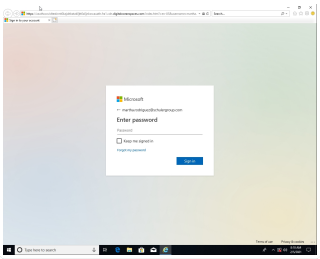
ID: 349041
Cookbook: browseurl.jbs
Time: 08:09:16
Date: 05/02/2021
Version: 31.0.0 Emerald

Table of Contents

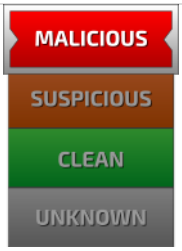
Analysis Report https://zauthxcovidtestinnt0kajxktkatak…

Overview

General Information

Sample URL:	https://zauthxcovidtestinnt0kajxktkatak0jtt0a0jnkowauath.fra1.cdn.digitaloc...oceanspaces.com/index.htm?=en-US&username=martha.rodriguez@schulergroup.com
Analysis ID:	349041
Most interesting Screenshot:	

Detection



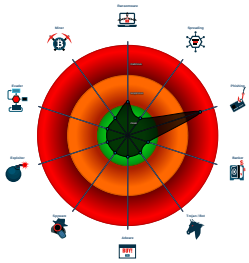
HTMLPhisher

Score:	68
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Phishing site detected (based on fav…
- Yara detected HtmlPhish_10
- Phishing site detected (based on log…
- Found iframes
- HTML body contains low number of …
- HTML title does not match URL
- Submit button contains javascript call
- URL contains potential PII (phishing…

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 5204 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 1740 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5204 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

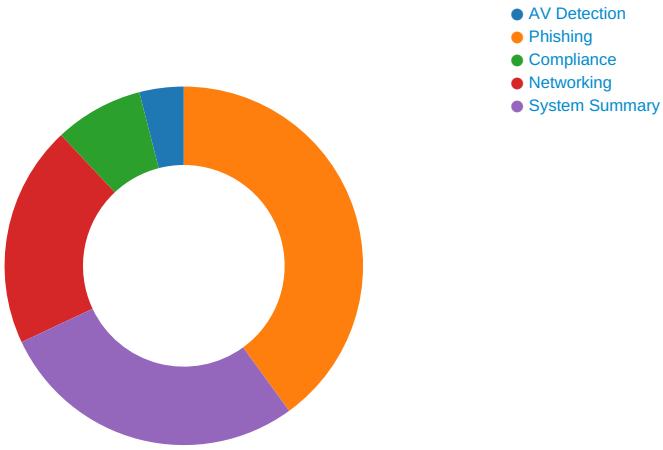
Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\index[1].htm	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Phishing:

Phishing site detected (based on favicon image match)

Yara detected HtmlPhish_10

Phishing site detected (based on logo template match)

Compliance:

