558702145E75BD44384F97BA99DC3AA742792A942CEA5C90E7387083B8F465AEAA131
Malicious:	false
Preview:	<head><title>Document Moved</title></head>.<body> Object Moved This document may be found <a HREF="https://docs.microsoft.com/en-us/iis/configuration/">here</body>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\customers-raygun[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	3956
Entropy (8bit):	4.92135465261614
Encrypted:	false
SSDEEP:	96:Dps6s5PcdSYoU/RecylwVFXfc1GTdVGeaCqtr:1rdSEgcjz01GTdVo
MD5:	E912349E571C068AE6ADFA647D019820
SHA1:	D24FF0901F4714A6A35E13F29AA7E154A50485DF
SHA-256:	A9F97C4BE0CE319E33EF481E4BAFEF3CEBA6E9939465CB1E4AADE0046BF70949
SHA-512:	6543919F10E7EE9F3E48E2ACB5EC6DD2C372D1ABC3B26D437D53BEDD747D5C9E9F1BD24BA439AE9F64ACB7AAB9FDA4CD537ECA77E23F328C95C0ED727724D7FA
Malicious:	false
IE Cache URL:	http://https://dotnet.microsoft.com/static/images/redesign/customers-raygun.svg?v=qfl8S-DOMZ4z70geS6_vPOum6ZOUZcseSq3gBGv3CUk
Preview:	<svg viewBox="0 0 158 30" version="1.1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink">..<title>Raygun-logo</title>..<desc>Created using Figma</desc>..<g id="Canvas" transform="translate(-955 -1863)">..<g id="Raygun-logo">..<g id="Vector">..<use xlink:href="#path0_fill" transform="translate(955 1863.27)" fill="#283140"/>..</g>..<g id="Vector">..<use xlink:href="#path1_fill" transform="translate(1004.15 1863.4)" fill="#283140"/>..</g>..<g id="Vector">..<use xlink:href="#path2_fill" transform="translate(1031.47 1863)" fill="#283140"/>..</g>..<g id="Vector">..<use xlink:href="#path3_fill" transform="translate(1060.94 1863.27)" fill="#283140"/>..</g>..<g id="Vector">..<use xlink:href="#path4_fill" transform="translate(1089.06 1863.27)" fill="#283140"/>..</g>..<g id="Group">..<g id="Vector">..<use xlink:href="#path5_fill" transform="translate(983.661 1863.27)" fill="#283140"/>..</g>..<g id="Vector">..<use xlink:href="#path6_fill" transform="translate(997.321 1

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\customers-stackoverflow[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	7119
Entropy (8bit):	4.219022155456865
Encrypted:	false
SSDEEP:	96:Ez2zCYzeb/ShtRpVmo9Nfn3c4RDdhCLnChzjyXVBlwpU2XpJzDftx1u+0wetyVsb:SsCpSxfmo3n3cSDdhugjcTngfH1V+
MD5:	F3A9EA8E847F91CF015789C507C34A57
SHA1:	11C070213EE596463877F7AAF22CDA5198622BC5
SHA-256:	5C3CE2B45BCEC4393A47CBE4FB8AFB0F162582DC5D5007D29938C4996FAB9B05
SHA-512:	225DBD074CAFC9C796F9C050B2911FC4E9E18023D2F14AE23AC8B4B8C4AA0846A15D8DDE8B1B5F44D0018F3FECC9EDE70272D0493BD21D67F6CF79FF0AB0474
Malicious:	false
IE Cache URL:	http://https://dotnet.microsoft.com/static/images/redesign/customers-stackoverflow.svg?v=XDzitFvOxDk6R8vk-4r7DxYlgtxdUAfSmTjEmW-rmwU
Preview:	<svg viewBox="0 0 204 40" version="1.1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink">..<title>StackOverflow-logo</title>..<desc >Created using Figma</desc>..<g id="Canvas" transform="translate(-175 -1858)">..<g id="StackOverflow-logo">..<g id="Vector">..<use xlink:href="#path0_fill" tran sform="translate(213.49 1869.94)" fill="#222426"/>..</g>..<g id="Vector">..<use xlink:href="#path1_fill" transform="translate(175 1883.72)" fill="#BCBBBB"/>..</g>..<g id= "Vector">..<use xlink:href="#path2_fill" transform="translate(182.113 1858)" fill="#F48024"/>..</g>..</g>..</g>..<defs>..<path id="path0_fill" d="M 7.60048 12.8136L 5.261 87 12.6188C 3.45919 12.4726 2.72838 11.7418 2.72838 10.5237C 2.72838 9.06211 3.84896 8.13641 5.94397 8.13641C 7.45432 8.13641 8.76979 8.47746 9.79293 9.30572L 11.1571 7.94153C 9.84165 6.86967 8.03897 6.38246 5.94397 6.38246C 2.87454 6.38246 0.633374 7.99025 0.633374 10.6212C 0.633374 13.0085 2.14373 14.2753 4.96955 14.5189L 7.35688 14.713

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\docons.225ca470[1].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), docons family
Category:	downloaded
Size (bytes):	24668
Entropy (8bit):	6.29473568075679
Encrypted:	false
SSDEEP:	384:hGPxZQfRmQ7gOzZm+4FWnM/XZYIFy3h8PuLU7/7iLQyAlEC:CzQfRmtUm+4AM9WWPuK/7iLQy3C
MD5:	CAFCFBC95173963CF09491C1AE7C8340
SHA1:	B06F06946765D7A14284BC643E69F9A1171A104D
SHA-256:	3C308094009479853D3FFD9EAE66F251F75A2F44629F1AF174977B1C5FD4FBE1
SHA-512:	15CFC9E4766EA911C1CD67F91F7CDA81780ACA85870FE01BF4CADCB7B48A21DE84D098F80D986AA89DF817C0509203A89402E7993BE8B3935A110B3B8255D181
Malicious:	false
IE Cache URL:	http://https://docs.microsoft.com/_themes/docs.theme/master/en-us/_themes/styles/docons.225ca470.eot
Preview:	\`..._.....LP.....?.....d.o.c.o.n.s.....R.e.g.u.l.a.r.....V.e.r.s.i.o.n. .1...0.....d.o.c.o.n.s.....0GSUB .%z...8...TOS/25.Z.....Vcmapj. .*.....>glyf*.g....8..FHhead.....6hhea.o.<.....$hmtx.....loca.....0....maxp...Y..... name..t...U....ypost.....W.....?...._.<.....A.....A..... .....M.....0.>..DFLT..latn.....liga.....D.9...>.D.9.....s.....PfEd.@...b.....(...A..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\dotnetmdl2-icons[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 13256, version 0.0
Category:	downloaded
Size (bytes):	13256
Entropy (8bit):	7.956885255902302
Encrypted:	false
SSDEEP:	384:HALh8vW4CAHNT7vsQUMLe9mAQX5iH2KlcF:BvkW8q69aMWKlS
MD5:	CB007C9EF525AC732418059FECA6BFA5
SHA1:	C4E55A78948C5CEC2B3ABE86768A608BFCFBB541
SHA-256:	B2CB1613A855B868A7D160031F988E8B8B1A343740D22566593AD0707531368D
SHA-512:	439564746E04669CF3FF96095088F0D99B0CB0ABE0EAAEDC77DD12C8594F59627CDBB11315C1DCC3EE1A497DBDD245E3896A358E5B8B96613ABEF36006E9B36
Malicious:	false
IE Cache URL:	http://https://dotnet.microsoft.com/static/fonts/dotnetmdl2-icons.woff
Preview:	wOFF.....3.....W.....OS/2...X...H...`JM.1VDMX.....^.qcmap.....v....pSc.cvt ... ... ...*....fpgm...@.....Y...gasp...0.....glyf...<..&M..=..i.head..,....5...6.] ..hhea..,.....$....hmtx..,....U.....loca..-<.....maxp..-..... .j._name..-....8....0..post..3(..... .Q.wprep..3<.....x...x.c`f..8.....u..1...4.f...$.....@ .....?.8.|...V...)00.... .Bx...S....._..m.m.m.m.m;e..y.~.....<p..a.0t.&...a.pa.0B.1..F...Q.ha.0F.3.....q.xa.0A.0L.&...l.da.0E.2L....i.ta.0C.1..f...Y.la.0G.3.....y.|a..@X0,....E.ba.DX2,....e.ra..BX1..V ...U.ja..FX3.....u.za..A.0l.6...M.fa.E.2l....m.va..C.1..v...].na..G.3.....}.~a.p@80.....C.a..pD82.....c.q..pB81..N...S.i..pF83.....s.y..pA.0\.....K.e..pE.2\....k.u..pC.1..n...[.m..pG.3..... {.}...@x0<.....G.c...Dx2<....g.s...Bx1..^...W.k...Fx3.....w.{...A.0|.>...O.g...E.2|....o.w...C.1..~..._.o..08.....?..0$.....x.c```b`d....f0+.....,.....,L!@z.C..T. ..A.9.s..2....<.~..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\downloads[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\downloads[1].css	
Category:	downloaded
Size (bytes):	33079
Entropy (8bit):	5.137551698888126
Encrypted:	false
SSDEEP:	384:qv0SxqEe57H96I/7+/sBC3nn5A9Rbs2pw5WWIP2yEsAqSl3cvNIjwSfTvNZ5wa1O:qv0S0Eea0M35I4oWI6wNITrpoY2
MD5:	9C0008E9C83675860632C0419649AD20
SHA1:	247BDC0D5C6E5B74AB9371647E3236290F9D3007
SHA-256:	2E53EB78F873CA5D27E00E76FF4E2AD984E4AB0BE0AA007F13BCE69AA9486335
SHA-512:	59E226FBA1BA79A3200C930155AAD76D8CD05AA1AB6F333F7D311201646D6F9CD61B618329DA2F3EB5256A420B2050A057590D751AE1840F69523C6BA1A70D32
Malicious:	false
IE Cache URL:	http://https://www-iis.azureedge.net/v-2021-01-05-01/css-bundle/downloads.css
Preview:	html,body,div,span,applet,object,iframe,h1,h2,h3,h4,h5,h6,p,blockquote,pre,a,abbr,acronym,address,big,cite,code,del,dfn,em,img,ins,kbd,q,s,samp,small,strike,strong,sub,sup,tt,var,b,u,i,center,dl,dt,dd,ol,ul,li,fieldset,form,label,legend,table,caption,tbody,tfoot,thead,tr,th,td,article,aside,canvas,details,embed,figure,figcaption,footer,header,hgroup,menu,nav,output,ruby,section,summary,time,mark,audio,video{margin:0;padding:0;border:0;font-size:100%;font:inherit;vertical-align:baseline;background:transparent}body{line-height:20px;height:100%}ol,ul{list-style:none}table{border-collapse:collapse;border-spacing:0}caption,th,td{text-align:left;font-weight:normal;vertical-align:middle}q,blockquote{quotes:none}q:before,q:after,blockquote:before,blockquote:after{content:"";content:none}a img{border:none}article,aside,details,figcaption,figure,footer,header,hgroup,menu,nav,section,summary{display:block}html{height:100%;overflow-y:scroll}body{background:#fff;font:14px/24px 'Segoe UI',Tahoma,Ari

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\errorPageStrings[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	4720
Entropy (8bit):	5.164796203267696
Encrypted:	false
SSDEEP:	96:z9UUiqRxqH211CUIRgRLnRynjZbRXkRPRk6C87Apsat/5/+mhPcF+5g+mOQb7A9o:JsUOG1yNlX6ZzWpHOWLia16Cb7bk
MD5:	D65EC06F21C379C87040B83CC1ABAC6B
SHA1:	208D0A0BB775661758394BE7E4AFB18357E46C8B
SHA-256:	A1270E90CEA31B46432EC44731BF4400D22B38EB2855326BF934FE8F1B169A4F
SHA-512:	8A166D26B49A5D95AEA49BC649E5EA58786A2191F4D2ADAC6F5FBB7523940CE4482D6A2502AA870A931224F215CB2010A8C9B99A2C1820150E4D365CAB28299
Malicious:	false
IE Cache URL:	res://ieframe.dll/errorPageStrings.js
Preview:	.//Split out for localization...var L_GOBACK_TEXT = "Go back to the previous page.";..var L_REFRESH_TEXT = "Refresh the page.";..var L_MOREINFO_TEXT = "More information";..var L_OFFLINE_USERS_TEXT = "For offline users";..var L_RELOAD_TEXT = "Retype the address.";..var L_HIDE_HOTKEYS_TEXT = "Hide tab shortcuts";..var L_SHOW_HOTKEYS_TEXT = "Show more tab shortcuts";..var L_CONNECTION_OFF_TEXT = "You are not connected to the Internet. Check your Internet connection.";..var L_CONNECTION_ON_TEXT = "It appears you are connected to the Internet, but you might want to try to reconnect to the Internet.";....//used by invalidcert.js and hstscerterror.js..var L_CertUnknownCA_TEXT = "Your PC doesn\u2019t trust this website\u2019s security certificate.";..var L_CertExpired_TEXT = "The website\u2019s security certificate is not yet valid or has expired.";..var L_CertCNMismatch_TEXT = "The hostname in the website\u2019s security certificate differs from the website you are trying to visit.";..var L

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\favicon[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 6 icons, 128x128, 16 colors, 72x72, 16 colors
Category:	downloaded
Size (bytes):	17174
Entropy (8bit):	2.9129715116732746
Encrypted:	false
SSDEEP:	24:QSNTmTFxg4lyyyyyyyyyyyyyio7eeeeeeeeekzgsLsLsLsLsLsQZp:nfgyyyyyyyyyyyyynzQQQQQO
MD5:	12E3DAC858061D088023B2BD48E2FA96
SHA1:	E08CE1A144ECEAE0C3C2EA7A9D6FBC5658F24CE5
SHA-256:	90CDAF487716184E4034000935C605D1633926D348116D198F355A98B8C6CD21
SHA-512:	C5030C55A855E7A9E20E22F4C70BF1E0F3C558A9B7D501CFAB6992AC2656AE5E41B050CCAC541EFA55F9603E0D349B247EB4912EE169D44044271789C719CD0
Malicious:	false
IE Cache URL:	http://https://c.s-microsoft.com/favicon.ico?v2
Preview:	.............h(..f...HH...........(..00......h....6.. ....=..............@..........(....A..(....................(....................................."P..."" ...333333333333333333333333333333333"" ...333333333333333333333333333333"" ...333333333333333333333333333333"" ...333333333333333333333333333333"" ...333333333333333333333333333333"" ...333333333333333333333333333333"" ...333333333333333333333333333333"" ...333333333333333333333333333333"" ...333333333333333333333333333333"" ...333333333333333333333333333333"" ...333333333333333333333333333333""

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\fb[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 4-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	191
Entropy (8bit):	6.138769124777432

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\fb[1].png	
Encrypted:	false
SSDEEP:	3:yionv//thPl9vhSFIfQfF7+SOIUdnJ50TBty2VjLKvAkx5zVO/pZzgTtWOKr4o3Z:6v/lhPIFIfK5+SSdn/0THy2VXKYkbzVE
MD5:	66E880958F835D468E7D4AF413E51736
SHA1:	AF2D794E61EB4501B4F2BA8B89089F0A802FF980
SHA-256:	25AA33A7BA0D9E1DE4258759BE8B42B9C16E2F59182AA58C47BDBB743CFF3B57
SHA-512:	089DBEF8347D7BF240EF080E76987AFFFD6101BF4F4D9342764A751809E49FEC8AEEE2EFEA30EEF0B8EE902EE30176301A53F1445A1A43132A88D4D5D33E0EE2
Malicious:	false
IE Cache URL:	http://https://www-iis.azureedge.net/v-2021-01-05-01/images/fb.png
Preview:	.PNG........IHDR................R...*PLTE:X.:X.:X.Fb._w.k..x.........................x....tRNS..".m...BIDAT..c.R..E.%(.3.+Z!..7 ..;.!...P5.. ...7Z...w....goNAUC...a(..rA#.........IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\free-code-editor-tools-bot-desk[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	17676
Entropy (8bit):	4.8364316824517815
Encrypted:	false
SSDEEP:	192:FpYIDA2zwLVlacto3Z9fMLTZpmefyPRFpBXxUIGNiGK0JUtgvJGbiIVETcir:FrkThltonfKmeaPL6UmHIVWr
MD5:	097D8293E9DD0C8A7246E7F008CFAB70
SHA1:	303F0E2C4C7A98C64949B3CFE89796EC650BF0E9
SHA-256:	596203A1C736D5010E78B8D3F63A1F668B1117B2A1A9E19C1AD690AF6641ED31
SHA-512:	8F70FD1F188EF95F9E0BE3CC89C5C3030FB57395FBAFCB6425FF1DA278205B2D8BB495E6D6CE2A0A16D94BAB68C8D907BFA66B5649DE51A8510F20E334C62AC4
Malicious:	false
IE Cache URL:	http://https://dotnet.microsoft.com/static/images/illustrations/free-code-editor-tools-bot-desk.svg?v=WWIDocc21QEOeLjT9jofZosRF7KhqeGcGtaQr2ZB7TE
Preview:	<svg width="636" height="300" viewBox="0 0 636 300" fill="none" xmlns="http://www.w3.org/2000/svg">..<path d="M557.81 248.32L545.05 131.49L533.72 138.4L553.62 248.27L557.81 248.32Z" fill="#C8C6C4"/>..<path d="M91.7399 258.17L86.9299 258.11L103.65 137.26L118 136.34L91.7399 258.17Z" fill="#C8C6C4"/>..<path d="M 125.62 238.91L147.69 134.51L135.06 136.01L121.44 238.86L125.62 238.91Z" fill="#C8C6C4"/>..<path d="M528.91 267.45L533.72 267.51L519.87 140.78L505.05 1 39.5L528.91 267.45Z" fill="#C8C6C4"/>..<path d="M527.81 142.94L562.98 123.01L563.72 111.81L527.94 132.17L527.81 142.94Z" fill="#848484"/>..<path d="M527.94 132.17L563.72 111.81L142.48 111.79L82.8699 129.05L83.7799 129.86L527.94 132.17Z" fill="#B2B2B2"/>..<path d="M82.6499 140.14L527.81 142.94L527.94 132.17L82 .8599 129.03L82.6499 140.14Z" fill="#848484"/>..<path d="M127.17 275.34L121.39 274.41L140.45 197.03C141.69 191.98 145.79 188 150.88 186.89L178.58 180. 85C181.36 180.25 184.2 180.77 186.57 182.32C188.94 183.87 190.55 186.25 191.11 1

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\iis-new-logo[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 94 x 70, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	1715
Entropy (8bit):	6.079695372617734
Encrypted:	false
SSDEEP:	24:SF1h8yxQumhpBt2BfWwQMGdlIa4HPddikAm5NJIBB7DLO:SLhDtMB/1MGdl14FqGvIBNDLO
MD5:	0456E8EAC54EDA32F6674DE66A81175D
SHA1:	60B4AF4696CF5CA16088811795A5A61B3CD985B4
SHA-256:	B3D431B09ABCF901FFC40EE7DE5EC9183DAC26B66EE0BBB8306824A858A8178C
SHA-512:	716F999A835206814228E8C77217DB4EDDC3D58772C11C0536DC429747E494456C3CCF40D89E460BE0324CBF5410B5125B118CC4BDB111E02CA99AB9007870B
Malicious:	false
IE Cache URL:	http://https://login-iis.azureedge.net/resources/v-2021-01-05-001/iis/style/images/iis-new-logo.png
Preview:	.PNG........IHDR...^...F.....r.....mPLTE......sss333sssssssssssssss333sss333sss333333ssssss333ssssss333ssssssssssss333333ssssssssssssssssssssssssssssss sssssss333sss333sssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss333ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss333ssssssssssssssssssssssssssss333sssssssssssssssssssssssssssssssss ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss ssssssssssssssssssssssssssss333ssssssssssss333sss....P"......q.......tRNS...@Q...`.... ....p0W..0.."M...L..P.!....9.8.......^./..R...1.....E.....P,..).....>....A..k....%[.?=...w..U.... ...]..G.b..V.. .SN..J......o$CY....O*T...5.B..:Fi.K.(.;.I{&....#.r.H5....,IDATx^...o....a.@CHh ...P..B...K.....&......?.2.;....v.2.v...9W....\|.&..M...M..TC..5.LU!..~..Y^Z....f.6......p$.!.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\iisstart[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 960 x 600, 8-bit/color RGB, non-interlaced
Category:	downloaded
Size (bytes):	99710
Entropy (8bit):	7.978141895886589
Encrypted:	false
SSDEEP:	1536:2y7Nz3UKkH95ZxQOOqKUa72n7QnTfv8+W4DK6TgHYou463gJLuz04Iqm4D7CaeJT:zV3U9HjfGaEnTNW4cHLJL14gMmPp
MD5:	7558B529A6A427F886EC405A097EC6FE
SHA1:	FE577840A48D2DCF4EF85500CB0C513CF55D7DD3
SHA-256:	5CD971D318349C4644488D55EDB1E7357DAD8AA3743BEF74B84C302580E37D82