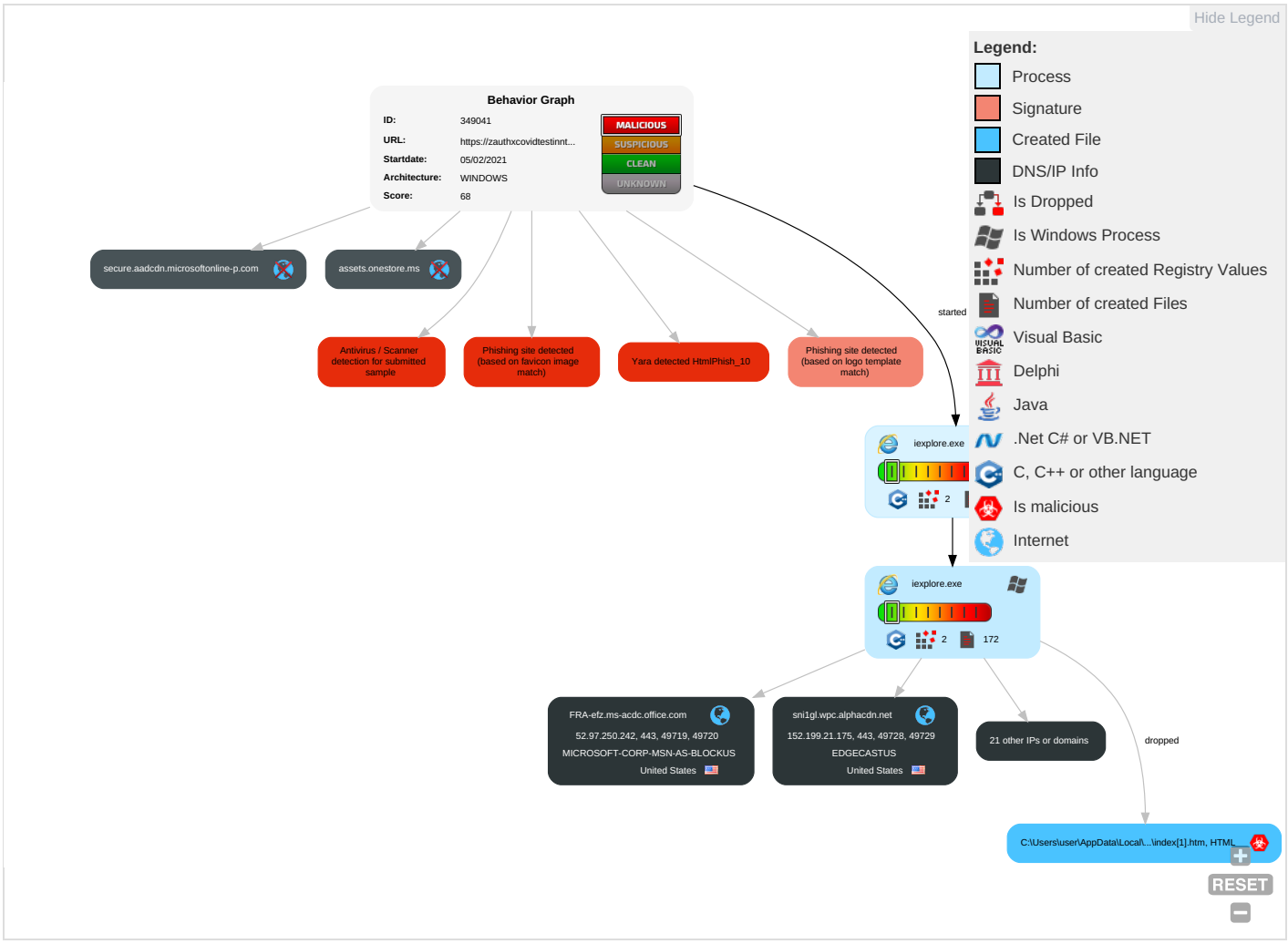
Uses new MSVCR Dlls

Uses secure TLS version for HTTPS connections

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	Im
Drive-by Compromise 1	Scripting 1	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Mo Sy Pa
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Application Window Discovery	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	De Lo
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Scripting 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	De De Da