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\iisstart[1].png	
SHA-512:	E2E1E4147D431393D38AD3E567938E54DF2AA9980C5324C859F3D474DABE86BD1CF9866D75E7956DF065AB35106804032C8585E15FD3C047212909EDD6EB896A
Malicious:	false
IE Cache URL:	http://https://sn.webrootcloudav.com/iisstart.png
Preview:	.PNG.....IHDR.....X.....''..V....gAMA.....a.....pHYs.....u.....tEXtSoftware.Paint.NET v3.5.100.r.....IDATx^...`...p.NHH...{/..C .....{.W.E:H..Q..D....X.a.....'.....y..w.3.g..9_...G.....x.....e.....0.....^.....#x.....e.....0.....^.....#x.....e.....0.....^.....#x.....e.....0.....^.....#x.....u.....7.....O...../..Cd?...._.f.]..8...+_?.....aj..]...../.....6.....c.oz.].|.[t....)....w.....r..}.c..>.....0.....e.....t.....0^.....r.....)X3}..o.K_S..02.....UVI.._.[tM.p..].-....;<.^.....G....?..;....8.#...A....my.{.e.....^.;.~.sq..L.3@.x.;Z.<..V/.....KTy..[V./..._.._R7.7.....}.iu&]:.....b...;.....<$.\v...M..h....+}f\...>.....r....|...;.....f?....._..Gz..?r..r../.-.}.O*.8.Z.....e...u&]...N.....ow.<....U/...yW.....C.Bo..X=.....o.r....4y.....J..~.w|.....K...a/.{]..7q.....^...?h...43..GG.....7.#.)..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\jquery-3.3.1.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	86929
Entropy (8bit):	5.289492706499139
Encrypted:	false
SSDEEP:	1536:aLiBdiaWLOczCmZx6+VWuGzQNOzdn6x2RZd9SEnk9HB96c9Yo/NWLbVj3kC6ta:+kn6x2xe9NK6nC6E
MD5:	378087A64E1394FC51F300BB9C11878C
SHA1:	0C3192B500A4FD550E483CF77A49806A5872185B
SHA-256:	4FE68FA216176E6D1F4580E924BAFECC9F519984ECC06B1A840A08B0D88C95DE
SHA-512:	9A2C70516EA0C8C37C7F072F214DE0AFD5DDEB643C6B5D3FA8ADE3EF8D2CE40BDF8B1B1194BAD296E9075562701EE7DAE48B18144B1CD2D735328BE5A3AC0BE6
Malicious:	false
IE Cache URL:	http://https://www.microsoft.com/onerfstatics/marketingsites-neu-prod/_h/46c44584/coreui.statics/externalscripts/jquery/jquery-3.3.1.min.js
Preview:	/*! jQuery v3.3.1 | (c) JS Foundation and other contributors | jquery.org/license */..!function(e,t){"use strict";"object"==typeof module&&"object"==typeof module.exports?module.exports=e.document?t(e,!0):function(e){if(!e.document)throw new Error("jQuery requires a window with a document");return t(e)}:t(e)}("undefined"!=typeof window?window:this,function(e,t){"use strict";var n=[],r=e.document,i=Object.getPrototypeOf,o=n.slice,a=n.concat,s=n.push,u=n.indexOf,l={},c=l.toString,f=l.hasOwnPropertyy,p=f.toString,d=p.call(Object),h={},g=function e(t){return"function"==typeof t&&"number"!=typeof t.nodeType},y=function e(t){return null!=t&&t===t.window},v={type:!0,src:!0,noModule:!0};function m(e,t,n){var i,o=(t=t||r).createElement("script");if(o.text=e,n)for(i in v)n[i]&&(o[i]=n[i]);t.head.appendChild(o).parentNode.removeChild(o)}function x(e){return null==e?e+"":"object"==typeof e||"function"==typeof e?l[c.call(e)]||"object":typeof e}var b="3.3.1",w=function(e,t){return new w.fn.init(e,t)}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\jsll-4[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):	65764
Entropy (8bit):	5.1621969217546715
Encrypted:	false
SSDEEP:	1536:LDh5jaj3z0T+dFNl8A8WhhWuC56bXV1eKuMTg:vzZKFNnC56bXV1g
MD5:	211E123B593464F3FEF68F0B6E00127A
SHA1:	0FAE8254D06B487F09A003CB8F610F96A95465D1
SHA-256:	589303CA15FBA4FE95432DBB456FF614D0F2AD12D99F8671F0443A7F0CF48DFF
SHA-512:	DAD54D7941A7588675EA9DD11275A60FB6290E1582D1C7A4ACB50642AF3C2A4AA35E32EDD8FA9DD01CE7FD777247D2706D5672A201633BF918B525936E93B14
Malicious:	false
IE Cache URL:	http://https://docs.microsoft.com/static/third-party/jsll/4.3.4/jsll-4.js
Preview:	(function () {.. var awa = awa || {}, behaviorKey; awa.isInitialized = !1; awa.verbosityLevels = { NONE: 0, ERROR: 1, WARNING: 2, INFORMATION: 3 }; awa.behavior = { UNDEFINED: 0, NAVIGATIONBACK: 1, NAVIGATION: 2, NAVIGATIONFORWARD: 3, APPLY: 4, REMOVE: 5, SORT: 6, EXPAND: 7, REDUCE: 8, CONTEXTMENU: 9, TAB: 10, COPY: 11, EXPERIMENTATION: 12, PRINT: 13, SHOW: 14, HIDE: 15, MAXIMIZE: 16, MINIMIZE: 17, BACKBUTTON: 18, STARTPROCESS: 20, PROCESSCHECKPOINT: 21, COMPLETEPROCESS: 22, SCENARIOCANCEL: 23, DOWNLOADCOMMIT: 40, DOWNLOAD: 41, SEARCHAUTOCOMPLETE: 60, SEARCH: 61, SEARCHINITIATE: 62, TEXTBOXINPUT: 63, PURCHASE: 80, ADDTOCART: 81, VIEWCART: 82, ADDWISHLIST: 83, FINDSTORE: 84, CHECKOUT: 85, REMOVEFROMCART: 86, PURCHASECOMPLETE: 87, VIEWCHECKOUTPAGE: 88, VIEWCARTPAGE: 89, VIEWPDP: 90, UPDATEITEMQUANTITY: 91, INTENTTOBUY: 92, PUSHTOINSTALL: 93, SIGNIN: 100, SIGNOUT: 101, SOCIALSHARE: 120, SOCIALLIKE: 121, SOCIALREPLY: 122, CALL: 123, EMAIL: 124, COMMUNITY: 125, SOCIALFOLLOW: 126, VOTE: 140

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\login[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with CRLF, LF line terminators
Category:	downloaded
Size (bytes):	17675
Entropy (8bit):	4.704627565383167
Encrypted:	false
SSDEEP:	384:UQ7DWeqxqS6KxvxUeuTCAQfHmoKCl73M/VdKiv:HEpXRmLTJQuon73Mt/
MD5:	9642D7C0AA115BF581F0411731C962CE
SHA1:	6C74EC1B70887B0E5B6AF35C09B37D48DB574FF5
SHA-256:	2BF76D297EC3F7ED1147CD4F0D361CF394AECCF55000EC70B6C19C2F01F09EA7
SHA-512:	21392F873631A973ED5CC658A367A0B7DDE86AF3F7DCE2CCBC7D6029D1481F51CBB92A342D6683D13949C75CBEA2612CD746EC9CD4D3DA1BFB68464596E945

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\login[1].htm	
Malicious:	false
IE Cache URL:	http://https://login.iis.net/account/login?ReturnUrl=https://www.iis.net/
Preview:	..<!DOCTYPE html>..<html lang="en">..<head>.. build date: Wed, 10 Feb 2021 16:45:37 GMT -->.. <title>Login | The IIS.NET Site</title>.. <meta name=" keywords" content="Microsoft IIS.NET" />.. <meta name="description" content="Home of the Microsoft IIS.NET community. Post to the forums, read IIS.NET blogs and learn about IIS.NET." />.. <meta name="author" content="Microsoft IIS.NET Team" />.. <meta content="text/html; charset=UTF-8" http-equiv="Content-Type" />.. <meta http-equiv="X-UA-Compatible" content="IE=10,chrome=1" />.. <meta name="viewport" content="width=device-width, initial-scale=1.0" />.. <link href="/f avicon.ico" rel="shortcut icon" />.... <link href="https://login-iis.azureedge.net/resources/v-2021-01-05-001/iis/style/css-bundle/common.css" rel="stylesheet" type="t ext/css" media="all" />.... [if lte IE 9]>.. <script src='<script src='https://login-iis.azureedge.net/resources/v-2021-01-05-001/scripts/html5.js' type="text/javascr

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\main[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):	30243
Entropy (8bit):	5.357437957641434
Encrypted:	false
SSDEEP:	768:6YBBgYl02Z+xwKLhBJRWVK3UokB/kdkNW7Hbr:6YBBgYl0gmhBJRV3ULiKOr
MD5:	BC1BE2131076F95E024C6DE13ED23E1A
SHA1:	1E8D791C6B8A2A0620DB05CC3FB51CA08D39B0FE
SHA-256:	09649C2446C57E9D40ABF380B1A87596FAFD4AD3303B563EE79F53D25D3151E6
SHA-512:	21879802BD8D5AA6EDD8C4D442000ABAFF29BB1F67B281FC08004F98D1BC95E00A07B42839A621EE49A6AA38C44DF4FDF6EA6E8A9D61A48CFB77F90310C6E5F
Malicious:	false
IE Cache URL:	http://https://www-iis.azureedge.net/v-2021-01-05-01/scripts-bundle/main.js
Preview:	../* Minification Error ..(40,83-84): run-time error JS1195: Expected expression: > ..(51,6-7): run-time error JS1195: Expected expression:) ..(53,70-71): run-time error JS1195: Expected expression: > ..(64,5-6): run-time error JS1002: Syntax error: } ..(71,5-6): run-time error JS1002: Syntax error: } ..(78,5-6): run-time error JS1002: S yntax error: } ..(80,7-15): run-time error JS1197: Too many errors. The file might not be a JavaScript file: document.. Minification Error */....$(document).ready(function () {.... $('#btn-search-submit').click(function () {.. var q = $('#txt-search').val();.. if (q.length) { window.location = searchDomain + '/search?searchterm=' + encodeURIComponent(q); }.. });.... $('#txt-search').keypress(function (e) {.. var keycode = (e.keyCode ? e.keyCode : e.which);.. if (keycode == '13') {.. e.preventDefault();.. $('#btn-search-submit').click();.. }.. });.... $(".user-profile a").on("click"

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\meBoot.min[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):	154427
Entropy (8bit):	5.55030568871564
Encrypted:	false
SSDEEP:	3072:9xTI1rl1dz269QXU9vfRYb6fGP9weLS1SP:3cVw6Kbx9FLS1SP
MD5:	C57C07C4674AE6F46031D21047D05989
SHA1:	A95BFD98F4698ED582A16395AC1FFD45961FD0E1
SHA-256:	DE6214A5477F1EE5BB72E015094923CAD51ED057A379BCEB817D82A9A1B0498D
SHA-512:	6ADBFB036C73F903DFA5F5C45B1B64B16E8791A57C23601A574B9CF804A452D03AFB446F8130A8F596382194FDFC1D752CA0821C35FE934BA1A31285F0865129
Malicious:	false
IE Cache URL:	http://https://mem.gfx.ms/scripts/me/MeControl/10.20321.2/de-DE/meBoot.min.js
Preview:	MeControlDefine("meBoot",["exports","@mecontrol/web-inline"],function(t,A){"use strict";var s=function(){},i={},u=[],p=[];function w(t,e){var n,r,o,i,a=p;for(i=arguments. length;2<i--;)u.push(arguments[i]);for(e&&null!=e.children&&(u.length||u.push(e.children),delete e.children);u.length;)if((r=u.pop())&&void 0!==r.pop)for(i=r.length;i--;) u.push(r[i]);else"boolean"==typeof r&&(r=null),(o="function"!=typeof t)&&(null==r?r="":"number"==typeof r?r=String(r):"string"!=typeof r&&(o=!1)),o&&n?a[a.length-1]+=r:a= ==p?a=[r]:a.push(r),n=o;var c=new s;return c.nodeName=t,c.children=a,c.attributes=null==e?void 0:e,c.key=null==e?void 0:e.key,c}function T(t,e){for(var n in e)t[n]=e[n];r eturn t}function d(t,e){t&&("function"==typeof t?t(e):t.current=e)}var e="function"==typeof Promise?Promise.resolve().then.bind(Promise.resolve()):setTimeout;var l=/acit|ex(?:s|g|n|p|$)|rph|ows|mnc|ntw|ine[ch]|zoo|^ord/i,n=[];function a(t){!t._dirty&&(t._dirty=!0)&&1==n.push(t)&&e(r)}function r(){for(var t;t=n.pop();)t

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\me[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	10320
Entropy (8bit):	5.437274504488252
Encrypted:	false
SSDEEP:	192:DwD4z1n+7Xr+cHEzFQD6Ds35b05e58ITZSTXh7gk0yi4BKOSmfn408:Mv7XrUJds35bd8cA3AN
MD5:	78787C9E738C3858DBA1CEA96C7AE2C8
SHA1:	ED5C60BE97D18758A0899BBF105C66850D6EF471
SHA-256:	3C4C17E219416782F720DA207E3F26777EFE57CC10AA57403C128039C76A7954
SHA-512:	5BB17BB67597ABA15159E929080BAC35CDAD238BED249168BFDF5A8C561DC2DE4AB41D81736162094EE1F7C987C500197AB7D6AB6D4EAA7B22F96211F02573D
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\me[1].htm	
Preview:	Copyright (C) Microsoft Corporation. All rights reserved. --><!DOCTYPE html> ServerInfo: BY1PEPF00001D6C 2021.02.19.22.59.33 LocVer:0 --> PreprocessInfo: azbldrun:AzBuildW2-Ha12, 2021-02-19T22:46:23.7548280-08:00 - Version: 16,0,28941,7 --> RequestLCID: 1033, Market:EN-US, PrefCountry: US, LangLCID: 1033, LangISO: EN --><html dir="ltr" lang="EN-US"><head><meta http-equiv="Content-Type" content="text/html; charset=utf-8"/><base href="https://login.live.com/pp1600/"/><noscript><meta http-equiv="Refresh" content="0; URL=https://login.live.com/jsDisabled.srf?mkt=EN-US&lc=1033&uaid=9784ffe4db8a4aed958ba39b47f09d46"/>Microsoft account requires JavaScript to sign in. This web browser either does not support JavaScript, or scripts are being blocked. To find out whether your browser supports JavaScript, or to allow scripts, see the browser's online help.</noscript><title>Windows Live ID</title><meta name="robots" content="none" /><meta name="PageID" content=""/><meta

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\meversion[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	27555
Entropy (8bit):	5.2404828771738865
Encrypted:	false
SSDEEP:	768:KVY26BzK4ey2FvZ60dQCn16JD2BlRnusqer6tAH6teJuN:p2AzK4ey2FvZRdQ3JD2BXAY6tAH6teJc
MD5:	AFB51461A64156D02DA76A25055D03B0
SHA1:	E1CB9BF380B29DBA03362EB9F7AFFF1E723788CD
SHA-256:	BD5E9477632F9F7EB9DD4853793DE09C3DAED8676F17AC5BB4041C3C57358C21
SHA-512:	392540C0BF5BFA0B46A3B57A17C6BF944F133A4CDD3CFA98F2B73BB1AD11B40F9B6BA403EAF28AE26F5DD4A478427CA641279968CC197E805D7C4BB927BBF930
Malicious:	false
IE Cache URL:	http://https://mem.gfx.ms/meversion?partner=MSHomePage&market=de-ch&uhf=1
Preview:	window.MSA=window.MSA||{};window.MSA.MeControl=window.MSA.MeControl||{};window.MSA.MeControl.Config={"ver":"10.20321.2","mkt":"de-DE","ptn":"mshomepage","gfx":"https://mem.gfx.ms","dbg":false,"aad":true,"int":false,"pxy":true,"msTxt":false,"rwd":true,"telEvs":"PageAction, PageView, ContentUpdate, OutgoingRequest, ClientError, PartnerApiCall, TrackedScenario","remAcc":true,"main":"meBoot","wrapperId":"uhf","cdnRegex":"^(?:https?:\/\/)?(mem\\.gfx\\.ms(?!\\.)|controls\\.account.microsoft?(?:-int|-dev)?(\\.com)?(:[0-9]{1,6})|amcdn\\.ms(?:ft)?auth\\.net(?!\\.))","timeoutMs":30000,"graph":false,"aadUrl":"https://myaccount.microsoft.com","msaUrl":"https://account.microsoft.com/"};window.MeControl=window.MeControl||{};window.MeControl.Config={"ver":"10.20321.2","mkt":"de-DE","ptn":"mshomepage","gfx":"https://mem.gfx.ms","dbg":false,"aad":true,"int":false,"pxy":true,"msTxt":false,"rwd":true,"telEvs":"PageAction, PageView, ContentUpdate, OutgoingRequest, ClientError, PartnerApiCall, TrackedSce

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\microsoft-logo2[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 89 x 19, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	1152
Entropy (8bit):	7.755397690287432
Encrypted:	false
SSDEEP:	24:9HuefFHH8rU+B+V8WUBgcjDt8CmSIgYiOo+DJdc:ZXfFHHLV985jWlSROo+DJdc
MD5:	A9B90F3D5C63149938FDB40A76C135C2
SHA1:	E55DDEC6D81066452FA8D68FB27E6AA6AA397FF3
SHA-256:	254251FD421ABFD7966A41EC0251D5B6796C99362C7CF90C8E286A9D457543F1
SHA-512:	C5F7318B4EB3885E34A2C933E71B8667F1A6530ADAE689852B3A752538C619DD89AF668E2BEF21E716913F47AB095DF413984BB6CEB2B0790DCF49BC18277E38
Malicious:	false
IE Cache URL:	http://https://login-iis.azureedge.net/resources/v-2021-01-05-001/iis/style/images/microsoft-logo2.png
Preview:	.PNG.....IHDR...Y.....GIDATX...h.U...j.....&..RT....XF..[w,A.A..i.....%.[..(.m...[...F.i..:4s.....o|.7...<..<.....~.....a:.g..!.#....5.D.:.+++.O\-.....61H.t.....(.V"...l...X.~...;[.;.~..^.Ipt.8#Z...*...Y,p.x.?..Z1P..$Wv....Gp.x*..E.k.BT...=Y,r/.,#... .?.H.....st&...D...0!.Y..O.Gm.\|h.s...x.-.S...;...E...u.f..?.Blc..N\|.....g.>26./\|)..D~G.....n..i.F.....\|3.L.U..\|L.pND>L.M...]....8!..s..'&Qn....;..y.$...2yOf.-8Z..o.I<.m1b..3.5Q.By.e[..b...!.....p..V.X+.....,...w.8J.Z.....A..F4[.6..!.9T.....KG.....l...l$.....R..#N...l7..m.;_.. ..fQ...L.U{....H...W\.-.....f.B...f(..rr..h....N....K).....80M.e.n...".h....9.-.t.M.....7q..R.z1.6...'8.\|..6.<9...P.v@Hz.....K..N....I..\|....D..].I.O.=.k{?.-.'.....y....X..n'x.{\..5.K..Va.;..E\.Fd...<..F...]\|scm+.....X..."\|D...x..=...O.....U...m.....$.K....o.....9&.:...c.<^.90..^..SyG.bY...{....}?../.....|...._.{|Ow.....M....0...o....Q$..n.[...o%%...@8

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\mwfmdl2-v3.54[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 26288, version 0.0
Category:	downloaded
Size (bytes):	26288
Entropy (8bit):	7.984195877171481
Encrypted:	false
SSDEEP:	768:56JqQaQphRbTHiKNF5z/02h5KpJW3pPOA8Y9g/:gdTTH5XKpJWdH1W/
MD5:	D0263DC03BE4C393A90BDA733C57D6DB
SHA1:	8A032B6DEAB53A33234C735133B48518F8643B92
SHA-256:	22B4DF5C33045B645CAFA45B04685F4752E471A2E933BFF5BF14324D87DEEE12
SHA-512:	9511BEF269AE0797ADDF4CD6F2FEC4AD0C4A4E06B3E5BF6138C7678A203022AC4818C7D446D154594504C947DA3061030E82472D2708149C0709B1A070FDD0E
Malicious:	false
IE Cache URL:	http://https://www.microsoft.com/mwf/_h/v3.54/mwf.app/fonts/mwfmdl2-v3.54.woff

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\mwfmdl2-v3.54[1].woff	
Preview:	wOFF.....f.....D.....OS/2...X...H...`JM.FVDMX.....^.qcmap.....*.9cvt ...4... ...*....fpgm...T.....Y...gasp...D.....glyf...P..U5.....head..]....2...6.. .Chhea..]....$$...hmtx..]....ye'loca..^.....Gmaxp..`.... ... ./..name..`....8....]..Rpost..f..... .Q.wprep..f$.....x...x.c`.Pf.....:....Q.B3_dHc..`e.bdb... .`@..`...../9.|... V...)00...-.Wx...S....._..m.m.m.m.m;e..y.~.....<p..a.0t.&...a.pa.0B.1..F...Q.ha.0F.3....q.xa.0A.0L.&...I.da.0E.2L....i.ta.0C.1..f...Y.la.0G.3.....y.|a..@X0,.....E.ba.DX2,....e .ra..BX1..V...U.ja..FX3.....u.za..A.0l.6...M.fa.E.2l....m.va..C.1..v...].na..G.3.....}.~a.p@80.....C.a..pD82.....c.q..pB81..N...S.i..pF83.....s.y..pA.0\....K.e..pE.2\....k.u..pC.1..n...[. m..pG.3.....{.}...@x0<.....G.c...Dx2<....g.s...Bx1..^...W.k...Fx3.....w.{...A.0|.>...O.g...E.2|....o.w...C.1..~..._.o..08.....?..0$.....x...mL.U.....9.x.`[...&BF@X...V.h.Z..h. .....`n....[..U

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\social[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	112978
Entropy (8bit):	5.163861138977889
Encrypted:	false
SSDEEP:	1536:GV8Utc49kADAKlyvpkmO5KqqVkii7nmFMfW6znlLXAirhnlOc8Azngzhe9WOU0RM:slyvpklZYWtzkAzg
MD5:	AE0935FF464917159FE28FB684DE6BC3
SHA1:	ADFF2BFEA6BC0129E2634639EB89BB1CDC43A05D
SHA-256:	172BEB2DDE1857755325F5BA1E6F7A4212CA1439C9CA73FBC5FF81C35A5579BE
SHA-512:	408DD35EF31CACB16035609E8F2D3FF8C241B22112738B0EA97E99E8367BDC33D2601FD196AD29905215D8B1DC123E7057968388DEDD140395E88638AC3FD12
Malicious:	false
IE Cache URL:	http://https://www.microsoft.com/mwf/js/MWF_20201028_28422223/alert/autosuggest/contentplacement/contentplacementitem/flipper/flyout/glyph/heading/hero/heroitem/hyperlinkgroup/image/list/pagebehaviors/singleslidecarousel/skiptomain/social?apiVersion=1.0
Preview:	define("componentFactory",["require","exports","htmlExtensions","utility","stringExtensions","pageBehaviors"],function(n,t,i,r,u,f){"use strict";Object.defineProperty(t,"__esModule",{value:!0});var e=function(){function n(){}return n.create=function(t){for(var i,r=0,u=t;r<u.length;r++){if(i=u[r],!i.c&&!i.component)throw"factoryInput should has either component or c to tell the factory what component to create.Eg.ComponentFactory.create([{ c: Carousel] or ComponentFactory.create([component: Carousel])";n.createComponent(i.component||i.c,i)}},n.createComponent=function(t,r){if(t){var o=r&&r.eventToBind?r.eventToBind:"",f=r&&r.selector?r.selector:t.selector,s=r&&r.context?r.context:null,u=[],e=function(n,f,e){var a,c,l,o,h;for(a=r.elements?r.elements:f?i.selectElementsT(f,s):[document.body],c=0,l=a;c<l.length;c++)o=l[c],o?(o.mwfInstances||(o.mwfInstances={}),o.mwfInstances[n]?u.push(o.mwfInstances[n]):(h=new t(o,e),(!h.isObserving||h.isObserving())&&(o.mwfInstances[n]=h,u.push(h)))):cons

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\spot-azure-accessible-everywhere[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	40931
Entropy (8bit):	5.440091622520611
Encrypted:	false
SSDEEP:	384:nESaQ293NSyOnIQ/O0Ygi3jee+BgsyeN1VE3TAIu5PjR:naF93b8Ih0YgCee+Bgsymb0MIuL
MD5:	050B95DE4CC8FA06292E3F5EF78CFBE0
SHA1:	725270C8D323FA83BF3C353A745545A654C1AAD9
SHA-256:	0DB82E9EDE020C13D1DE4AF050283A40116840C634362B6049DAC1038A381930
SHA-512:	77936B4512ACDDB6EBAEF111F5E70F959A8C8DD402125021ED81AE9368792B6EFDB1B5BD6DA18A10E25299163C0831880349E798A81B25803D34E921AC906D7
Malicious:	false
IE Cache URL:	http://https://dotnet.microsoft.com/static/images/illustrations/spot-azure-accessible-everywhere.svg?v=Dbgunt4CDBPR3krwUCg6QBFoQMY0NitgSdrBA4o4GTA
Preview:	<?xml version="1.0" encoding="utf-8"?>.. Generator: Adobe Illustrator 24.3.0, SVG Export Plug-In . SVG Version: 6.00 Build 0) -->..<svg version="1.1" id="Layer_1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" x="0px" y="0px"... viewBox="0 0 636 300" style="enable-background:new 0 0 636 300;" xml:space="preserve">..<style type="text/css">....st0{fill:#FBC977;}....st1{fill:#57AA9A;}....st2{fill:#F7B548;}....st3{fill:#6BA8F1;}....st4{fill:#BDD8F9;}....st5{fill:#8065E0;}....st6{fill:#FFFFFF;}....st7{fill:#1572E0;}....st8{fill:#B0D1F7;}....st9{fill:#FFD590;}....st10{fill:#7FD5CA;}....st11{fill:#D8E8FB;}....st12{fill:#C2E8E3;}....st13{fill:#FFECCD;}....st14{fill:#FEDEA7;}....st15{fill:#D1C5F4;}....st16{fill:#70D6E0;}....st17{fill:#25BACA;}....st18{fill:#1BA1B5;}....st19{fill:#8A6FE8;}....st20{fill:url(#SVGID_1_);}....st21{fill:#522CD5;}....st22{fill:url(#SVGID_2_);}....st23{fill:url(#SVGID_3_);}....st24{fill:url(#SVGID_4_);}....st25{fill:url(#SVGID_5_);}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\swimlane-subscribe-to-news-tips[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	61984
Entropy (8bit):	5.513213775541559
Encrypted:	false
SSDEEP:	1536:64DTEm1Wo7f5iVM5j6hytfXtqoq5XIY2EnngAOu:6fyf5i82hy99jq5XsengAOu
MD5:	4CED8713C7634F173A8159C62403850D
SHA1:	70DA7DD9549BF78B5FE66F27021AD6304A751A5A
SHA-256:	B9CC82D9748343C98C9E378702807EC54A6D295021ACD0B0BBFCB96BF28CA8DE
SHA-512:	E0353E5231E425849B25C8C9F241B0FCE73D8445E09E0C43563775F484836C3D7F829B802BD5F51005104D0C5ABB06676B3DB1D662330A0B3E9A8107B5F78117
Malicious:	false
IE Cache URL:	http://https://dotnet.microsoft.com/static/images/illustrations/swimlane-subscribe-to-news-tips.svg?v=ucyC2XSDQ8mMnjeHAoB-xUptKVAhrNCwu_y5a_KMqN4

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\swimlane-subscribe-to-news-tips[1].svg	
Preview:	<?xml version="1.0" encoding="utf-8"?>.. Generator: Adobe Illustrator 24.3.0, SVG Export Plug-In . SVG Version: 6.00 Build 0) -->..<svg version="1.1" id="Layer_1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" x="0px" y="0px"... viewBox="0 0 636 300" style="enable-background:new 0 0 636 300;" xml:space="preserve">..<style type="text/css">....st0{fill:#FBC977;}....st1{fill:#57AA9A;}....st2{fill:#F7B548;}....st3{fill:#6BA8F1;}....st4{fill:#BDD8F9;}....st5{fill:#8065E0;}....st6{fill:#FFFFFF;}....st7{fill:#1572E0;}....st8{fill:#B0D1F7;}....st9{fill:#FFD590;}....st10{fill:#7FD5CA;}....st11{fill:#D8E8FB;}....st12{fill:#C2E8E3;}....st13{fill:#FFECCD;}....st14{fill:#FEDEA7;}....st15{fill:#D1C5F4;}....st16{fill:#70D6E0;}....st17{fill:#25BACA;}....st18{fill:#1BA1B5;}....st19{fill:#8A6FE8;}....st20{fill:url(#SVGID_1_);}....st21{fill:#522CD5;}....st22{fill:url(#SVGID_2_);}....st23{fill:url(#SVGID_3_);}....st24{fill:url(#SVGID_4_);}....st25{fill:url(#SVGID_5_);}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\tech-empower-results[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	28726
Entropy (8bit):	4.30530000010501
Encrypted:	false
SSDEEP:	384:RPIudZWISsGJjFBpJwoTEvwZpzXoSLxFTyG+LO0X+XTXm45DxCjY+hU/XRXNXSR+:xIudZH501KmTx9ysDMMzZ84R
MD5:	85F702FC1D9D3C72764939E19F224A6E
SHA1:	190A8153118A1B0E48F4B1D3FB0E7BDB2FA91034
SHA-256:	1210232E2981884D420EABA25DDED4D362A4EF084035E5EEC7006372FFE2852A
SHA-512:	5F6AFA95C26BB9A909C025261D89A491590A7A768A6546637F207A77AE373BAA831A358C36E34B01EEF6352D91B2FED53F7152C49BAF5A9C14A8B496CDDAE2F7
Malicious:	false
IE Cache URL:	http://https://dotnet.microsoft.com/static/images/redesign/shared/tech-empower-results.svg?v=EhAjLimBiE1CDquiXd7U02Kk7whANeXuxwBjcv_ihSo
Preview:	<?xml version="1.0" encoding="utf-8"?>.. Generator: Adobe Illustrator 25.0.0, SVG Export Plug-In . SVG Version: 6.00 Build 0) -->..<svg version="1.1" id="Layer_1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" x="0px" y="0px"... viewBox="0 0 636 300" style="enable-background:new 0 0 636 300;" xml:space="preserve">..<style type="text/css">....st0{fill:#3E8EED;}....st1{fill:#D1C5F4;}....st2{fill:#FFFFFF;}....st3{fill:#A3C9F6;}....st4{fill:#0064DA;}....st5{fill:#522CD5;}....st6{fill:#957EE6;}....st7{enable-background:new ;}....st8{fill:#605D5A;}..</style>..<g>...<circle class="st0" cx="320.2" cy="151.8" r="90.1"/>...<g>....<path class="st0" d="M159.3,93.8c-35.8,0-64.9,29.1-64.9,64.9s29.1,64.9,64.9,64.9s64.9-29.1,64.9-64.9.....C224.3,122.9,195.1,93.8,159.3,93.8z"/>...</g>...<path class="st0" d="M481.1,94.2c-35.8,0-64.9,29.1-64.9,64.9s29.1,64.9,64.9,64.9s64.9-29.1,64.9-64.9S516.9,94.2,481.1,94.2z"/>...<path class="st1" d="M276.6,164.6c-1.2-4.1-1.9-8.4-

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\twitter[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	475
Entropy (8bit):	7.450353829038362
Encrypted:	false
SSDEEP:	6:6v/lhPWhuBEFkuAa4ltxK+10Ws/qjL1HVs2Ss3c8D7oJQDbp5cbox/Ev19GO5AQM:6v/7OOSWMY001Hnq8PLcbOA41rDmY
MD5:	DED33F31216FCFB32F5DBD759BAA6524
SHA1:	381B7478B19DDCAFE989C0D8FF4B72A180566BC6
SHA-256:	6037E54BCA54475B36C472CBEF76CFF389480694A1316279BA528F787C4EABF8
SHA-512:	85BD9E3679A98CAA339457DCD923C0BA6119F272B0A3641C274EE284D47DA0E8B2FE1A23DF4456B9E35BA2E4DB5DFE15D17EF88AE35EAE11C27EA4DCCE79D711
Malicious:	false
IE Cache URL:	http://https://www-iis.azureedge.net/v-2021-01-05-01/images/twitter.png
Preview:	.PNG.....IHDR.....a....IDAT8.S=K.P...R.A...._. . .....n.NN...a[.a...b...."...bE..m^./...x..3-.....$.{.}.r\(.....@..\.<".....-.....a?EH....)...Y .0..0s..."....1.Hc..W.....9.G..g-...y...../..$...Vbyd.....*<o2FC..C.<...0X."......2.(.yBF}....C.C..iS.ZI.)X_....oUm.....?..~.z.w...),...\...&.Lz.K.v6.>.{...."......`!J.....\#]../a.$....|.*....,Qe.u.Y{.....|...S...2.....z9Q3.]4.c..V.t..C..f....c...k.x.....qi.~B.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\3605364[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 32 x 32, 8-bit/color RGB, non-interlaced
Category:	downloaded
Size (bytes):	2596
Entropy (8bit):	7.889468153252516
Encrypted:	false
SSDEEP:	48:08OJtGoudNsqcgwV/AYfuW9WJxuHDHPxnYCwh+KnzOfxIjyUtSadcEKTWr5:0bJDEbnwRAYWHxsPqxznjTtSaGEKqr5
MD5:	68162E7BC2979EF0351DFAECF3320FE1
SHA1:	1B4697E74AE1D11FC28BDB0748A001BCB90EA4EE
SHA-256:	B2911231AE957FFA2C8E49C856C8853C63339CCF855199238E8B62146BAA4748
SHA-512:	A9A07E927480F2A4F5FB2022944115A21B63623B093149893398942DAB483D79B70CB88F67269411BCD97F261ED99F71E53B7492016320446C9318991DC24361
Malicious:	false
IE Cache URL:	http://https://avatars.githubusercontent.com/u/3605364?s=32&v=4
Preview:	.PNG.....IHDR... ... .IDATx...I.]W^..x.w..z...9.G.....(.P....Z-5...,z..5... .Bb.B...E@....E.N'1e.;..qUjxC...{w>3z.[..H.H....9....WY..O".a.....4k8..:;.C'...,...I.....j.B..x7^....UQ..@.-.".(...d.W..._.6...Y..W\HB...2...g..x.....QJ.%.Z;....JA..w.....NQ1.1..b..sq...~..::.k.c%...;.....S2>.on...E.T.....4...Mf..... !.!T2.....F..,)..,.....o6...Z).I<.ru.k.$.A.b.r..J.....h.-..%SB.)..&.d.S'J..z&..{u3.B..k>.L...$..0L...G.....B==_b#.1.!m.1.....yer6.R.....1f.'.+C.....0A. x~r.....?..q^T.m'9..L...".4.>{...Z.H0.z.Vt1.....^[[.:....;...N`[.4.f#.T.'.....n.C..d)S.....h.%...TJJ.....\...v.....<. .h...M.uX.fE..y..7...k.I.)&..*+8.J(.n...yR&9..`...Y....).sc}...G..Og....wn....qtx6.^.s..bE.?.....yaS.....?.....Q.B.....g....<.zV.d..-....c.....h>.1...m...-T.Rj.o..x~4.e. .i...#.BH..=.y..h..h2;:...O...C..d.L.....k.....G.Ac.$...x) .[Y.|s<n{..b...X....YY]..{.g..:=[..q.V...u...?~8...2.,..[..z../.}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\38636870[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, baseline, precision 8, 32x32, frames 3
Category:	downloaded
Size (bytes):	947
Entropy (8bit):	7.422493794081961
Encrypted:	false
SSDEEP:	24:Q9YMa6M0XxDuLHeOWXG427DAJuLHenX33ukODI0QfmdiU:Q9YMabuETAMkhfmd/
MD5:	C9394571BA067735E872E9A625786FD4
SHA1:	94FAAE199C043693EA20B49B6E38A3D6F21A2D95
SHA-256:	C8CAF78A202DDEDE63AC571964D33CE0401B2615BF40824D68090DD17537895C
SHA-512:	72E304374F888E4919AAB0419748ECDA29F1DD81C648B46142E16270F28FDFB6BE8CC86092594253EDC04EC78ED276164CF7E296A2217A7113B4835823C2C9F0
Malicious:	false
IE Cache URL:	http://https://avatars.githubusercontent.com/u/38636870?s=32&v=4
Preview:	..... $.' '',#..(7),01444.'9=82<.342.....2!.!2222222222222222222222222222222222222222222222222..... . .."..... ....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... ..w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?...Zhb.ug1q.....2.j osc`g.\.2.[.;...m_jW..i.|.1XE.}.`..}r8...{I.[x...@f..~.H.....t)sji..-..v.m-..w.C...C.....x%.vK..l....u.I..lV..b.3..l.s.....[.o....vd.^N.@'..Q.].U..z6.=...H..F2....[<.j.....G*"...._..Z..M....u....z..! .....ry.Nf.;]....{.....O.UR.J.T'..c.... ..-..^.>..p:.....}.r67.|.g...d.....t..0.....i.6X.....Q.0u#!.0.....k.^...?..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\4643903[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, baseline, precision 8, 32x32, frames 3
Category:	downloaded
Size (bytes):	929
Entropy (8bit):	7.404131186802209
Encrypted:	false
SSDEEP:	24:Q9YMa6M0XxDuLHeOWXG427DAJuLHenX3WXHfg0cY14vPsW+q:Q9YMabuETAAX1cYm
MD5:	7E6323A70DF93D063A1A6DAB7C1589E9
SHA1:	E998FC4581C1A0F7AED5696FF5464F00FB60161B
SHA-256:	18AE6F2F70069CE28D3C2CFF1506E584BC67C0F4C1C970EBDAFEB8CEC1986FE6
SHA-512:	15ECBA0F9698A068902429DD8C4B0507233934A01C3813EBBFD70BE42428A5FD9BBC6DF52D73D583A10C2B555C4287189E1D1F9FE6ACEC73A711C726012CE1C 3
Malicious:	false
IE Cache URL:	http://https://avatars.githubusercontent.com/u/4643903?s=32&v=4
Preview:	..... $.' '',#..(7),01444.'9=82<.342.....2!.!2222222222222222222222222222222222222222222222222..... . .."..... ....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... ..w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?.....4wH x.X6...9.s..C ..y%...DL.A...n.8..e.\.>.y.$f.....q.....r.....#>..z.+.....:.,?Q.....`.\`J.;.o..yv.{q..*.C...M..R....&%.`..;I.G...~5.#u.....T.....y.=....Co....I.zF.....Ps.....]..t./I..!..4.w;..?.....`.....p~... R....J.\.:...D....PFdiA.Gr..&.ON.d...Z...j+{lt...b<..@..>..Ac..a.3.....ZF.j.T..c..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\6RJ6ZB23.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	21839
Entropy (8bit):	5.1243647220902515
Encrypted:	false
SSDEEP:	384:gqENBz3e9jcxvxRmusLQCAy3An7oKCAgeQrEabbSm5d0+BVdmea:QPRvzsMJ+4oNeQwabb30+H6
MD5:	D5F333C64F9B23DBBEBA3B97294A680E
SHA1:	5D4B8D5FA8CD55495BA4D31A19CE30D5BFA0A586
SHA-256:	7122BB68E7EF8CE25CD34A1AEFC4B63CF568D05BC7F313E0B41C9367E390743E
SHA-512:	E3AB0C912B37E174CF52E8334CEF2CAEC61D1CDA2CEE51F47B124CA7266EEA4A842F1D62DA3B7C41789721CE21BC9903EE72870183E48DEAC09FF6F1BD325 AF
Malicious:	false
Preview:	.....<!DOCTYPE HTML>.. [if IE 7]><html class="ie7" lang="en"><![endif]-->.. [if IE 8]><html class="ie8" lang="en"><![endif]-->.. [if gt IE 8]> >..<html lang="en">.. <! [endif]-->..<head>.. build date: Mon, 22 Feb 2021 06:29:04 GMT -->.. <meta charset="UTF-8">.. <meta http-equiv="X-UA-Compatible" content="IE=10,chrome=1" / >.. <meta name="viewport" content="width=device-width, initial-scale=1.0" />.. <title>.. Home.. :.. The Official Microsoft IIS Site.. </title>.. [if IE]><s cript src='https://www-iis.azureedge.net/v-2021-01-05-01/scripts-bundle/html5.js'></script><![endif]-->.. ..<meta name="description" content="Learn, download, & di scuss IIS7 and more on the official Microsoft IIS site for the IIS.NET development community." />.. .. <link rel="shortcut icon" type="image/ico" href="/favicon.ico">.. <l ink rel="apple-touch-icon-precomposed" href="/touch-icon-iphone-precomposed.png" />.. <link rel="apple-