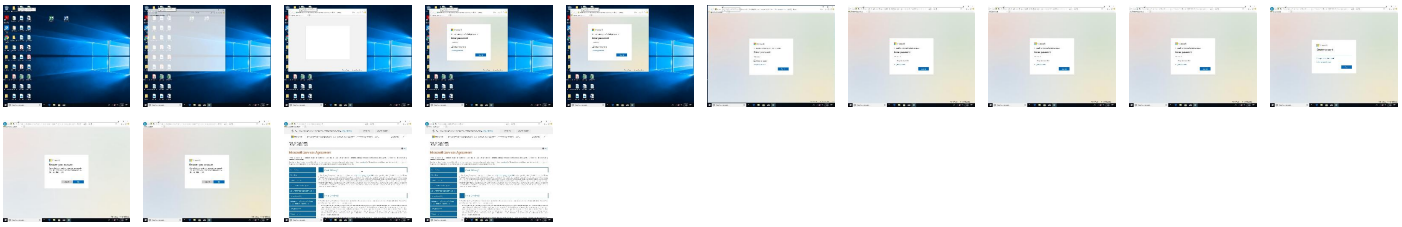
Behavior Graph

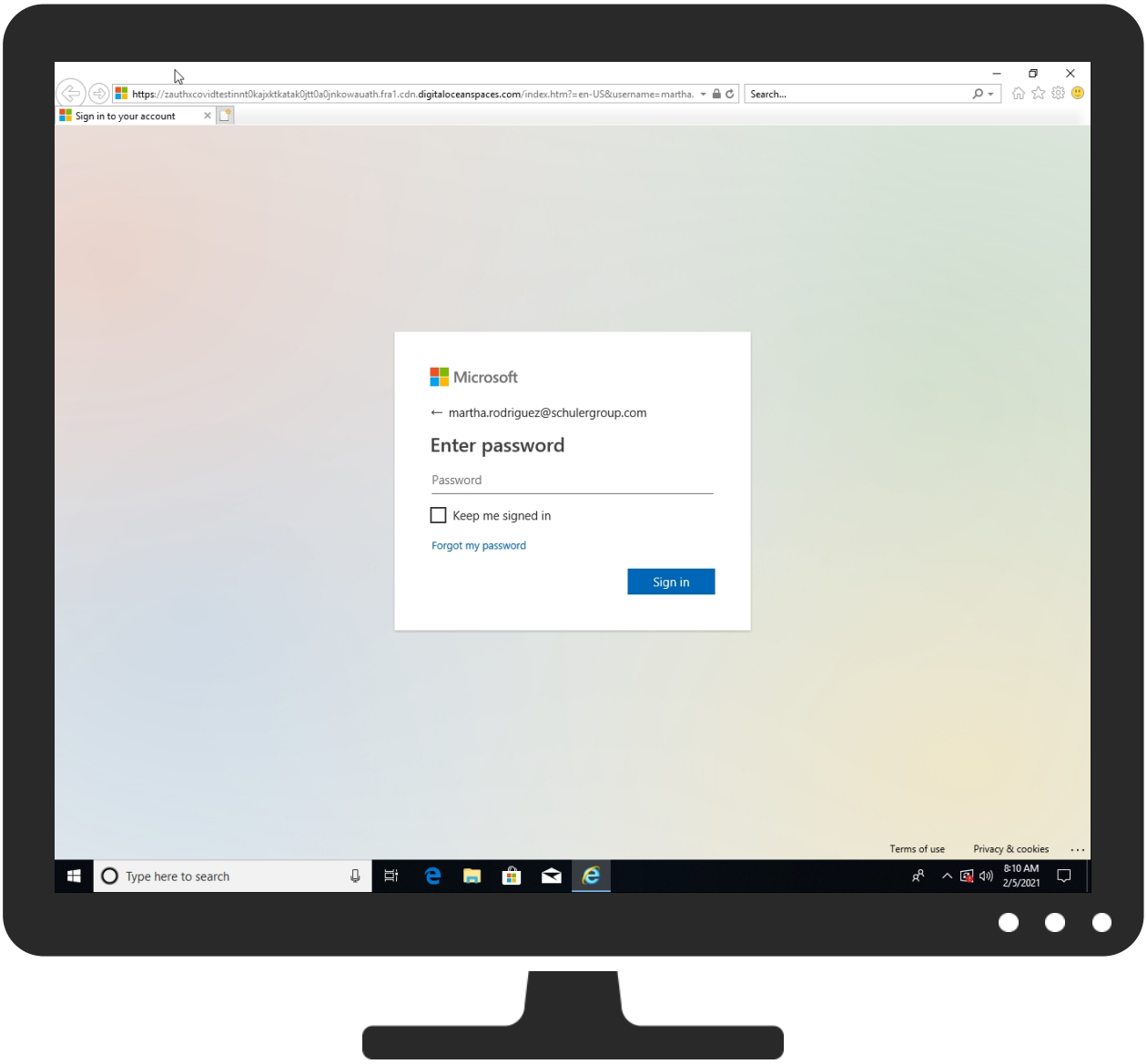


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://zauthxcovidtestinnt0kajxktkatak0jtt0a0jnkowauath.fra1.cdn.digitaloceanspaces.com/index.htm?=en-US&username=martha.rodriguez@schulergroup.com	0%	Avira URL Cloud	safe	
http://https://zauthxcovidtestinnt0kajxktkatak0jtt0a0jnkowauath.fra1.cdn.digitaloceanspaces.com/index.htm?=en-US&username=martha.rodriguez@schulergroup.com	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://https://zauthxcovidtestinnt0kajxktkatak0jtt0a0jnkowauath.fra1.cdn.digitaloceanspaces.com/index.htm?=en-US&username=martha.rodriguez@schulergroup.com	100%	UrlScan	phishing brand: microsoft	Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
cs1100.wpc.omegacdn.net	0%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
sni1gl.wpc.alphacdn.net	0%	Virustotal		Browse
aadcdn.msftauth.net	0%	Virustotal		Browse
prod.msocdn.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://ncuillery.github.io/angular-breadcrumb	0%	Avira URL Cloud	safe	
http://https://prod.msocdn.com/2021.1.28.2/en-US/WebControls/JS/ProductKeyControl.js	0%	Avira URL Cloud	safe	
http://https://prod.msocdn.com/2021.1.28.2/en-US/JS/NetPerf.js	0%	Avira URL Cloud	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/images/backgrounds/2_bc3d32a696895f78c19df6c717586a5d.s	0%	Avira URL Cloud	safe	
http://https://www.youradchoices.ca/fr	0%	URL Reputation	safe	
http://https://www.youradchoices.ca/fr	0%	URL Reputation	safe	
http://https://www.youradchoices.ca/fr	0%	URL Reputation	safe	
http://https://prod.msocdn.com/images/scrollbar/arrow_staticdown_16.png	0%	Avira URL Cloud	safe	
http://https://prod.msocdn.com/en-US/css/webfonts/SegoeUI-Regular-final.ttf	0%	Avira URL Cloud	safe	
http://https://prod.msocdn.com/2021.1.28.2/en-US/css/EmbeddedFonts.css	0%	Avira URL Cloud	safe	
http://https://prod.msocdn.com/2021.1.28.2/en-US/JS/PasswordStrengthMeter.js	0%	Avira URL Cloud	safe	
http://https://prod.msocdn.com/2021.1.28.2/en-US/JS/SearchBox.js	0%	Avira URL Cloud	safe	
http://https://prod.msocdn.com/2021.1.28.2/en-US/js/reporting.js	0%	Avira URL Cloud	safe	
http://https://prod.msocdn.com/Shell/Images/header_wizard_hl_mos.jpg	0%	Avira URL Cloud	safe	
http://https://acctcdn.msauth.net/wlivepackagefull_gkQfr3DPKXxDWQ1F0WVujA2.js?v=1	0%	Avira URL Cloud	safe	
http://https://prod.msocdn.com/2021.1.28.2/en-US/JSC/ControlBundle.js	0%	Avira URL Cloud	safe	
http://https://prod.msocdn.com/en-US/css/webfonts/SegoeUI-Light-final.eot	0%	Avira URL Cloud	safe	