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\IIS-Administration[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with CRLF, LF line terminators
Category:	downloaded
Size (bytes):	36235

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\IIS-Administration[1].htm	
Entropy (8bit):	5.023801728933389
Encrypted:	false
SSDEEP:	384:42O+KnubZslGzfEoCJSkKEm67b3d9NtC9ISp3NJCJUoLgkOHG3GtyfWGt4ElT18q:9I6CnXXzsnEP4pBhyMaAaPGhyMaAa5
MD5:	88C8C3ADC1C1790605F1B5044B900852
SHA1:	EFDA93B27857B4DD0184738A09CB57D3526F1F94
SHA-256:	7F6528C5B095857ADE76D5206A0523E2768A3F4E9C214B0C8A7C87E65C0CECD7
SHA-512:	0EBBE30A1CC3FAE902219F6078E0D099D118F7F228001908A1AEA7B305F72461827CC61BCA53AC5BB8D735303AA1FE8367E9DFB1B2A23CEE8ED3B485F2061DB
Malicious:	false
IE Cache URL:	http://https://docs.microsoft.com/en-us/IIS-Administration/
Preview:	<!DOCTYPE html>.....<html class="hasSidebar hasPageActions hasBreadcrumb conceptual has-default-focus theme-light" lang="en-us" dir="ltr" data-css-variable-support="true" data-authenticated="false" data-auth-status-determined="false" data-target="docs" x-ms-format-detection="none">....<head>...<meta charset="utf-8" />...<meta name="viewport" content="width=device-width, initial-scale=1.0" />...<meta property="og:title" content="Introduction to the Microsoft IIS Administration API" />...<meta property="og:type" content="website" />...<meta property="og:url" content="https://docs.microsoft.com/en-us/iis-administration/" />.....<meta name="twitter:card" content="summary" />...<meta name="twitter:site" content="@docsmsft" />.....<meta name="color-scheme" content="light dark">.....<meta name="author" content="shirhatti" />..<meta name="ms.author" content="soshir" />..<meta name="ms.topic"

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\RE4H9G0[1].wdp	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG-XR
Category:	downloaded
Size (bytes):	3344
Entropy (8bit):	7.606706374378652
Encrypted:	false
SSDEEP:	96:opqeLrM1AUt3fBrVJowWnBb8pmaWluKKJYc9OVVBrB:oYeLrPUJZpJvWnepXWluKAYc9OVVB
MD5:	574D5D951372DAB93A22C51E97849E25
SHA1:	3E175EB9918F1D3F3193636319113FDED1F9091C
SHA-256:	65F01E47E338ED535B1DDE3DBE52EA783726F6852E966F469957177C719ADE14
SHA-512:	ECB3461D68C4016FA50E0524E08F32109F00D832D6F5643BE81D13AFB867FDAB7BA12C565B57D2AF90703D5BE2EBC85406923E690EABDDE92CEAD68DDEFCADF1
Malicious:	false
IE Cache URL:	http://https://img-prod-cms-rt-microsoft-com.akamaized.net/cms/api/am/imageFileData/RE4H9G0?ver=5bb0&q=90&m=6&h=157&w=279&b=%23FFFFFFFF&l=f&o=t&aim=true
Preview:	II.. ...$..o.N.K..=wv.....$..B.....$..B.....WMPHOTO..F.q....0.....PPZ.EE.....G.#..... .....UUUUy...u.D..... ..UUPP.3...$.....D..;.....4.H|.H0...0.@..%....)....".B.....H.=p.t'..K.P.....F .....Y.1Tj..C D...?.....n|..N8.UP*.BE..Z.....UR..u.G... ...2.....=~.F...H..,0. A.....,g.q.D0.O..P.;.XyZ4.....4...&.....F..P.R.T.....7/.%.P...hAh@....nal./....=.....3.:i.B...|R...A.._.....3..].....U$..S..X....w.",...k|2.e.h..B.g....`1U.P@.p..r.$.....E.....G_. ....)$h.O..a.H..d,....)....^...../..T.e.D.....<...N.!,....@.@.F.IOW.....D....:.e+.-i\...Y.g;A.....l%..;.wZ....G.....t.1Y..?.....`p.L?.xy4.V\..Z-..D.8.....H8.....p.....&K.....$..z..'.).y.....R=....t...4.\....(..yg.Aj..EG.q+.4Y.].R:l....Y%Q.m"d.i.fA!.....\.....1.{.V....X@.9..Cb....I....dL.UN....]m..`uR...R*$..Z.dt..I....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\RE4pndL[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 40 x 40, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	1093
Entropy (8bit):	7.746658713530522
Encrypted:	false
SSDEEP:	24:pMgiCBITQBLZ02PHSeJN3Z+BKkrT3miwuU9ML8b9:p77d0cHSeJNZszT3mzuUq8R
MD5:	207E963B5CC48A36CE47FD9AD2E8F702
SHA1:	EE6EE0FB1EA66B60E6C58DF10799C0066CC121EB
SHA-256:	816CE5B6288F867E1ED48FD06CCF82E016392B1D3684CDD79924963BA44AF4D7
SHA-512:	234575043369F5A8A98B565104332B30AF3E774D6F4D78A3E0D24C96443ACBB1D848E72F6FEC9C4DF172B0A54BDD4937F55676350CC52395350C49F15CF2B472
Malicious:	false
IE Cache URL:	http://https://img-prod-cms-rt-microsoft-com.akamaized.net/cms/api/am/imageFileData/RE4pndL?ver=5217&q=90&m=6&h=40&w=40&b=%23FFFFFFFF&l=f&o=t&aim=true
Preview:	.PNG.....IHDR...(...(.....m....gAMA.....a.....pHYs.....o.d....sRGB.....IDATXG.M..G...uv.GW..5.....$xP.Uw.^.\<...C .I.. ..<x.+(...._.=K.*Btf...ww.g..{....w.h.6..Cu=. T.S.~.7k.1..c.1.....e....59...n-..v..Zr.C..\+..v.,d.T.9..YJM).B .h.~.....g....X..F.t.`...z...Y....kv...)..-.....hk..e..hc....(.....M.3E.Q..0r...R...Ya(....1^...._..r.../.<.S..qbki.-...?....U...:. .F.....r.@{...J...c...Zh....y<.<M...\...Yb.6.b.)....sL.U..P.....6B.).1D0....m.E,\2.R..n'.H.&...$GY*A .F..Q.W0DPV..E.N.Q.....O0HP..._..{..WLy.}.....?....a.x...f.$..\&$...8....yW. .}. T....z..]..x...<.....<Mz.....8.'...FU..o.;kW*..R.I.W@..T....M9`...w..Br.....r....=b.)....&..zxA.....j..."..N n..._H.}3x....9.xM..;bT0..o%..^m1.R.T.q%..*...Im.....g].o ...~B..... ....x ^.....B.x;.....%.B.. 4.f...n..M\....B....,.....C7....s.Z.....".\XN).X.G?...<....Z.....%?B.7..o..m.i~...n.....L.*H.1....S.3..%6..s...i2.A~`.("J..O...S..n.CD..#3..0,u3..8...9.....N!$..$.I

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\XDCN866V.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	163
Entropy (8bit):	4.758476922425921
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\XDCN866V.htm	
SSDEEP:	3:8ROFKGQIeNi1Xbvx9M84JxeCAIuREg7F6nmqDtyR8etRyL0HuWFq:AYSI0MXLxu2CAIuh7FUpyRHD7e
MD5:	877F8B0E3F3E29D6395AD926C80100F9
SHA1:	2881005E97F634973FB29C0E8B83AE068F0005EA
SHA-256:	EE8AAC22520665A9216BA2273FF10565829D7910884B18C09D956D8DF40AA6F5
SHA-512:	B676F9A7FC8E1B09BACF5FF9ED08525FDEFC15698CF92C9EB7B60D43057EB54FCCA1792E888E45BCEDC09FD707D2043EB1D0BB23D1A21902D3017AE520DD37D
Malicious:	false
Preview:	<head><title>Document Moved</title></head>.<body> Object Moved This document may be found <a HREF="https://dotnet.microsoft.com/apps/aspnet">here</body>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\bluebird.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators, with escape sequences
Category:	downloaded
Size (bytes):	79576
Entropy (8bit):	5.23717134330721
Encrypted:	false
SSDEEP:	768:HeK37qcI6j9doNmQ7rztoxtj6dOTwhiTnAO9Db8EufsLeo6fvHvpT999GL4necW3:HendH7FGtjrEO9DYkmJ9JecW5oanrT
MD5:	8C0479914B7B3B840BF9F62CFFE4ADAF
SHA1:	C33559D5F359521E58ED375D6863A2E85A37EADD
SHA-256:	AEC354E7DEA8B95F5A6242C12DBC66C54D6264795CDDF1CE685F59DE541CBA86
SHA-512:	7C31C0BD521562CC0F6DD604B568267FC217D198DAAE568B384A49B9CB93E21A27FED0FAB3B2A989F3715A864E0F7F867040474799ABFA6C344360310CAF4C7
Malicious:	false
IE Cache URL:	http://https://docs.microsoft.com/static/third-party/bluebird/3.5.0/bluebird.min.js
Preview:	/* @preserve.. * The MIT License (MIT).. * .. * Copyright (c) 2013-2017 Petka Antonov.. * .. * Permission is hereby granted, free of charge, to any person obtaining a copy.. * of this software and associated documentation files (the "Software"), to deal.. * in the Software without restriction, including without limitation the rights.. * to use, copy, modify, merge, publish, distribute, sublicense, and/or sell.. * copies of the Software, and to permit persons to whom the Software is.. * furnished to do so, subject to the following conditions:.. * .. * The above copyright notice and this permission notice shall be included in.. * all copies or substantial portions of the Software... * .. * THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR.. * IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,.. * FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE.. * AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR O

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\cartcount[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1283
Entropy (8bit):	4.393500974386876
Encrypted:	false
SSDEEP:	12:KPgkrfXKLf7fcabNBGFMpYMNwy+Mz4zMGgZv4c0EgtiQ5FgWyb0gDIgdcZPx+Ydg:KPv6HUY5+yAZFAXJqiXZXTMK
MD5:	1BF3F6D72753254D68A4A8C99DB850AD
SHA1:	E98B92CFF496817E3D5E6CD117F06BEEFAAD3E5F
SHA-256:	68D929A10C3CD609B936B50A541533994B044B38558A33530FF45D1B420CC07E
SHA-512:	C2F17E5861E800E32F3AC3DEA7424384E82B2F27B79C14D24686C286D5A6559CABDABB6A58DF9125334E196CC7D3116B583B3AE1D9AE6711AB21F9F4B06AF20
Malicious:	false
Preview:	.....<!DOCTYPE html>..<html>..<head>.. <title>title</title>..</head>..<body>.. <script>.. function getCartItemCountFromCookie() {.. var name = 'cartItemCount=';.. var allCookies = document.cookie.split(';');.. for (var i = 0; i < allCookies.length; i++) {.. var c = allCookies[i];.. while (c.charAt(0) === ' ') {.. c = c.substring(1);.. }.. if (c.indexOf(name) === 0) {.. return c.substring(name.length, c.length);.. }.. }.. return 0;.. }.... var count = getCartItemCountFromCookie();.... var parentHost = '';.. var parentOriginProtocol = '';.. var parentOrigin = '';.. try {.. parentHost = parent.location.hostname || '';.. parentOriginProtocol = parent.location.protocol;.. parentOrigin = parent.location.origin;.. } catch {..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\cookie-consent.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):	870
Entropy (8bit):	4.968001006158111
Encrypted:	false
SSDEEP:	24:2Qk2T+e+XuO9dFtn5FTK6ovH413RR/QRRcrpRmzfBQVM0Hb4+dEe:Xkt9r4Zs3rQYNAzfBGX7t
MD5:	7DC3A1A0BCBAA940DBF76D4BC7B763F6
SHA1:	B151D7FA9BBDB097D9356AA0B1DD3E1EB8A38662
SHA-256:	7EC0B0020B7E56B1A86A5B46C1A632736B841DF13B318B5050831C603302DC79
SHA-512:	FFD1F50046A7C7A814965556A5E6F6CE73AFC8EED51652E0DA91F6B02A0C9849B613AFBBDA1A280008A35ABC748CDE7EB7ED46BB329FE367E01BEBF3899B547A

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\cookie-consent.min[1].js	
Malicious:	false
IE Cache URL:	http://https://dotnet.microsoft.com/static/js/cookie-consent.min.js?v=A3Ym-tGu-1v2_1cMSBPdoSsFk4rf3MkGouymn5XJ4WQ
Preview:	(function(){function n(n){n==="set"?(setClarity(),setGTM()):(Cookies.remove("dismissed-alerts"),Cookies.remove("_clck"))}function t(n){n==="set"}function i(n){n==="set"}function r(r){r.Advertising?t("set"):t("reSet");r.SocialMedia?i("set"):i("reSet");r.Analytics?n("set"):n("reSet")}function f(n){r(n)}function e(n){n&&n.insertAdjacentHTML("afterend",'<li id="c-uhff-manage-cookies">Manage cookies ')}function u(){if(WcpConsent.siteConsent){WcpConsent.onConsentChanged(f);if(WcpConsent.siteConsent.isConsentRequired){e(document.getElementById("c-uhff-privacy & cookies"));var n=document.getElementById("c-uhff-manage-cookies");n.firstElementChild.addEventListener("click",function(n){n.preventDefault();WcpConsent.siteConsent.manageConsent()})}r(WcpConsent.siteConsent.getConsent())}else setTimeout(u,5e3)}setTimeout(u,5e3)})();

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\customers-ge-aviation[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 511 x 173, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	30179
Entropy (8bit):	7.9762935317355685
Encrypted:	false
SSDEEP:	768:yd/li/E6UD9v/jToXwY7gAj7BkOGcLg5YRSA020:ydwicl9v/X1YkAmD8qz
MD5:	28F92A0CB550895990B50871487B831E
SHA1:	23CA17C339EB2A3CF37DF93CB897864EF7931640
SHA-256:	4D4821DBCDF53EC11501CA88906EDFEC8663EE22F6F691238312CBA4708DA4B3
SHA-512:	80F2096E8BCAD0D9F92C0F2BA6B9D1A0255B38C41BD9326E33AFC513827B2A45A5AC9540997ACBB4231599EEAD8FB0886063E9283AD48B6CB18BCCF080BE79A
Malicious:	false
IE Cache URL:	http://https://dotnet.microsoft.com/static/images/redesign/customers-ge-aviation.png?v=TUgh2831PsEVAcqIkG7f7IZj7iL29pEjgxLLpHCNpLM
Preview:	.PNG.....IHDR.....v.....sRGB.....gAMA.....a.....pHYs.....o.d...!tEXtCreation Time.2020:05:21 12:14:34..s...uKIDATx^....E.._u.....v..%.%...$8....;..xH6...%.r.....<...t....{3..c;..$..O.t..tWWw.{U..=.h4..F..h4..F..h4..F..h4..F..h4..F..h4..F..h4..F..h4..F..h4..F..h4..F..h4..F..h4..F..h4..F..h4..F.E...X.../.,...P/2.|.DBd.!2...^.6..U}Zv3...8....kQ.k4..F.Y....t.<j..d...../..@2h3..6$..Q*.".O>..n...M..@P...$$.F.}..z.....d...6.!a}N..edvo....M<..j4..F..X;....&....v&...Uo.A.....:..$.(."..-.y.....O.h\|D..-uv.h4....X3..U.._.....A....J....o..z..qU yh.g(.?@.x...<...N[|..&N..}4..F..8.,...Y....{A.bk.,.C.....A.f....q.....!|o"....H.....3O..Kp..ID^....Q+...F..(V.....~..c....j3\Zt|>.iAX..g!.....]..d.$.z....l ..D"..".l..oQ..6.X.o.I.4...gA....'..P>.."...9.....l.....A..(._!./.Z&.2.#..x...F..h49a...l...{A...AY.+....t=M..{|..._!^G..5...;...6..Z. ...Y.I.#....6.dCB/.Z...X.....U.}.~..h4.M.X...4j.Z.E[..>..'..6.U$..s..Z h...d.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\dnserror[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	2997
Entropy (8bit):	4.4885437940628465
Encrypted:	false
SSDEEP:	48:u7u5V4VyhhV2lFUW29vj0RkpNc7KpAP8Rra:vIlJ6G7Ao8Ra
MD5:	2DC61EB461DA1436F5D22BCE51425660
SHA1:	E1B79BCAB0F073868079D807FAEC669596DC46C1
SHA-256:	ACDEB4966289B6CE46ECC879531F85E9C6F94B718AAB521D38E2E00F7F7F7993
SHA-512:	A88BECB4FBDDC5AFC55E4DC0135AF714A3EEC4A63810AE5A989F2CECB824A686165D3CEDB8CBD8F35C7E5B9F4136C29DEA32736AABB451FE8088B978B493AC6D
Malicious:	false
IE Cache URL:	res://ieframe.dll/dnserror.htm?ErrorStatus=0x800C0005&DNSError=1460
Preview:	.<!DOCTYPE HTML>..<html>.. <head>.. <link rel="stylesheet" type="text/css" href="NewErrorPageTemplate.css" >.. <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.. <title>Can’t reach this page</title>.. <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="getInfo(); initMoreInfo('infoBlockID');">.. .. Can’t reach this page .. .. <ul id="cantDisplayTasks" class="tasks">.. <li id="task1-1">Make sure the web address is correct .. <li id="task1-2">Search for this site on Bing ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\down[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	748
Entropy (8bit):	7.249606135668305
Encrypted:	false
SSDEEP:	12:6v/7/2QeZ7HVJ6o6yiq1p4tSQfAVFcm6R2HkZuU4fB4CsY4NJlrvMezoW2uONroc:GeZ6oLiqkbDuU4fqzTrvMeBBlE
MD5:	C4F558C4C8B56858F15C09037CD6625A
SHA1:	EE497CC061D6A7A59BB66DEFEA65F9A8145BA240
SHA-256:	39E7DE847C9F731EAA72338AD9053217B957859DE27B50B6474EC42971530781
SHA-512:	D60353D3FBEA2992D96795BA30B20727B022B9164B2094B922921D33CA7CE1634713693AC191F8F5708954544F7648F4840BCD5B62CB6A032EF292A8B0E52A44
Malicious:	false
IE Cache URL:	res://ieframe.dll/down.png

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\down[1]	
Preview:	.PNG.....IHDR.....ex....PLTE....W..W..W..W..W..W..W..W..W..W..W..W..W..W.U.....W..W.!Y.#Z.$\.'].<r.=s.P..Q..Q..U..o..p..r..x..z..~.....b.....$..s...7tRNS.a.o(,.s....e.....q*.....F.Z....IDATx^%.S..@.C..jm.mTk...m.?|;.y..S....F.t...,.....D.>..LpX=f.M...H4.....=...=..xy.[h..7....7.....<.q.kH....#+....I..z.....'.ksC...X<.+..J>....%3BmqaV...h..Z._.:<.Y_jG...vN^.<>.Nu.u@.....M....?...1D.m~)s8..&....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\e3-082b89[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):	112400
Entropy (8bit):	5.228169564162013
Encrypted:	false
SSDEEP:	1536:uzUHQcyAz9ppxS7grUU59gQ9lwInL2dS6q09RhY8WOyd1EwgXA9GKamAMKihAGDb:uzUnppxvIeq0y9d1EwgXA95KinDCE4+
MD5:	B65C8811340C54C9C9AB8BEACFF8ED30
SHA1:	671AF88A583151054B4982560B35F5A1CD1D2758
SHA-256:	44E895D6299B5E835190E6DC9503A077EF08B2FF4D04C9EC4190EC9225B92274
SHA-512:	1912D5E1456F6749DBA198EA01ED59BB2973FD9F712A1BB57BFB61AB9F06875B02EC232D78853B6643300D02D4E7526904C5111ED833347766891A7739AA90E5
Malicious:	false
IE Cache URL:	http://https://www.microsoft.com/onerfstatics/marketingsites-neu-prod/mscomhp/_scrf/js/themes=default/2f-63ce8f/45-f9a0d4/aa-dc1460/2d-7a9063/dc-7e9864/4f-5115f8/7d-266f10/4a-abd94b/6d-c07ea1/29-1ec5a9/f6-aa5278/cd-23d3b0/6d-1e7ed0/b7-cadaa7/c4-898cf2/ca-40b7b0/4e-ee3a55/3e-f5c39b/c3-6454d7/f9-7592d3/92-10345d/f8-73a5f2/79-499886/7e-cda2d3/69-13871c/e5-08f1c0/91-97a04f/1f-100dea/33-abe4df/17-f90ef1/e3-082b89?ver=2.0
Preview:	var __extends;define("ajaxWithAnimation",["jqReady!","jsll"],function(n,t){var i=[" <\/span><\/span><\/span><\/span><\/span><\/div>"],u=function(t,r){var u=n(t),o,f,e;u.length&&(o=(r.loaderType||"").toUpperCase(),i[1]=o==="PROGRESS"||o==="PROGRESSBAR"?"regional":o==="SPINNERLARGE"?"local f-progress-large f-center":"local f-progress-small",r.margin&&r.margin.length&&(i[3]=r.margin),f=i.join(""),e=(r.loaderPosition||"").toUpperCase(),e==="TOP"||e==="BOTTOM"?(u.addClass("ajaxloader"),e==="BOTTOM"?u.append(f):u.prepend(f)):(u.parent().addClass("ajaxloader"),e==="BEFORE"?u.before(f):u.after(f)))},f=function(t,i){var r=n(t),u;r.length&&(u=(i.loaderPosition||"").toUpperCase(),u!=="TOP"&&u!=="BOTTOM"&&(r=r.parent()),r.removeClass("ajaxloader").children().remove(".c-progress"))},r=function(i){i.refreshElement&&u(i.refreshElement,i);var r=n.extend(i,{s