http://getbootstrap.com)	0%	Avira URL Cloud	safe	
http://https://mindblog.com.ng/zltmworld/yhost.php	0%	Avira URL Cloud	safe	
http://https://blobs.officehome.msocdn.com/bundles/app-bundle-916fcbf3c234b31aac35.js	0%	Avira URL Cloud	safe	
http://https://prod.msocdn.com/en-US/css/webfonts/SegoeUI-SemiLight-final.eot?iefix	0%	Avira URL Cloud	safe	
http://https://prod.msocdn.com/en-US/css/webfonts/SegoeUI-SemiLight-final.woff	0%	Avira URL Cloud	safe	
http://https://prod.msocdn.com/2021.1.28.2/en-US/JS/mscorlib.js	0%	Avira URL Cloud	safe	
http://https://prod.msocdn.com/en-US/css/webfonts/SegoeUI-Regular-final.woff	0%	Avira URL Cloud	safe	
http://https://prod.msocdn.com/Images/transparent.gif	0%	Avira URL Cloud	safe	
http://https://prod.msocdn.com/Shell/Images/pagelayout_nav_highlight.jpg	0%	Avira URL Cloud	safe	
http://https://acctcdn.msauth.net/images/microsoft_logo_7lyNn7YkjJOP0NwZNw6QvQ2.svg	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/images/microsoft_logo_7lyNn7YkjJOP0NwZNw6QvQ2.svg	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/images/microsoft_logo_7lyNn7YkjJOP0NwZNw6QvQ2.svg	0%	URL Reputation	safe	
http://https://prod.msocdn.com/en-US/css/webfonts/SegoeUI-SemiBold-final.ttf	0%	Avira URL Cloud	safe	
http://www.mpegla.com).	0%	Avira URL Cloud	safe	
http://https://acctcdn.msauth.net/jquerypackage_1.10_5V7LAuc3bNAQx2QQfr1RPw2.js?v=1	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/jquerypackage_1.10_5V7LAuc3bNAQx2QQfr1RPw2.js?v=1	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/jquerypackage_1.10_5V7LAuc3bNAQx2QQfr1RPw2.js?v=1	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/bootstrap_3.3.0_B68S-_daR6nLiLVZsh4XiA2.js?v=1	0%	Avira URL Cloud	safe	
http://https://secure.aadcdn.microsoftonline-p.com/ests/2.1.8576.13/content/cdnbundles/converged.v2.login.m	0%	Avira URL Cloud	safe	
http://https://prod.msocdn.com/2021.1.28.2/en-US/css/AssistancePanel.css	0%	Avira URL Cloud	safe	
http://https://prod.msocdn.com/2021.1.28.2/en-US/css/conciergehelper.css	0%	Avira URL Cloud	safe	
http://https://prod.msocdn.com/2021.1.28.2/en-US/js/AssistancePanel.js	0%	Avira URL Cloud	safe	
http://https://prod.msocdn.com/en-US/css/webfonts/SegoeUI-Light-final.eot?iefix	0%	Avira URL Cloud	safe	
http://https://prod.msocdn.com/Images/list_bullet_5x5.gif	0%	Avira URL Cloud	safe	
http://https://acctcdn.msauth.net/converged_ux_v2_RfnRCrmapm3W_OFn994CMA2.css?v=1	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/converged_ux_v2_RfnRCrmapm3W_OFn994CMA2.css?v=1	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/converged_ux_v2_RfnRCrmapm3W_OFn994CMA2.css?v=1	0%	URL Reputation	safe	