Static File Info

General

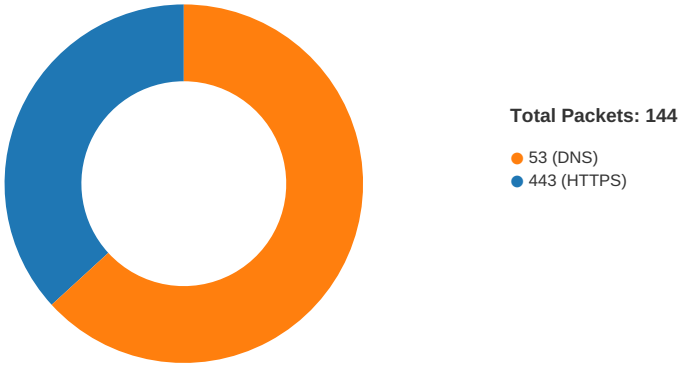
File type:	Microsoft Word 2007+
Entropy (8bit):	7.851441203844124
TrID:	• Word Microsoft Office Open XML Format document (49504/1) 49.01% • Word Microsoft Office Open XML Format document (43504/1) 43.07% • ZIP compressed archive (8000/1) 7.92%
File name:	2021-02-18 Fivoor - Overleg - Kwartaaloverleg.docx
File size:	182929
MD5:	14b364f395dd53fa6b36d00e46c514da
SHA1:	0b97138df21f05c020e43f2c882694bdc805c4a1
SHA256:	1f39fb321c3902a9506b3f3529f5fdbf868053018099991d95e254596658bdfd
SHA512:	f9cdc8f81305f9a89913aa8212ae935f0f2f86d367b426d3e6a5cfbddf4ca66cf1da5db958123e1986c24018a0447bb47a9adb829c66d101a58f3d894e63ffa5
SSDEEP:	3072:uNN8nVGbLDzApKPKlMT+F5edQjPGZdoL/C8GY64iUG0BaI66V5GPUPo:uFLfGKP+K+FUmjPGPo2zY6lVzbGB
File Content Preview:	PK.....!.....D.....[Content_Types].xml ...(..... ....

File Icon

Icon Hash:	74fcd0d2d6d6d0cc

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 21:41:14.931339979 CET	49725	443	192.168.2.3	34.253.10.100
Feb 25, 2021 21:41:14.931715965 CET	49726	443	192.168.2.3	34.253.10.100
Feb 25, 2021 21:41:14.992935896 CET	443	49725	34.253.10.100	192.168.2.3
Feb 25, 2021 21:41:14.993163109 CET	49725	443	192.168.2.3	34.253.10.100
Feb 25, 2021 21:41:14.995471954 CET	443	49726	34.253.10.100	192.168.2.3
Feb 25, 2021 21:41:14.995610952 CET	49726	443	192.168.2.3	34.253.10.100
Feb 25, 2021 21:41:15.000545979 CET	49726	443	192.168.2.3	34.253.10.100
Feb 25, 2021 21:41:15.000921965 CET	49725	443	192.168.2.3	34.253.10.100
Feb 25, 2021 21:41:15.062052965 CET	443	49725	34.253.10.100	192.168.2.3
Feb 25, 2021 21:41:15.062956095 CET	443	49725	34.253.10.100	192.168.2.3
Feb 25, 2021 21:41:15.063005924 CET	443	49725	34.253.10.100	192.168.2.3
Feb 25, 2021 21:41:15.063040972 CET	49725	443	192.168.2.3	34.253.10.100
Feb 25, 2021 21:41:15.063047886 CET	443	49725	34.253.10.100	192.168.2.3
Feb 25, 2021 21:41:15.063072920 CET	49725	443	192.168.2.3	34.253.10.100
Feb 25, 2021 21:41:15.063085079 CET	443	49725	34.253.10.100	192.168.2.3
Feb 25, 2021 21:41:15.063102961 CET	49725	443	192.168.2.3	34.253.10.100
Feb 25, 2021 21:41:15.063139915 CET	49725	443	192.168.2.3	34.253.10.100
Feb 25, 2021 21:41:15.064285040 CET	443	49726	34.253.10.100	192.168.2.3
Feb 25, 2021 21:41:15.065525055 CET	443	49726	34.253.10.100	192.168.2.3
Feb 25, 2021 21:41:15.065563917 CET	443	49726	34.253.10.100	192.168.2.3
Feb 25, 2021 21:41:15.065603018 CET	443	49726	34.253.10.100	192.168.2.3
Feb 25, 2021 21:41:15.065639973 CET	443	49726	34.253.10.100	192.168.2.3
Feb 25, 2021 21:41:15.065645933 CET	49726	443	192.168.2.3	34.253.10.100
Feb 25, 2021 21:41:15.065681934 CET	49726	443	192.168.2.3	34.253.10.100
Feb 25, 2021 21:41:15.065694094 CET	49726	443	192.168.2.3	34.253.10.100
Feb 25, 2021 21:41:15.065700054 CET	49726	443	192.168.2.3	34.253.10.100
Feb 25, 2021 21:41:15.102319002 CET	49725	443	192.168.2.3	34.253.10.100
Feb 25, 2021 21:41:15.102397919 CET	49726	443	192.168.2.3	34.253.10.100
Feb 25, 2021 21:41:15.108792067 CET	49725	443	192.168.2.3	34.253.10.100
Feb 25, 2021 21:41:15.108922005 CET	49726	443	192.168.2.3	34.253.10.100
Feb 25, 2021 21:41:15.109767914 CET	49725	443	192.168.2.3	34.253.10.100
Feb 25, 2021 21:41:15.163988113 CET	443	49725	34.253.10.100	192.168.2.3
Feb 25, 2021 21:41:15.164042950 CET	443	49725	34.253.10.100	192.168.2.3
Feb 25, 2021 21:41:15.164084911 CET	49725	443	192.168.2.3	34.253.10.100
Feb 25, 2021 21:41:15.164134026 CET	49725	443	192.168.2.3	34.253.10.100
Feb 25, 2021 21:41:15.164788008 CET	49725	443	192.168.2.3	34.253.10.100
Feb 25, 2021 21:41:15.166565895 CET	443	49726	34.253.10.100	192.168.2.3
Feb 25, 2021 21:41:15.166599989 CET	443	49726	34.253.10.100	192.168.2.3
Feb 25, 2021 21:41:15.166652918 CET	49726	443	192.168.2.3	34.253.10.100
Feb 25, 2021 21:41:15.166692019 CET	49726	443	192.168.2.3	34.253.10.100
Feb 25, 2021 21:41:15.167203903 CET	49726	443	192.168.2.3	34.253.10.100
Feb 25, 2021 21:41:15.170011044 CET	443	49725	34.253.10.100	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 21:41:15.170162916 CET	49725	443	192.168.2.3	34.253.10.100
Feb 25, 2021 21:41:15.171901941 CET	443	49725	34.253.10.100	192.168.2.3
Feb 25, 2021 21:41:15.171933889 CET	443	49725	34.253.10.100	192.168.2.3
Feb 25, 2021 21:41:15.171976089 CET	49725	443	192.168.2.3	34.253.10.100
Feb 25, 2021 21:41:15.172003031 CET	49725	443	192.168.2.3	34.253.10.100
Feb 25, 2021 21:41:15.172916889 CET	443	49726	34.253.10.100	192.168.2.3
Feb 25, 2021 21:41:15.172983885 CET	49726	443	192.168.2.3	34.253.10.100
Feb 25, 2021 21:41:15.237724066 CET	49725	443	192.168.2.3	34.253.10.100
Feb 25, 2021 21:41:15.268968105 CET	443	49725	34.253.10.100	192.168.2.3
Feb 25, 2021 21:41:15.274389029 CET	443	49726	34.253.10.100	192.168.2.3
Feb 25, 2021 21:41:15.300395012 CET	443	49725	34.253.10.100	192.168.2.3
Feb 25, 2021 21:41:15.302679062 CET	443	49725	34.253.10.100	192.168.2.3
Feb 25, 2021 21:41:15.302736044 CET	443	49725	34.253.10.100	192.168.2.3
Feb 25, 2021 21:41:15.302778959 CET	443	49725	34.253.10.100	192.168.2.3
Feb 25, 2021 21:41:15.302804947 CET	49725	443	192.168.2.3	34.253.10.100
Feb 25, 2021 21:41:15.302826881 CET	443	49725	34.253.10.100	192.168.2.3
Feb 25, 2021 21:41:15.302845955 CET	49725	443	192.168.2.3	34.253.10.100
Feb 25, 2021 21:41:15.302854061 CET	49725	443	192.168.2.3	34.253.10.100
Feb 25, 2021 21:41:15.302880049 CET	49725	443	192.168.2.3	34.253.10.100
Feb 25, 2021 21:41:15.302886963 CET	443	49725	34.253.10.100	192.168.2.3
Feb 25, 2021 21:41:15.302938938 CET	443	49725	34.253.10.100	192.168.2.3
Feb 25, 2021 21:41:15.302947044 CET	49725	443	192.168.2.3	34.253.10.100
Feb 25, 2021 21:41:15.302985907 CET	443	49725	34.253.10.100	192.168.2.3
Feb 25, 2021 21:41:15.302994013 CET	49725	443	192.168.2.3	34.253.10.100
Feb 25, 2021 21:41:15.303029060 CET	443	49725	34.253.10.100	192.168.2.3
Feb 25, 2021 21:41:15.303039074 CET	49725	443	192.168.2.3	34.253.10.100
Feb 25, 2021 21:41:15.303067923 CET	443	49725	34.253.10.100	192.168.2.3
Feb 25, 2021 21:41:15.303083897 CET	49725	443	192.168.2.3	34.253.10.100
Feb 25, 2021 21:41:15.303107023 CET	443	49725	34.253.10.100	192.168.2.3
Feb 25, 2021 21:41:15.303121090 CET	49725	443	192.168.2.3	34.253.10.100
Feb 25, 2021 21:41:15.303163052 CET	49725	443	192.168.2.3	34.253.10.100
Feb 25, 2021 21:41:15.364387989 CET	443	49725	34.253.10.100	192.168.2.3
Feb 25, 2021 21:41:15.364459038 CET	443	49725	34.253.10.100	192.168.2.3
Feb 25, 2021 21:41:15.364502907 CET	443	49725	34.253.10.100	192.168.2.3
Feb 25, 2021 21:41:15.364509106 CET	49725	443	192.168.2.3	34.253.10.100
Feb 25, 2021 21:41:15.364551067 CET	49725	443	192.168.2.3	34.253.10.100
Feb 25, 2021 21:41:15.364552021 CET	443	49725	34.253.10.100	192.168.2.3
Feb 25, 2021 21:41:15.364574909 CET	49725	443	192.168.2.3	34.253.10.100
Feb 25, 2021 21:41:15.364599943 CET	49725	443	192.168.2.3	34.253.10.100
Feb 25, 2021 21:41:15.364603996 CET	443	49725	34.253.10.100	192.168.2.3
Feb 25, 2021 21:41:15.364654064 CET	443	49725	34.253.10.100	192.168.2.3
Feb 25, 2021 21:41:15.364661932 CET	49725	443	192.168.2.3	34.253.10.100
Feb 25, 2021 21:41:15.364711046 CET	49725	443	192.168.2.3	34.253.10.100
Feb 25, 2021 21:41:15.364712954 CET	443	49725	34.253.10.100	192.168.2.3
Feb 25, 2021 21:41:15.364767075 CET	443	49725	34.253.10.100	192.168.2.3
Feb 25, 2021 21:41:15.364772081 CET	49725	443	192.168.2.3	34.253.10.100
Feb 25, 2021 21:41:15.364819050 CET	443	49725	34.253.10.100	192.168.2.3
Feb 25, 2021 21:41:15.364823103 CET	49725	443	192.168.2.3	34.253.10.100
Feb 25, 2021 21:41:15.364866018 CET	443	49725	34.253.10.100	192.168.2.3
Feb 25, 2021 21:41:15.364882946 CET	49725	443	192.168.2.3	34.253.10.100
Feb 25, 2021 21:41:15.364917994 CET	443	49725	34.253.10.100	192.168.2.3
Feb 25, 2021 21:41:15.364922047 CET	49725	443	192.168.2.3	34.253.10.100
Feb 25, 2021 21:41:15.364965916 CET	443	49725	34.253.10.100	192.168.2.3
Feb 25, 2021 21:41:15.364984989 CET	49725	443	192.168.2.3	34.253.10.100
Feb 25, 2021 21:41:15.365016937 CET	443	49725	34.253.10.100	192.168.2.3
Feb 25, 2021 21:41:15.365031958 CET	49725	443	192.168.2.3	34.253.10.100
Feb 25, 2021 21:41:15.365056992 CET	443	49725	34.253.10.100	192.168.2.3
Feb 25, 2021 21:41:15.365076065 CET	49725	443	192.168.2.3	34.253.10.100

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 21:40:30.794023991 CET	51281	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:40:30.802548885 CET	53	50200	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 21:40:30.843131065 CET	53	51281	8.8.8.8	192.168.2.3
Feb 25, 2021 21:40:31.718322992 CET	49199	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:40:31.770412922 CET	53	49199	8.8.8.8	192.168.2.3
Feb 25, 2021 21:40:32.887468100 CET	50620	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:40:32.940795898 CET	53	50620	8.8.8.8	192.168.2.3
Feb 25, 2021 21:40:33.876821995 CET	64938	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:40:33.928133011 CET	53	64938	8.8.8.8	192.168.2.3
Feb 25, 2021 21:40:34.292228937 CET	60152	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:40:34.345801115 CET	53	60152	8.8.8.8	192.168.2.3
Feb 25, 2021 21:40:34.761425018 CET	57544	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:40:34.812439919 CET	53	57544	8.8.8.8	192.168.2.3
Feb 25, 2021 21:40:39.095114946 CET	55984	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:40:39.145857096 CET	53	55984	8.8.8.8	192.168.2.3
Feb 25, 2021 21:40:39.691848040 CET	64185	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:40:39.772082090 CET	53	64185	8.8.8.8	192.168.2.3
Feb 25, 2021 21:40:40.697396040 CET	64185	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:40:40.758196115 CET	53	64185	8.8.8.8	192.168.2.3
Feb 25, 2021 21:40:41.065035105 CET	65110	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:40:41.149493933 CET	53	65110	8.8.8.8	192.168.2.3
Feb 25, 2021 21:40:41.367927074 CET	58361	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:40:41.418664932 CET	53	58361	8.8.8.8	192.168.2.3
Feb 25, 2021 21:40:41.713066101 CET	64185	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:40:41.771709919 CET	53	64185	8.8.8.8	192.168.2.3
Feb 25, 2021 21:40:42.354639053 CET	58361	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:40:42.407001019 CET	53	58361	8.8.8.8	192.168.2.3
Feb 25, 2021 21:40:43.369683981 CET	58361	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:40:43.420336962 CET	53	58361	8.8.8.8	192.168.2.3
Feb 25, 2021 21:40:43.728034019 CET	64185	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:40:43.785264015 CET	53	64185	8.8.8.8	192.168.2.3
Feb 25, 2021 21:40:45.385472059 CET	58361	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:40:45.436098099 CET	53	58361	8.8.8.8	192.168.2.3
Feb 25, 2021 21:40:47.729032040 CET	64185	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:40:47.781733990 CET	53	64185	8.8.8.8	192.168.2.3
Feb 25, 2021 21:40:49.400793076 CET	58361	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:40:49.451190948 CET	53	58361	8.8.8.8	192.168.2.3
Feb 25, 2021 21:40:55.943768024 CET	63492	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:40:56.000905991 CET	53	63492	8.8.8.8	192.168.2.3
Feb 25, 2021 21:40:56.783761978 CET	60831	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:40:56.837583065 CET	53	60831	8.8.8.8	192.168.2.3
Feb 25, 2021 21:40:57.771251917 CET	60100	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:40:57.820229053 CET	53	60100	8.8.8.8	192.168.2.3
Feb 25, 2021 21:40:59.132236958 CET	53195	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:40:59.182521105 CET	53	53195	8.8.8.8	192.168.2.3
Feb 25, 2021 21:40:59.956496000 CET	50141	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:41:00.007957935 CET	53	50141	8.8.8.8	192.168.2.3
Feb 25, 2021 21:41:00.771009922 CET	53023	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:41:00.821688890 CET	53	53023	8.8.8.8	192.168.2.3
Feb 25, 2021 21:41:01.922107935 CET	49563	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:41:01.971167088 CET	53	49563	8.8.8.8	192.168.2.3
Feb 25, 2021 21:41:03.053873062 CET	51352	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:41:03.107527018 CET	53	51352	8.8.8.8	192.168.2.3
Feb 25, 2021 21:41:04.250716925 CET	59349	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:41:04.310791969 CET	53	59349	8.8.8.8	192.168.2.3
Feb 25, 2021 21:41:05.062347889 CET	57084	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:41:05.113193989 CET	53	57084	8.8.8.8	192.168.2.3
Feb 25, 2021 21:41:06.440845013 CET	58823	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:41:06.489615917 CET	53	58823	8.8.8.8	192.168.2.3
Feb 25, 2021 21:41:07.247868061 CET	57568	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:41:07.298465014 CET	53	57568	8.8.8.8	192.168.2.3
Feb 25, 2021 21:41:08.574279070 CET	50540	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:41:08.641036034 CET	53	50540	8.8.8.8	192.168.2.3
Feb 25, 2021 21:41:08.667678118 CET	54366	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:41:08.719248056 CET	53	54366	8.8.8.8	192.168.2.3
Feb 25, 2021 21:41:09.546241999 CET	53034	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 21:41:09.595365047 CET	53	53034	8.8.8.8	192.168.2.3
Feb 25, 2021 21:41:11.542777061 CET	57762	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:41:11.605082035 CET	53	57762	8.8.8.8	192.168.2.3
Feb 25, 2021 21:41:14.861677885 CET	55435	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:41:14.922781944 CET	53	55435	8.8.8.8	192.168.2.3
Feb 25, 2021 21:41:15.676208019 CET	50713	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:41:15.745105028 CET	53	50713	8.8.8.8	192.168.2.3
Feb 25, 2021 21:41:15.942719936 CET	56132	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:41:15.994520903 CET	53	56132	8.8.8.8	192.168.2.3
Feb 25, 2021 21:41:16.651503086 CET	58987	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:41:16.658580065 CET	56579	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:41:16.705427885 CET	53	58987	8.8.8.8	192.168.2.3
Feb 25, 2021 21:41:16.707844019 CET	53	56579	8.8.8.8	192.168.2.3
Feb 25, 2021 21:41:26.891546011 CET	60633	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:41:26.970753908 CET	53	60633	8.8.8.8	192.168.2.3
Feb 25, 2021 21:41:41.516658068 CET	61292	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:41:41.568906069 CET	53	61292	8.8.8.8	192.168.2.3
Feb 25, 2021 21:41:41.623121023 CET	63619	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:41:41.688282967 CET	53	63619	8.8.8.8	192.168.2.3
Feb 25, 2021 21:41:42.516108036 CET	61292	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:41:42.564861059 CET	53	61292	8.8.8.8	192.168.2.3
Feb 25, 2021 21:41:43.530632019 CET	61292	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:41:43.579440117 CET	53	61292	8.8.8.8	192.168.2.3
Feb 25, 2021 21:41:44.292984962 CET	64938	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:41:44.342717886 CET	53	64938	8.8.8.8	192.168.2.3
Feb 25, 2021 21:41:45.280611038 CET	64938	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:41:45.329958916 CET	53	64938	8.8.8.8	192.168.2.3
Feb 25, 2021 21:41:45.532988071 CET	61292	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:41:45.583522081 CET	53	61292	8.8.8.8	192.168.2.3
Feb 25, 2021 21:41:46.296519041 CET	64938	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:41:46.353547096 CET	53	64938	8.8.8.8	192.168.2.3
Feb 25, 2021 21:41:48.296327114 CET	64938	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:41:48.346287966 CET	53	64938	8.8.8.8	192.168.2.3
Feb 25, 2021 21:41:49.546390057 CET	61292	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:41:49.595269918 CET	53	61292	8.8.8.8	192.168.2.3
Feb 25, 2021 21:41:52.312041998 CET	64938	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:41:52.363518953 CET	53	64938	8.8.8.8	192.168.2.3
Feb 25, 2021 21:42:00.172915936 CET	61946	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:42:00.224659920 CET	53	61946	8.8.8.8	192.168.2.3
Feb 25, 2021 21:42:03.904637098 CET	64910	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:42:03.965959072 CET	53	64910	8.8.8.8	192.168.2.3
Feb 25, 2021 21:42:22.758856058 CET	52123	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:42:22.819511890 CET	53	52123	8.8.8.8	192.168.2.3
Feb 25, 2021 21:42:28.086925030 CET	56130	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:42:28.204360008 CET	53	56130	8.8.8.8	192.168.2.3
Feb 25, 2021 21:42:29.097681046 CET	56338	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:42:29.179064035 CET	53	56338	8.8.8.8	192.168.2.3
Feb 25, 2021 21:42:30.248378992 CET	59420	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:42:30.312254906 CET	53	59420	8.8.8.8	192.168.2.3
Feb 25, 2021 21:42:30.647038937 CET	58784	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:42:30.666747093 CET	63978	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:42:30.681154013 CET	62938	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:42:30.683667898 CET	55708	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:42:30.683806896 CET	56803	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:42:30.684114933 CET	57145	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:42:30.718445063 CET	53	63978	8.8.8.8	192.168.2.3
Feb 25, 2021 21:42:30.721105099 CET	53	58784	8.8.8.8	192.168.2.3
Feb 25, 2021 21:42:30.731864929 CET	53	62938	8.8.8.8	192.168.2.3
Feb 25, 2021 21:42:30.740792990 CET	53	57145	8.8.8.8	192.168.2.3
Feb 25, 2021 21:42:30.742094040 CET	55359	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:42:30.742352962 CET	53	55708	8.8.8.8	192.168.2.3
Feb 25, 2021 21:42:30.747288942 CET	53	56803	8.8.8.8	192.168.2.3
Feb 25, 2021 21:42:30.760251999 CET	58306	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:42:30.795320988 CET	53	55359	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 21:42:30.824337959 CET	53	58306	8.8.8.8	192.168.2.3
Feb 25, 2021 21:42:32.841383934 CET	64124	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:42:32.901817083 CET	53	64124	8.8.8.8	192.168.2.3
Feb 25, 2021 21:42:33.227467060 CET	49361	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:42:33.288023949 CET	53	49361	8.8.8.8	192.168.2.3
Feb 25, 2021 21:42:33.395440102 CET	63150	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:42:33.470958948 CET	53	63150	8.8.8.8	192.168.2.3
Feb 25, 2021 21:42:33.562849998 CET	53279	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:42:33.625966072 CET	53	53279	8.8.8.8	192.168.2.3
Feb 25, 2021 21:42:34.046034098 CET	56881	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:42:34.097850084 CET	53	56881	8.8.8.8	192.168.2.3
Feb 25, 2021 21:42:34.480319977 CET	53642	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:42:34.538945913 CET	53	53642	8.8.8.8	192.168.2.3
Feb 25, 2021 21:42:36.600368023 CET	55667	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:42:36.652136087 CET	53	55667	8.8.8.8	192.168.2.3
Feb 25, 2021 21:42:36.687690020 CET	54833	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:42:36.767836094 CET	53	54833	8.8.8.8	192.168.2.3
Feb 25, 2021 21:42:37.198556900 CET	62476	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:42:37.252001047 CET	53	62476	8.8.8.8	192.168.2.3
Feb 25, 2021 21:42:37.540642023 CET	49705	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:42:37.589566946 CET	53	49705	8.8.8.8	192.168.2.3
Feb 25, 2021 21:42:40.363773108 CET	61477	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:42:40.422234058 CET	53	61477	8.8.8.8	192.168.2.3
Feb 25, 2021 21:42:47.706176996 CET	61633	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:42:47.766391039 CET	53	61633	8.8.8.8	192.168.2.3
Feb 25, 2021 21:42:48.178364038 CET	55949	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:42:48.246787071 CET	53	55949	8.8.8.8	192.168.2.3
Feb 25, 2021 21:42:49.015881062 CET	57601	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:42:49.051368952 CET	49342	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:42:49.064927101 CET	53	57601	8.8.8.8	192.168.2.3
Feb 25, 2021 21:42:49.111641884 CET	53	49342	8.8.8.8	192.168.2.3
Feb 25, 2021 21:42:50.124392033 CET	56253	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:42:50.178324938 CET	53	56253	8.8.8.8	192.168.2.3
Feb 25, 2021 21:42:50.445250988 CET	49667	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:42:50.494132042 CET	53	49667	8.8.8.8	192.168.2.3
Feb 25, 2021 21:43:26.257018089 CET	55439	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:43:26.317435980 CET	53	55439	8.8.8.8	192.168.2.3
Feb 25, 2021 21:43:27.239350080 CET	57069	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:43:27.291636944 CET	53	57069	8.8.8.8	192.168.2.3
Feb 25, 2021 21:43:28.571367979 CET	57659	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:43:28.633780956 CET	53	57659	8.8.8.8	192.168.2.3
Feb 25, 2021 21:43:29.180572987 CET	54717	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:43:29.264525890 CET	53	54717	8.8.8.8	192.168.2.3
Feb 25, 2021 21:43:29.793845892 CET	63975	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:43:29.847876072 CET	53	63975	8.8.8.8	192.168.2.3
Feb 25, 2021 21:43:30.427064896 CET	56639	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:43:30.478955030 CET	53	56639	8.8.8.8	192.168.2.3
Feb 25, 2021 21:43:31.109392881 CET	51856	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:43:31.178111076 CET	53	51856	8.8.8.8	192.168.2.3
Feb 25, 2021 21:43:31.934676886 CET	56546	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:43:31.983760118 CET	53	56546	8.8.8.8	192.168.2.3
Feb 25, 2021 21:43:32.643978119 CET	62152	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:43:32.703350067 CET	53	62152	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 25, 2021 21:40:41.065035105 CET	192.168.2.3	8.8.8.8	0xb08a	Standard query (0)	lemontree1 .sharepoint.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:41:14.861677885 CET	192.168.2.3	8.8.8.8	0xfcd0	Standard query (0)	sn.webroot cloudav.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:41:15.942719936 CET	192.168.2.3	8.8.8.8	0xe7d9	Standard query (0)	www.iis.net	A (IP address)	IN (0x0001)
Feb 25, 2021 21:41:16.658580065 CET	192.168.2.3	8.8.8.8	0x508d	Standard query (0)	consentdel iveryfd.az urefd.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 25, 2021 21:42:22.758856058 CET	192.168.2.3	8.8.8.8	0x4c63	Standard query (0)	www.iis.net	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:28.086925030 CET	192.168.2.3	8.8.8.8	0x9c46	Standard query (0)	login.iis.net	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:30.681154013 CET	192.168.2.3	8.8.8.8	0x9cda	Standard query (0)	assets.onestore.ms	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:30.683667898 CET	192.168.2.3	8.8.8.8	0x162c	Standard query (0)	mem.gfx.ms	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:30.684114933 CET	192.168.2.3	8.8.8.8	0x9350	Standard query (0)	microsoftwindows.112.2o7.net	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:30.742094040 CET	192.168.2.3	8.8.8.8	0xc9c	Standard query (0)	mem.gfx.ms	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:32.841383934 CET	192.168.2.3	8.8.8.8	0xa510	Standard query (0)	publisher.liveperson.net	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:34.480319977 CET	192.168.2.3	8.8.8.8	0xae1f	Standard query (0)	logincdn.msauth.net	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:37.198556900 CET	192.168.2.3	8.8.8.8	0xabae	Standard query (0)	github.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:37.540642023 CET	192.168.2.3	8.8.8.8	0x9e30	Standard query (0)	avatars.githubusercontent.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:50.124392033 CET	192.168.2.3	8.8.8.8	0x6922	Standard query (0)	dc.services.visualstudio.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:50.445250988 CET	192.168.2.3	8.8.8.8	0x6945	Standard query (0)	www.asp.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 25, 2021 21:40:41.149493933 CET	8.8.8.8	192.168.2.3	0xb08a	No error (0)	lemontree1.sharepoint.com	222-ipv4e.clump.dprodmgd104.aa-rt.sharepoint.com		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:40:41.149493933 CET	8.8.8.8	192.168.2.3	0xb08a	No error (0)	222-ipv4e.clump.dprodmgd104.aa-rt.sharepoint.com	187105-ipv4e.farm.dprodmgd104.aa-rt.sharepoint.com		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:40:41.149493933 CET	8.8.8.8	192.168.2.3	0xb08a	No error (0)	187105-ipv4e.farm.dprodmgd104.aa-rt.sharepoint.com	187105-ipv4e.farm.dprodmgd104.sharepointonline.com.akadns.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:41:14.922781944 CET	8.8.8.8	192.168.2.3	0xfcd0	No error (0)	sn.webrootcloudav.com		34.253.10.100	A (IP address)	IN (0x0001)
Feb 25, 2021 21:41:14.922781944 CET	8.8.8.8	192.168.2.3	0xfcd0	No error (0)	sn.webrootcloudav.com		18.203.30.130	A (IP address)	IN (0x0001)
Feb 25, 2021 21:41:14.922781944 CET	8.8.8.8	192.168.2.3	0xfcd0	No error (0)	sn.webrootcloudav.com		34.251.114.126	A (IP address)	IN (0x0001)
Feb 25, 2021 21:41:14.922781944 CET	8.8.8.8	192.168.2.3	0xfcd0	No error (0)	sn.webrootcloudav.com		52.215.10.170	A (IP address)	IN (0x0001)
Feb 25, 2021 21:41:14.922781944 CET	8.8.8.8	192.168.2.3	0xfcd0	No error (0)	sn.webrootcloudav.com		18.202.145.200	A (IP address)	IN (0x0001)
Feb 25, 2021 21:41:14.922781944 CET	8.8.8.8	192.168.2.3	0xfcd0	No error (0)	sn.webrootcloudav.com		54.76.197.132	A (IP address)	IN (0x0001)
Feb 25, 2021 21:41:14.922781944 CET	8.8.8.8	192.168.2.3	0xfcd0	No error (0)	sn.webrootcloudav.com		52.208.207.23	A (IP address)	IN (0x0001)
Feb 25, 2021 21:41:14.922781944 CET	8.8.8.8	192.168.2.3	0xfcd0	No error (0)	sn.webrootcloudav.com		34.249.57.158	A (IP address)	IN (0x0001)
Feb 25, 2021 21:41:15.994520903 CET	8.8.8.8	192.168.2.3	0xe7d9	No error (0)	www.iis.net	iis-umbraco.azurewebsites.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:41:15.994520903 CET	8.8.8.8	192.168.2.3	0xe7d9	No error (0)	iis-umbraco.azurewebsites.net	waws-prod-bay-029.sip.azurewebsites.windows.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 25, 2021 21:41:15.994520903 CET	8.8.8.8	192.168.2.3	0xe7d9	No error (0)	waws-prod-bay-029.sip.azurewebsites.windows.net		40.118.185.161	A (IP address)	IN (0x0001)
Feb 25, 2021 21:41:16.707844019 CET	8.8.8.8	192.168.2.3	0x508d	No error (0)	consentdeliveryfd.azurefd.net	star-azurefd-prod.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:42:22.819511890 CET	8.8.8.8	192.168.2.3	0x4c63	No error (0)	www.iis.net	iis-umbraco.azurewebsites.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:42:22.819511890 CET	8.8.8.8	192.168.2.3	0x4c63	No error (0)	iis-umbraco.azurewebsites.net	waws-prod-bay-029.sip.azurewebsites.windows.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:42:22.819511890 CET	8.8.8.8	192.168.2.3	0x4c63	No error (0)	waws-prod-bay-029.sip.azurewebsites.windows.net		40.118.185.161	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:28.204360008 CET	8.8.8.8	192.168.2.3	0x9c46	No error (0)	login.iis.net	iis-login.azurewebsites.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:42:28.204360008 CET	8.8.8.8	192.168.2.3	0x9c46	No error (0)	iis-login.azurewebsites.net	waws-prod-bay-029.sip.azurewebsites.windows.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:42:28.204360008 CET	8.8.8.8	192.168.2.3	0x9c46	No error (0)	waws-prod-bay-029.sip.azurewebsites.windows.net		40.118.185.161	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:30.718445063 CET	8.8.8.8	192.168.2.3	0x4c51	No error (0)	consentdeliveryfd.azurefd.net	star-azurefd-prod.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:42:30.731864929 CET	8.8.8.8	192.168.2.3	0x9cda	No error (0)	assets.onestore.ms	assets.onestore.ms.akadns.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:42:30.740792990 CET	8.8.8.8	192.168.2.3	0x9350	No error (0)	microsoftwindows.112.2o7.net		15.237.136.106	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:30.740792990 CET	8.8.8.8	192.168.2.3	0x9350	No error (0)	microsoftwindows.112.2o7.net		15.237.76.117	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:30.740792990 CET	8.8.8.8	192.168.2.3	0x9350	No error (0)	microsoftwindows.112.2o7.net		35.181.18.61	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:30.742352962 CET	8.8.8.8	192.168.2.3	0x162c	No error (0)	mem.gfx.ms	cdn.account.microsoft.com.akadns.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:42:30.795320988 CET	8.8.8.8	192.168.2.3	0xc9c	No error (0)	mem.gfx.ms	cdn.account.microsoft.com.akadns.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:42:32.901817083 CET	8.8.8.8	192.168.2.3	0xa510	No error (0)	publisher.liveperson.net	publisher.livepersonk.akadns.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:42:32.901817083 CET	8.8.8.8	192.168.2.3	0xa510	No error (0)	liveperson.map.fastly.net		151.101.1.192	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:32.901817083 CET	8.8.8.8	192.168.2.3	0xa510	No error (0)	liveperson.map.fastly.net		151.101.65.192	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:32.901817083 CET	8.8.8.8	192.168.2.3	0xa510	No error (0)	liveperson.map.fastly.net		151.101.129.192	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:32.901817083 CET	8.8.8.8	192.168.2.3	0xa510	No error (0)	liveperson.map.fastly.net		151.101.193.192	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:34.097850084 CET	8.8.8.8	192.168.2.3	0x94db	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:42:34.538945913 CET	8.8.8.8	192.168.2.3	0xae1f	No error (0)	logincdn.msauth.net	lgincdn.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:42:34.538945913 CET	8.8.8.8	192.168.2.3	0xae1f	No error (0)	cs1227.wpc.alphacdn.net		192.229.221.185	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:37.252001047 CET	8.8.8.8	192.168.2.3	0xabae	No error (0)	github.com		140.82.121.3	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 25, 2021 21:42:37.589566946 CET	8.8.8.8	192.168.2.3	0x9e30	No error (0)	avatars.githubusercontent.com		185.199.108.133	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:37.589566946 CET	8.8.8.8	192.168.2.3	0x9e30	No error (0)	avatars.githubusercontent.com		185.199.111.133	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:37.589566946 CET	8.8.8.8	192.168.2.3	0x9e30	No error (0)	avatars.githubusercontent.com		185.199.110.133	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:37.589566946 CET	8.8.8.8	192.168.2.3	0x9e30	No error (0)	avatars.githubusercontent.com		185.199.109.133	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:47.766391039 CET	8.8.8.8	192.168.2.3	0x4799	No error (0)	dotnetwebsite.azurefd.net	star-azurefd-prod.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:42:49.111641884 CET	8.8.8.8	192.168.2.3	0x9393	No error (0)	sni1gl.wpc.gammacdn.net		152.199.21.175	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:50.178324938 CET	8.8.8.8	192.168.2.3	0x6922	No error (0)	dc.services.visualstudio.com	dc.applicationinsights.microsoft.com		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:42:50.178324938 CET	8.8.8.8	192.168.2.3	0x6922	No error (0)	dc.applicationinsights.azure.com	global.in.ai.monitor.azure.com		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:42:50.178324938 CET	8.8.8.8	192.168.2.3	0x6922	No error (0)	global.in.ai.monitor.azure.com	global.in.ai.privatelink.monitor.azure.com		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:42:50.178324938 CET	8.8.8.8	192.168.2.3	0x6922	No error (0)	global.in.ai.privatelink.monitor.azure.com	dc.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:42:50.494132042 CET	8.8.8.8	192.168.2.3	0x6945	No error (0)	www.asp.net	asp.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:42:50.494132042 CET	8.8.8.8	192.168.2.3	0x6945	No error (0)	asp.net		40.118.185.161	A (IP address)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 25, 2021 21:41:15.063085079 CET	34.253.10.100	443	192.168.2.3	49725	CN=*.webrootcloudav.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Thu May 14 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Mon Jun 14 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 25, 2021 21:41:15.065639973 CET	34.253.10.100	443	192.168.2.3	49726	CN=*.webrootcloudav.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Thu May 14 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Mon Jun 14 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Feb 25, 2021 21:42:33.048290014 CET	151.101.1.192	443	192.168.2.3	49773	CN=liveperson.net, O="LivePerson, Inc.", L=New York, ST=New York, C=US CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE	CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Fri Mar 27 04:17:26 CET 2020 Wed Aug 19 02:00:00 CEST 2015	Sun Mar 28 05:17:26 CEST 2021 Tue Aug 19 02:00:00 CEST 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=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Wed Aug 19 02:00:00 CEST 2015	Tue Aug 19 02:00:00 CEST 2025		
Feb 25, 2021 21:42:33.048917055 CET	151.101.1.192	443	192.168.2.3	49774	CN=liveperson.net, O="LivePerson, Inc.", L=New York, ST=New York, C=US CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE	CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Fri Mar 27 04:17:26 CET 2020 Wed Aug 19 02:00:00 CEST 2015	Sun Mar 28 05:17:26 CEST 2021 Tue Aug 19 02:00:00 CEST 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=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Wed Aug 19 02:00:00 CEST 2015	Tue Aug 19 02:00:00 CEST 2025		
Feb 25, 2021 21:42:34.644218922 CET	192.229.221.185	443	192.168.2.3	49785	CN=identitycdn.msauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Jul 20 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013 Fri Nov 10 01:00:00 CET 2006	Tue Jul 20 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023 Mon Nov 10 01:00:00 CET 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c

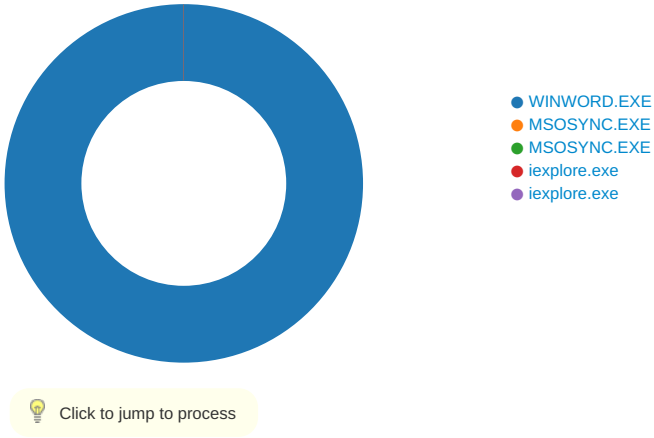
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
Feb 25, 2021 21:42:34.644292116 CET	192.229.221.185	443	192.168.2.3	49784	CN=identitycdn.msauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Jul 20 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013 Fri Nov 10 01:00:00 CET 2006	Tue Jul 20 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023 Mon Nov 10 01:00:00 CET 2031	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=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
Feb 25, 2021 21:42:37.342211008 CET	140.82.121.3	443	192.168.2.3	49789	CN=github.com, O="GitHub, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue May 05 02:00:00 CEST 2020 Tue Oct 22 14:00:00 CEST 2013	Tue May 10 14:00:00 CEST 2022 Sun Oct 22 14:00:00 CEST 2028	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=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Feb 25, 2021 21:42:37.342720985 CET	140.82.121.3	443	192.168.2.3	49791	CN=github.com, O="GitHub, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue May 05 02:00:00 CEST 2020 Tue Oct 22 14:00:00 CEST 2013	Tue May 10 14:00:00 CEST 2022 Sun Oct 22 14:00:00 CEST 2028	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=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Feb 25, 2021 21:42:37.343425035 CET	140.82.121.3	443	192.168.2.3	49790	CN=github.com, O="GitHub, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue May 05 02:00:00 CEST 2020 Tue Oct 22 14:00:00 CEST 2013	Tue May 10 14:00:00 CEST 2022 Sun Oct 22 14:00:00 CEST 2028	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=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 25, 2021 21:42:37.690087080 CET	185.199.108.133	443	192.168.2.3	49792	CN=www.github.com, O="GitHub, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed May 06 02:00:00 CEST 2020 Tue Oct 22 14:00:00 CEST 2013	Thu Apr 14 14:00:00 CEST 2022 Sun Oct 22 14:00:00 CEST 2028	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=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Feb 25, 2021 21:42:37.697190046 CET	185.199.108.133	443	192.168.2.3	49794	CN=www.github.com, O="GitHub, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed May 06 02:00:00 CEST 2020 Tue Oct 22 14:00:00 CEST 2013	Thu Apr 14 14:00:00 CEST 2022 Sun Oct 22 14:00:00 CEST 2028	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=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Feb 25, 2021 21:42:37.697948933 CET	185.199.108.133	443	192.168.2.3	49793	CN=www.github.com, O="GitHub, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed May 06 02:00:00 CEST 2020 Tue Oct 22 14:00:00 CEST 2013	Thu Apr 14 14:00:00 CEST 2022 Sun Oct 22 14:00:00 CEST 2028	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=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Feb 25, 2021 21:42:49.360111952 CET	152.199.21.175	443	192.168.2.3	49804	CN=sni1e6ffgl.wpc.edgecastcdn.net, OU=SecOps, O="Verizon Digital Media Services, Inc.", L=Los Angeles, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Apr 16 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Thu Apr 21 14:00:00 CEST 2022 Wed Mar 08 13:00:00 CET 2023	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=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
Feb 25, 2021 21:42:49.360470057 CET	152.199.21.175	443	192.168.2.3	49805	CN=sni1e6ffgl.wpc.edgecastcdn.net, OU=SecOps, O="Verizon Digital Media Services, Inc.", L=Los Angeles, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Apr 16 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Thu Apr 21 14:00:00 CEST 2022 Wed Mar 08 13:00:00 CET 2023	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=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: WINWORD.EXE PID: 6368 Parent PID: 792

General

Start time:	21:40:37
Start date:	25/02/2021
Path:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE' /Automation -Embedding
Imagebase:	0x12f0000
File size:	1937688 bytes
MD5 hash:	0B9AB9B9C4DE429473D6450D4297A123
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6609977C	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\25299F9C.png	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | delete on close | open no recall	success or wait	1	65FC5805	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\EF142ED.png	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | delete on close | open no recall	success or wait	1	65FC5805	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\6C0FD40A.jpeg	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | delete on close | open no recall	success or wait	1	65FC5805	unknown
C:\Users\user\AppData\Local\Temp\imgs\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	65FC5805	unknown
C:\Users\user\AppData\Local\Temp\imgs\item0001.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	65FC5805	unknown
C:\Users\user\AppData\Local\Temp\imgs\props002.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	65FC5805	unknown
C:\Users\user\AppData\Local\Temp\imgs\item0003.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	65FC5805	unknown
C:\Users\user\AppData\Local\Temp\imgs\props004.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	65FC5805	unknown
C:\Users\user\AppData\Local\Temp\imgs\item0005.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	65FC5805	unknown
C:\Users\user\AppData\Local\Temp\imgs\props006.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	65FC5805	unknown
C:\Users\user\AppData\Local\Temp\imgs\item0007.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	65FC5805	unknown
C:\Users\user\AppData\Local\Temp\imgs\props008.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	65FC5805	unknown
C:\Users\user\AppData\Local\Temp\imgs\theme.thm	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	65FC5805	unknown
C:\Users\user\AppData\Local\Temp\imgs\cscheme.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	65FC5805	unknown
C:\Users\user\AppData\Local\Temp\imgs\header.htm	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	65FC5805	unknown
C:\Users\user\AppData\Local\Temp\imgs\filelist.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	65FC5805	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$21-02-18 Fivoor - Overleg - Kwartaaloverleg.docx	success or wait	1	65FC5805	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\25299F9C.png	0	59420	89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 02 8e 00 00 03 9b 08 06 00 00 00 dd 62 00 7c 00 00 00 01 73 52 47 42 00 ae ce 1c e9 00 00 00 09 70 48 59 73 00 00 0e c4 00 00 0e c4 01 95 2b 0e 1b 00 00 00 19 74 45 58 74 53 6f 66 74 77 61 72 65 00 4d 69 63 72 6f 73 6f 66 74 20 4f 66 66 69 63 65 7f ed 35 71 00 00 e7 9c 49 44 41 54 78 5e ec 9d 05 80 1d d5 d5 c7 4f 76 37 ee ee 09 21 04 49 08 ee 04 77 2d ae 2d 52 ac b4 94 52 a4 82 94 22 a5 48 5b ac 38 c5 3e 28 ee 52 dc dd dd 03 49 20 ee ae bb fb 9d ff 9d 37 bb 93 97 b7 bb 6f 43 08 37 9b df 6d 97 ec be 37 6f e6 cc ef dc 37 f3 9f 73 ef 39 b7 ac d2 9b d1 20 00 01 08 40 00 02 10 80 00 04 20 50 0b 81 b3 cf 3e bb 51 19 84 20 00 01 08 40 00 02 10 80 00 04 20 50 0c 01 84 63 31 94 d8 06 02 10 80 00 04 20 00 01 08	.PNG.....IHDR..... b.|....sRGB.....pHYs..... ....+.....tEXtSoftware.Microsoft Office..5q....IDATx^..... ..Ov7...!.I...w-.-R...R...".H[.8.>(.R....I .....7.....oC.7 ..m...7o....7..s.9..... ...@.. .... P....>.Q.. ...@..... P.. .c1..... ...	success or wait	1	65FC5805	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\EF142ED.png	0	3055	89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 af 00 00 00 51 08 02 00 00 00 2b 68 61 4b 00 00 00 01 73 52 47 42 00 ae ce 1c e9 00 00 0b a9 49 44 41 54 78 5e ed 5c 09 90 15 c5 19 fe 97 88 08 e8 c2 72 b8 0a c2 02 72 2d 28 97 88 20 68 40 42 88 11 50 22 49 d4 94 89 1c 82 84 14 21 1a 4d 45 f1 88 31 a5 18 83 21 60 bc a2 41 8a 4b 12 0b 41 63 40 11 10 58 51 10 65 41 56 90 53 01 01 17 04 16 57 4e 25 5f 6f bf d7 d3 d3 73 f5 ac 6f 67 5e de eb bf 5e 6d bd 37 d3 dd d3 fd ff df fc fd 5f bd 39 a7 4f 9f 26 43 86 03 15 1c a8 66 f8 60 38 20 38 60 d0 60 c0 60 71 c0 a0 c1 a0 c1 a0 c1 60 c0 8d 03 46 37 18 5c 18 dd 60 30 60 74 83 c1 80 3f 07 cc 4e 61 10 62 76 0a 83 01 b3 53 18 0c 98 9d c2 60 40 97 03 c6 6e d0 e5 54 36 b4 33 68 c8 06 29 eb ae d1 a0 41 97 53 d9 d0 ce	.PNG.....IHDR.....Q.....+ haK....sRGB.....IDATx^.\ .....r....r-(.. h@B..P"I.. .....!.ME..1...!`..A.K..Ac@.. X Q.eAV.S.....WN%_o....s..o g^... ^m.7....._.9.O.&C.....f.`8 8`.`.`q.....`...F7.\..`0`t.. .?..Na.bv....S.....`@...n..T6. 3h..)....A.S...	success or wait	1	65FC5805	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\6C0FD40A.jpeg	0	23216	ff d8 ff e0 00 10 4a 46 49 46 00 01 01 01 00 48 00 48 00 00 ff db 00 43 00 08 06 06 07 06 05 08 07 07 07 09 09 08 0a 0c 14 0d 0c 0b 0b 0c 19 12 13 0f 14 1d 1a 1f 1e 1d 1a 1c 1c 20 24 2e 27 20 22 2c 23 1c 1c 28 37 29 2c 30 31 34 34 34 1f 27 39 3d 38 32 3c 2e 33 34 32 ff db 00 43 01 09 09 09 0c 0b 0c 18 0d 0d 18 32 21 1c 21 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 ff c0 00 11 08 00 e0 04 00 03 01 22 00 02 11 01 03 11 01 ff c4 00 1f 00 00 01 05 01 01 01 01 01 01 00 00 00 00 00 00 00 00 01 02 03 04 05 06 07 08 09 0a 0b ff c4 00 b5 10 00 02 01 03 03 02 04 03 05 05 04 04 00 00 01 7d 01 02 03 00 04 11 05 12 21 31 41 06 13 51 61 07 22 71 14 32 81 91 a1 08	......JFIF.....H.H.....C...... .... $.' ",#.. (7),01444.'9=82<.342. ..C..........2!.!22222222222 2 2222222222222222222222222 22222222 22222222..........."........... ....}........! 1A..Qa."q.2....	success or wait	1	65FC5805	unknown
C:\Users\user\AppData\Local\Temp\imgs\props002.xml	unknown	425	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 6e 6f 22 3f 3e 0d 0a 3c 64 73 3a 64 61 74 61 73 74 6f 72 65 49 74 65 6d 20 64 73 3a 69 74 65 6d 49 44 3d 22 7b 43 36 34 44 44 30 32 31 2d 43 35 35 39 2d 34 38 41 33 2d 41 43 38 36 2d 34 34 30 36 43 39 33 32 37 44 33 34 7d 22 20 78 6d 6c 6e 73 3a 64 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6f 70 65 6e 78 6d 6c 66 6f 72 6d 61 74 73 2e 6f 72 67 2f 6f 66 66 69 63 65 44 6f 63 75 6d 65 6e 74 2f 32 30 30 36 2f 63 75 73 74 6f 6d 58 6d 6c 22 3e 3c 64 73 3a 73 63 68 65 6d 61 52 65 66 73 3e 3c 64 73 3a 73 63 68 65 6d 61 52 65 66 20 64 73 3a 75 72 69 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63	<?xml version="1.0" encoding="UTF-8" standalone="no"?>..<ds:datastoreItem ds:itemID="{C64DD021-C559-48A3-AC86-4406C9327D34}" xmlns:ds="http://schemas.openxmlformats.org/officeDocument/2006/customXml"><ds:schemaRefs><ds:schemaRef ds:uri="http://schemas.mic	success or wait	1	65FC5805	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\imgs\item0001.xml	unknown	290	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 75 74 66 2d 38 22 3f 3e 3c 70 3a 70 72 6f 70 65 72 74 69 65 73 20 78 6d 6c 6e 73 3a 70 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 6f 66 66 69 63 65 2f 32 30 30 36 2f 6d 65 74 61 64 61 74 61 2f 70 72 6f 70 65 72 74 69 65 73 22 20 78 6d 6c 6e 73 3a 78 73 69 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 31 2f 58 4d 4c 53 63 68 65 6d 61 2d 69 6e 73 74 61 6e 63 65 22 20 78 6d 6c 6e 73 3a 70 63 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 6f 66 66 69 63 65 2f 69 6e 66 6f 70 61 74 68 2f 32 30 30 37 2f 50 61 72 74 6e 65 72 43 6f 6e 74 72 6f 6c 73 22 3e 3c	<?xml version="1.0" encoding="utf-8"?> <p:properties xmlns:p= "http://schemas.microsoft.com/ office/2006/metadata/properties" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xml ns:pc="http://schemas.microsoft.com/office/infopath/2007/PartnerControls"><	success or wait	1	65FC5805	unknown
C:\Users\user\AppData\Local\Temp\imgs\item0003.xml	unknown	4096	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 3f 3e 3c 63 74 3a 63 6f 6e 74 65 6e 74 54 79 70 65 53 63 68 65 6d 61 20 63 74 3a 5f 3d 22 22 20 6d 61 3a 5f 3d 22 22 20 6d 61 3a 63 6f 6e 74 65 6e 74 54 79 70 65 4e 61 6d 65 3d 22 44 6f 63 75 6d 65 6e 74 22 20 6d 61 3a 63 6f 6e 74 65 6e 74 54 79 70 65 49 44 3d 22 30 78 30 31 30 31 30 30 34 38 42 41 45 38 33 41 33 36 30 34 43 35 34 43 38 34 46 32 41 42 44 33 37 36 42 32 30 44 35 39 22 20 6d 61 3a 63 6f 6e 74 65 6e 74 54 79 70 65 56 65 72 73 69 6f 6e 3d 22 31 30 22 20 6d 61 3a 63 6f 6e 74 65 6e 74 54 79 70 65 44 65 73 63 72 69 70 74 69 6f 6e 3d 22 43 72 65 61 74 65 20 61 20 6e 65 77 20 64 6f 63 75 6d 65 6e 74 2e 22 20 6d 61 3a 63 6f 6e 74 65 6e 74 54 79 70 65 53 63 6f 70 65 3d 22 22 20 6d 61 3a 76 65	<?xml version="1.0"?> <ct:contentTypeSchema ct:_="" ma:_="" m a:contentTypeName="Document" m a:contentTypeID="0x01010048BAE 83A3604C54C84F2ABD376B20D59" m a:contentTypeVersion="10" ma:contentTypeDescr iption="Create a new d ocument." ma:contentTypeScope="" ma:ve	success or wait	1	65FC5805	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\imgs\item0003.xml	unknown	4096	3e 0d 0a 3c 78 73 64 3a 65 6c 65 6d 65 6e 74 20 6e 61 6d 65 3d 22 4d 65 64 69 61 53 65 72 76 69 63 65 41 75 74 6f 4b 65 79 50 6f 69 6e 74 73 22 20 6d 61 3a 69 6e 64 65 78 3d 22 31 36 22 20 6e 69 6c 6c 61 62 6c 65 3d 22 74 72 75 65 22 20 6d 61 3a 64 69 73 70 6c 61 79 4e 61 6d 65 3d 22 4d 65 64 69 61 53 65 72 76 69 63 65 41 75 74 6f 4b 65 79 50 6f 69 6e 74 73 22 20 6d 61 3a 68 69 64 64 65 6e 3d 22 74 72 75 65 22 20 6d 61 3a 69 6e 74 65 72 6e 61 6c 4e 61 6d 65 3d 22 4d 65 64 69 61 53 65 72 76 69 63 65 41 75 74 6f 4b 65 79 50 6f 69 6e 74 73 22 20 6d 61 3a 72 65 61 64 4f 6e 6c 79 3d 22 74 72 75 65 22 3e 0d 0a 3c 78 73 64 3a 73 69 6d 70 6c 65 54 79 70 65 3e 0d 0a 3c 78 73 64 3a 72 65 73 74 72 69 63 74 69 6f 6e 20 62 61 73 65 3d 22 64 6d 73 3a 4e 6f 74 65 22 2f	>..<xsd:element name="MediaServiceAutoKeyPoints" ma:index="16" nillable="true" ma:displayName="MediaServiceAutoKeyPoints" ma:hidden="true" ma:internalName="MediaServiceAutoKeyPoints" ma:readOnly="true">..<xsd:simpleType>..<xsd:restriction base="dms:Note"/	success or wait	1	65FC5805	unknown
C:\Users\user\AppData\Local\Temp\imgs\props004.xml	unknown	1149	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 6e 6f 22 3f 3e 0d 0a 3c 64 73 3a 64 61 74 61 73 74 6f 72 65 49 74 65 6d 20 64 73 3a 69 74 65 6d 49 44 3d 22 7b 44 32 41 32 30 30 43 43 2d 46 42 36 32 2d 34 31 32 32 2d 38 44 34 31 2d 43 30 39 42 41 34 42 31 31 31 39 35 7d 22 20 78 6d 6c 6e 73 3a 64 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6f 70 65 6e 78 6d 6c 66 6f 72 6d 61 74 73 2e 6f 72 67 2f 6f 66 66 69 63 65 44 6f 63 75 6d 65 6e 74 2f 32 30 30 36 2f 63 75 73 74 6f 6d 58 6d 6c 22 3e 3c 64 73 3a 73 63 68 65 6d 61 52 65 66 73 3e 3c 64 73 3a 73 63 68 65 6d 61 52 65 66 20 64 73 3a 75 72 69 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63	<?xml version="1.0" encoding="UTF-8" standalone="no"?>..<ds:datastoreItem ds:itemID="{D2A200CC-FB62-4122-8D41-C09BA4B11195}" xmlns:ds="http://schemas.openxmlformats.org/officeDocument/2006/customXml"><ds:schemaRefs><ds:schemaRef ds:uri="http://schemas.mic	success or wait	1	65FC5805	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\imgs\item0003.xml	unknown	3475	69 73 20 72 65 73 70 6f 6e 73 69 62 6c 65 20 66 6f 72 20 75 70 64 61 74 69 6e 67 20 74 68 69 73 20 76 61 6c 75 65 20 61 66 74 65 72 20 65 61 63 68 20 72 65 76 69 73 69 6f 6e 2e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 2f 78 73 64 3a 64 6f 63 75 6d 65 6e 74 61 74 69 6f 6e 3e 0d 0a 3c 2f 78 73 64 3a 61 6e 6e 6f 74 61 74 69 6f 6e 3e 0d 0a 3c 2f 78 73 64 3a 65 6c 65 6d 65 6e 74 3e 0d 0a 3c 78 73 64 3a 65 6c 65 6d 65 6e 74 20 6e 61 6d 65 3d 22 6c 61 73 74 4d 6f 64 69 66 69 65 64 42 79 22 20 6d 69 6e 4f 63 63 75 72 73 3d 22 30 22 20 6d 61 78 4f 63 63 75 72 73 3d 22 31 22 20 74 79 70 65 3d 22 78 73 64 3a 73 74 72 69 6e 67 22 2f 3e 0d 0a 3c 78 73 64 3a 65 6c 65 6d 65 6e 74 20 72 65 66 3d 22 64 63 74 65 72 6d 73 3a 6d 6f 64 69 66 69 65	is responsible for updating this value after each revision... </xsd:documentation>.. </xsd:annotation>.. </xsd:element>.. <xsd:element name="lastModifiedBy" minOccurs="0" maxOccurs="1" type="xsd :string"/>..<xsd:element ref="dcterms:modifie	success or wait	1	65FC5805	unknown
C:\Users\user\AppData\Local\Temp\imgs\props006.xml	unknown	335	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 6e 6f 22 3f 3e 0d 0a 3c 64 73 3a 64 61 74 61 73 74 6f 72 65 49 74 65 6d 20 64 73 3a 69 74 65 6d 49 44 3d 22 7b 31 33 43 46 34 32 33 32 2d 46 34 39 42 2d 34 34 39 39 2d 39 36 39 41 2d 34 36 35 46 37 31 44 36 43 30 44 38 7d 22 20 78 6d 6c 6e 73 3a 64 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6f 70 65 6e 78 6d 6c 66 6f 72 6d 61 74 73 2e 6f 72 67 2f 6f 66 66 69 63 65 44 6f 63 75 6d 65 6e 74 2f 32 30 30 36 2f 63 75 73 74 6f 6d 58 6d 6c 22 3e 3c 64 73 3a 73 63 68 65 6d 61 52 65 66 73 3e 3c 64 73 3a 73 63 68 65 6d 61 52 65 66 20 64 73 3a 75 72 69 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63	<?xml version="1.0" encoding="UTF-8" standalone="no"?>..<ds: datastoreItem ds:itemID="{13CF4232-F49B-4499-969A-465F71D6C0D8}" xmlns:ds="http://schemas.openxmlformats.org/officeDocum ent/2006/customXml"> <ds:schemaRefs> <ds:schemaRef ds:uri="http://schemas.mic	success or wait	1	65FC5805	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\imgs\item0005.xml	unknown	219	3c 3f 6d 73 6f 2d 63 6f 6e 74 65 6e 74 54 79 70 65 3f 3e 3c 46 6f 72 6d 54 65 6d 70 6c 61 74 65 73 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 73 68 61 72 65 70 6f 69 6e 74 2f 76 33 2f 63 6f 6e 74 65 6e 74 74 79 70 65 2f 66 6f 72 6d 73 22 3e 3c 44 69 73 70 6c 61 79 3e 44 6f 63 75 6d 65 6e 74 4c 69 62 72 61 72 79 46 6f 72 6d 3c 2f 44 69 73 70 6c 61 79 3e 3c 45 64 69 74 3e 44 6f 63 75 6d 65 6e 74 4c 69 62 72 61 72 79 46 6f 72 6d 3c 2f 45 64 69 74 3e 3c 4e 65 77 3e 44 6f 63 75 6d 65 6e 74 4c 69 62 72 61 72 79 46 6f 72 6d 3c 2f 4e 65 77 3e 3c 2f 46 6f 72 6d 54 65 6d 70 6c 61 74 65 73 3e	<?mso-contentType?><FormTemplates xmlns="http://schemas.microsoft.com/sharepoint/v3/contenttype/forms"><Display>DocumentLibraryForm</Display><Edit>DocumentLibraryForm</Edit><New>DocumentLibraryForm</New></FormTemplates>	success or wait	1	65FC5805	unknown
C:\Users\user\AppData\Local\Temp\imgs\props008.xml	unknown	341	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 6e 6f 22 3f 3e 0d 0a 3c 64 73 3a 64 61 74 61 73 74 6f 72 65 49 74 65 6d 20 64 73 3a 69 74 65 6d 49 44 3d 22 7b 45 44 45 42 37 30 44 35 2d 46 33 37 39 2d 34 42 37 43 2d 42 42 31 35 2d 38 38 35 41 37 36 36 37 31 31 31 34 37 7d 22 20 78 6d 6c 6e 73 3a 64 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6f 70 65 6e 78 6d 6c 66 6f 72 6d 61 74 73 2e 6f 72 67 2f 6f 66 66 69 63 65 44 6f 63 75 6d 65 6e 74 2f 32 30 30 36 2f 63 75 73 74 6f 6d 58 6d 6c 22 3e 3c 64 73 3a 73 63 68 65 6d 61 52 65 66 73 3e 3c 64 73 3a 73 63 68 65 6d 61 52 65 66 20 64 73 3a 75 72 69 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6f 70 65	<?xml version="1.0" encoding="UTF-8" standalone="no"?>..<ds:datastoreItem ds:itemID="{EDEB70D5-F379-4B7C-BB15-885A76671147}" xmlns:ds="http://schemas.openxmlformats.org/officeDocument/2006/customXml"><ds:schemaRefs><ds:schemaRef ds:uri="http://schemas.ope	success or wait	1	65FC5805	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\imgs\item0007.xml	unknown	306	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 6e 6f 22 3f 3e 3c 62 3a 53 6f 75 72 63 65 73 20 78 6d 6c 6e 73 3a 62 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6f 70 65 6e 78 6d 6c 66 6f 72 6d 61 74 73 2e 6f 72 67 2f 6f 66 66 69 63 65 44 6f 63 75 6d 65 6e 74 2f 32 30 30 36 2f 62 69 62 6c 69 6f 67 72 61 70 68 79 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6f 70 65 6e 78 6d 6c 66 6f 72 6d 61 74 73 2e 6f 72 67 2f 6f 66 66 69 63 65 44 6f 63 75 6d 65 6e 74 2f 32 30 30 36 2f 62 69 62 6c 69 6f 67 72 61 70 68 79 22 20 53 65 6c 65 63 74 65 64 53 74 79 6c 65 3d 22 5c 41 50 41 53 69 78 74 68 45 64 69 74 69 6f 6e 4f 66 66 69 63 65 4f	<?xml version="1.0" encoding="UTF-8" standalone="no"?><b:Sources xmlns:b="http://schemas.openxmlformats.org/officeDocument/2006/bibliography" xmlns="http://schemas.openxmlformats.org/officeDocument/2006/bibliography" SelectedStyle="\APASixthEditionOfficeO	success or wait	1	65FC5805	unknown
C:\Users\user\AppData\Local\Temp\imgs\theme.thm	unknown	3138	50 4b 03 04 14 00 06 00 08 00 00 00 21 00 e9 de 0f bf ff 00 00 00 1c 02 00 00 13 00 00 00 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c ac 91 cb 4e c3 30 10 45 f7 48 fc 83 e5 2d 4a 9c b2 40 08 25 e9 82 c7 8e c7 a2 7c c0 c8 99 24 16 c9 d8 b2 a7 55 fb f7 4c d2 54 42 a8 20 16 6c 2c d9 33 f7 9e 3b e3 72 bd 1f 07 b5 c3 98 9c a7 4a af f2 42 2b 24 eb 1b 47 5d a5 df 37 4f d9 ad 56 89 81 1a 18 3c 61 a5 0f 98 f4 ba be bc 28 37 87 80 49 89 9a 52 a5 7b e6 70 67 4c b2 3d 8e 90 72 1f 90 a4 d2 fa 38 02 cb 35 76 26 80 fd 80 0e cd 75 51 dc 18 eb 89 91 38 e3 c9 43 d7 e5 03 b6 b0 1d 58 3d ee e5 f9 98 24 e2 90 b4 ba 3f 36 4e ac 4a 43 08 83 b3 c0 92 d4 ec a8 f9 46 c9 16 42 2e ca b9 27 f5 2e a4 2b 89 a1 cd 59 c2 54 f9 19 b0 e8 5e 65 35 d1 35 a8 de 20 f2 0b 8c 12 c3	PK.....!..... [Content_Types].xml...N.0. E.H...- J..@.%.....|...$.....U..L.TB. .l,.3..;.r.....J..B+$.. G]..7O..V....<a.....(7..I..R. {.pgL.=..r.....8..5v&.....uQ. ....8..C.....X=....$....?6N.J C.....F..B...'...+...Y.T.. ..^e5.5..	success or wait	1	65FC5805	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\imgs\cscheme.xml	unknown	314	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 61 3a 63 6c 72 4d 61 70 20 78 6d 6c 6e 73 3a 61 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6f 70 65 6e 78 6d 6c 66 6f 72 6d 61 74 73 2e 6f 72 67 2f 64 72 61 77 69 6e 67 6d 6c 2f 32 30 30 36 2f 6d 61 69 6e 22 20 62 67 31 3d 22 6c 74 31 22 20 74 78 31 3d 22 64 6b 31 22 20 62 67 32 3d 22 6c 74 32 22 20 74 78 32 3d 22 64 6b 32 22 20 61 63 63 65 6e 74 31 3d 22 61 63 63 65 6e 74 31 22 20 61 63 63 65 6e 74 32 3d 22 61 63 63 65 6e 74 32 22 20 61 63 63 65 6e 74 33 3d 22 61 63 63 65 6e 74 33 22 20 61 63 63 65 6e 74 34 3d 22 61 63 63 65 6e 74 34 22 20 61 63 63 65 6e 74 35 3d 22 61 63 63	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<a: clrMap xmlns:a="http://schemas .openxmlformats.org/drawi ngml/2006/main" bg1="lt1" tx1="dk1" bg2="lt2" tx2="dk2" accent1=" accent1" accent2="accent2" acc ent3="accent3" accent4="accent4" accent5="acc	success or wait	1	65FC5805	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{31CB24EF-1DEB-4C38-BB46-32AB8B1362AD}.tmp	unknown	1024	7a 00 69 00 6a 00 6e 00 20 00 70 00 72 00 69 00 6d 00 61 00 69 00 72 00 20 00 61 00 61 00 6e 00 73 00 70 00 72 00 65 00 65 00 6b 00 70 00 75 00 6e 00 74 00 20 00 65 00 6e 00 20 00 4a 00 57 00 20 00 6d 00 65 00 65 00 6e 00 65 00 6d 00 65 00 6e 00 20 00 69 00 6e 00 20 00 64 00 65 00 20 00 43 00 43 00 20 00 76 00 61 00 6e 00 20 00 65 00 6d 00 61 00 69 00 6c 00 20 00 63 00 6f 00 6d 00 6d 00 75 00 6e 00 69 00 63 00 61 00 74 00 69 00 65 00 2e 00 0d 00 0d 00 0d 00 09 00 2f 00 0d 00 2f 00 0d 00 2f 00 46 00 69 00 76 00 6f 00 6f 00 72 00 20 00 13 20 20 00 56 00 65 00 72 00 62 00 65 00 74 00 65 00 72 00 69 00 6e 00 67 00 65 00 6e 00 20 00 6f 00 6d 00 67 00 65 00 76 00 69 00 6e 00 67 00 09 00 20 00 50 00 41 00 47 00 45 00 20 00 38 00 15 00 14 00 13 00 09 00 0d 00 0d	z.i.j.n. .p.r.i.m.a.i.r. .a.a. n.s.p.r.e.e.k.p.u.n.t. .e.n. . J.W. .m.e.e.n.e.m.e.n. .i.n. .d.e. .C.C. .v.a.n. .e.m.a.i.l. .c.o.m.m.u.n.i.c.a.t.i.e..... ...../.../.../.F.i.v.o.o.r. .. .V.e.r.b.e.t.e.r.i.n.g.e.n. .o.m.g.e.v.i.n.g... .P.A.G.E. .8.....	success or wait	2	65FC5805	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\imgs\header.htm	unknown	2627	38 5a 4f 32 32 36 41 6f 54 45 61 69 39 4f 78 70 37 33 50 4f 2f 4e 65 48 31 37 74 49 59 64 49 45 54 74 73 4f 50 4e 6f 75 59 4d 55 4c 70 65 34 37 37 6a 33 37 38 39 76 48 6e 50 0d 0a 57 55 77 43 65 32 45 63 51 73 64 50 45 50 6e 74 35 76 57 72 39 65 68 62 57 4c 72 42 6d 52 34 43 49 78 4b 4d 37 65 67 37 50 71 54 6b 32 36 71 4b 63 67 41 72 34 73 4a 35 51 44 70 55 4c 6c 69 52 4b 41 7a 37 71 67 39 69 4a 48 5a 72 0d 0a 71 6d 56 64 72 36 72 52 68 64 34 48 4a 79 46 47 32 72 32 66 44 76 6d 6d 38 43 73 46 4d 6e 31 52 4b 6b 4a 69 70 75 4e 55 57 79 70 72 4b 4f 73 75 72 39 56 6d 4c 64 70 39 45 48 37 51 38 6c 79 47 65 45 59 56 56 6d 69 6b 53 32 65 71 0d 0a 65 35 45 45 2b 78 6e 30 48 31 52 57 79 2b 43 69 55 32 6b 68 6e 61 32 63 55 6c 70 43 30 55 42 71 6d 76 6f 33 4e 56 38	8ZO226AoTEai9Oxp73PO /NeH17tlYd IETtsOPNouYMULpe477j3 789vHnP.. WUwCe2EcQsdPEPnt5v Wr9ehbWLrBmR 4CIxKM7eg7PqTk26qKcg Ar4sJ5QDpU LliRKAz7qg9iJHZr..qmVdr 6rRhd4H JyFG2r2fDvmm8CsFMn1 RKkJipuNUWy prKOsur9VmLdp9EH7Q8ly GeEYVVmik S2eq..e5EE+xn0H1RWy+ CiU2khna2c UlpC0UBqmvo3NV8	success or wait	1	65FC5805	unknown
C:\Users\user\AppData\Local\Temp\imgs\filelist.xml	unknown	626	3c 78 6d 6c 20 78 6d 6c 6e 73 3a 6f 3d 22 75 72 6e 3a 73 63 68 65 6d 61 73 2d 6d 69 63 72 6f 73 6f 66 74 2d 63 6f 6d 3a 6f 66 66 69 63 65 3a 6f 66 66 69 63 65 22 3e 0d 0a 20 3c 6f 3a 4d 61 69 6e 46 69 6c 65 20 48 52 65 66 3d 22 2e 2e 2f 69 6d 67 73 2e 68 74 6d 22 2f 3e 0d 0a 20 3c 6f 3a 46 69 6c 65 20 48 52 65 66 3d 22 69 74 65 6d 30 30 30 31 2e 78 6d 6c 22 2f 3e 0d 0a 20 3c 6f 3a 46 69 6c 65 20 48 52 65 66 3d 22 70 72 6f 70 73 30 30 32 2e 78 6d 6c 22 2f 3e 0d 0a 20 3c 6f 3a 46 69 6c 65 20 48 52 65 66 3d 22 69 74 65 6d 30 30 30 33 2e 78 6d 6c 22 2f 3e 0d 0a 20 3c 6f 3a 46 69 6c 65 20 48 52 65 66 3d 22 70 72 6f 70 73 30 30 34 2e 78 6d 6c 22 2f 3e 0d 0a 20 3c 6f 3a 46 69 6c 65 20 48 52 65 66 3d 22 69 74 65 6d 30 30 30 35 2e 78 6d 6c 22 2f 3e 0d 0a 20 3c 6f	<xml xmlns:o="urn:schemas-microsoft-com:office:office">.. <o :MainFile HRef="../imgs.htm"/>.. <o:File HRef="item0001.xml"/>.. <o:File HRef="props002.xml"/>.. <o:File HRef="item0003.xml"/>.. <o:File HRef="props004.xml"/>.. <o:File HRef="item0005.xml"/>.. <o	success or wait	1	65FC5805	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\2021-02-18 Fivoor - Overleg - Kwartaaloverleg.docx	81486	59420	success or wait	3	65FC5805	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{31CB24EF-1DEB-4C38-BB46-32AB8B1362AD}.tmp	unknown	512	success or wait	1	65FC5805	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{31CB24EF-1DEB-4C38-BB46-32AB8B1362AD}.tmp	unknown	512	success or wait	1	65FC5805	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{31CB24EF-1DEB-4C38-BB46-32AB8B1362AD}.tmp	unknown	512	success or wait	12	65FC5805	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{31CB24EF-1DEB-4C38-BB46-32AB8B1362AD}.tmp	unknown	512	success or wait	1	65FC5805	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{31CB24EF-1DEB-4C38-BB46-32AB8B1362AD}.tmp	unknown	512	success or wait	5	65FC5805	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{31CB24EF-1DEB-4C38-BB46-32AB8B1362AD}.tmp	unknown	512	success or wait	4	65FC5805	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{31CB24EF-1DEB-4C38-BB46-32AB8B1362AD}.tmp	unknown	512	success or wait	1	65FC5805	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{31CB24EF-1DEB-4C38-BB46-32AB8B1362AD}.tmp	unknown	512	success or wait	19	65FC5805	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{31CB24EF-1DEB-4C38-BB46-32AB8B1362AD}.tmp	unknown	55	success or wait	38	65FC5805	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{31CB24EF-1DEB-4C38-BB46-32AB8B1362AD}.tmp	unknown	512	success or wait	9	65FC5805	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{31CB24EF-1DEB-4C38-BB46-32AB8B1362AD}.tmp	unknown	512	success or wait	2	65FC5805	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{31CB24EF-1DEB-4C38-BB46-32AB8B1362AD}.tmp	unknown	512	success or wait	155	65FC5805	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{31CB24EF-1DEB-4C38-BB46-32AB8B1362AD}.tmp	unknown	512	success or wait	1	65FC5805	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{31CB24EF-1DEB-4C38-BB46-32AB8B1362AD}.tmp	unknown	264	success or wait	1	65FC5805	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{31CB24EF-1DEB-4C38-BB46-32AB8B1362AD}.tmp	unknown	512	success or wait	1	65FC5805	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{31CB24EF-1DEB-4C38-BB46-32AB8B1362AD}.tmp	unknown	512	success or wait	1	65FC5805	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{31CB24EF-1DEB-4C38-BB46-32AB8B1362AD}.tmp	unknown	512	success or wait	2	65FC5805	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{31CB24EF-1DEB-4C38-BB46-32AB8B1362AD}.tmp	unknown	512	success or wait	1	65FC5805	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	65FD8A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1	success or wait	1	65FD8A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common	success or wait	1	65FD8A84	RegCreateKeyExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	success or wait	1	65FC5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery	success or wait	1	65FC5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery\20074	success or wait	1	65FC5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations	success or wait	1	65FC5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	success or wait	1	65FC5805	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Name	unicode	Recover Text from Any File	success or wait	1	65FC5805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Path	unicode	C:\Program Files (x86)\Common Files\Microsoft Shared\TextConv\RECOVR32.CNV	success or wait	1	65FC5805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Extensions	unicode	*	success or wait	1	65FC5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Cambria Math	binary	02 04 05 03 05 04 06 03 02 04	success or wait	1	65FC5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Century Gothic	binary	02 0B 05 02 02 02 02 02 02 04	success or wait	1	65FC5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Verdana	binary	02 0B 06 04 03 05 04 04 02 04	success or wait	1	65FC5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Tahoma	binary	02 0B 06 04 03 05 04 04 02 04	success or wait	1	65FC5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Cambria	binary	02 04 05 03 05 04 06 03 02 04	success or wait	1	65FC5805	unknown
HKEY_CURRENT_USER\Software\Mic	20074	binary		success or wait	1	65FC5805	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery\20074	20074	binary	04 00 00 00 E0 18 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 68 00 61 00 72 00 64 00 7A 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 08 00 00 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 00 00 00 00 01 00 00 00 00 00 00 00 9A 62 32 00 02 0C D7 01 74 00 02 00 74 00 02 00 00 00 00 00 DB 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	[illegible]	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00				
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	File Path	unicode	C:\Users\user\AppData\Local\Temp\imgs.htm	success or wait	1	65FC5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	Datetime	unicode	2021-02-25T21:41	success or wait	1	65FC5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	Position	unicode	2032632766 0	success or wait	1	65FC5805	unknown

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109110000000000000000F01FEC\Usage	ProductFiles	dword	1381564438	1381564439	success or wait	1	65FC5805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109110000000000000000F01FEC\Usage	ProductFiles	dword	1381564439	1381564440	success or wait	1	65FC5805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Name	unicode	Recover Text from Any File	WordPerfect 5.x	success or wait	1	65FC5805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Path	unicode	C:\Program Files (x86)\Common Files\Microsoft Shared\TextConv\RECOVR32.CNV	C:\Program Files (x86)\Common Files\Microsoft Shared\TextConv\WPFT532.CNV	success or wait	1	65FC5805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Extensions	unicode	*	doc	success or wait	1	65FC5805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Name	unicode	WordPerfect 5.x	WordPerfect 6.x - 7.0	success or wait	1	65FC5805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Path	unicode	C:\Program Files (x86)\Common Files\Microsoft Shared\TextConv\WPFT532.CNV	C:\Program Files (x86)\Common Files\Microsoft Shared\TextConv\WPFT632.CNV	success or wait	1	65FC5805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Extensions	unicode	doc	wpd doc	success or wait	1	65FC5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery\20074	20074	binary	04 00 00 00 E0 18 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 68 00 61 00 72 00 64 00 7A 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 08 00 00 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 00 00 00 00 01 00 00 00 00 00 00 00 9A 62 32 00 02 0C D7 01 74 00 02 00 74 00 02 00 00 00 00 00 DB 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	04 00 00 00 E0 18 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 68 00 61 00 72 00 64 00 7A 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 08 00 00 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 74 00 02 00 74 00 02 00 00 00 00 00 DB 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	65FC5805	unknown

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

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

Analysis Process: MSOSYNC.EXE PID: 6552 Parent PID: 6368

General

Start time:	21:40:40
Start date:	25/02/2021
Path:	C:\Program Files (x86)\Microsoft Office\Office16\MSOSYNC.EXE
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\Microsoft Office\Office16\MsoSync.exe
Imagebase:	0x13a0000
File size:	466688 bytes
MD5 hash:	EA19F4A0D18162BE3A0C8DAD249ADE8C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: MSOSYNC.EXE PID: 6568 Parent PID: 6368

General

Start time:	21:40:40
Start date:	25/02/2021
Path:	C:\Program Files (x86)\Microsoft Office\Office16\MSOSYNC.EXE
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\Microsoft Office\Office16\MsoSync.exe
Imagebase:	0x13a0000
File size:	466688 bytes
MD5 hash:	EA19F4A0D18162BE3A0C8DAD249ADE8C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: iexplore.exe PID: 6732 Parent PID: 792

General

Start time:	21:41:10
Start date:	25/02/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff682d10000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: iexplore.exe PID: 6816 Parent PID: 6732

General

Start time:	21:41:11
Start date:	25/02/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6732 CREDAT:17410 /prefetch:2
Imagebase:	0x2f0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Disassembly