http://https://prod.msocdn.com/en-US/css/webfonts/FabMDL2.4.05.woff	0%	Avira URL Cloud	safe	
http://fontello.comiconsRegulariconsiconsVersion	0%	URL Reputation	safe	
http://fontello.comiconsRegulariconsiconsVersion	0%	URL Reputation	safe	
http://fontello.comiconsRegulariconsiconsVersion	0%	URL Reputation	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://aadcdn.msftauth.net/ests/2.1/content/images/ellipsis_grey_5bc252567ef56db648207d9c36a9d004.p	0%	Avira URL Cloud	safe	
http://https://prod.msocdn.com/en-US/css/webfonts/SegoeUI-SemiLight-final.eot	0%	Avira URL Cloud	safe	
http://https://prod.msocdn.com/Shell/Images/O365SharedClusteredImage.png	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://account.live.c	0%	Avira URL Cloud	safe	
http://https://blobs.officehome.msocdn.com/bundles/staticscripts-d40cc02c2c.js	0%	Avira URL Cloud	safe	
http://https://acctcdn.msauth.net	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net	0%	URL Reputation	safe	
http://https://prod.msocdn.com/2021.1.28.2/en-US/css/home.css	0%	Avira URL Cloud	safe	
http://https://prod.msocdn.com/2021.1.28.2/en-US/JSC/HeadBundle.js	0%	Avira URL Cloud	safe	
http://https://prod.msocdn.com/images/servicestatus.png	0%	Avira URL Cloud	safe	
http://https://prod.msocdn.com/shell/images/o365_gallatin_logo.png	0%	Avira URL Cloud	safe	
http://https://prod.msocdn.com/en-US/css/webfonts/SegoeUI-Regular-final.eot?iefix	0%	Avira URL Cloud	safe	
http://https://prod.msocdn.com/2021.1.28.2/en-US/css/commonhealthdashboard.css	0%	Avira URL Cloud	safe	
http://https://prod.msocdn.com/domains/images/Domain_Purchase_16x16.png	0%	Avira URL Cloud	safe	
http://https://acctcdn.msauth.net/images/Microsoft_Logotype_White_4MYDQRab31HKDWWN-1HafA2.svg	0%	Avira URL Cloud	safe	
http://https://rn00dfrr0f0rfdrnddrdr00n.azurewebsites.net/handler.php	0%	Avira URL Cloud	safe	
http://https://prod.msocdn.com/Shell/Images/pagelayout_mos_background_right.jpg	0%	Avira URL Cloud	safe	
http://https://www.youradchoices.ca	0%	URL Reputation	safe	
http://https://www.youradchoices.ca	0%	URL Reputation	safe	
http://https://www.youradchoices.ca	0%	URL Reputation	safe	
http://https://chieffancypants.github.io/angular-hotkeys	0%	Avira URL Cloud	safe	
http://https://blobs.officehome.msocdn.com/bundles/app-bundle-98c3925f7b2d1a4dbc40.css	0%	Avira URL Cloud	safe	
http://https://secure.aadcdn.microsoftonline-p.com/ests/2.1.8576.13/content/cdnbundles/convergedloginpagina	0%	Avira URL Cloud	safe	
http://https://secure.aadcdn.microsoftonline-p.com/ests/2.1.8576.13/content/cdnbundles/oldconvergedlogin_pc	0%	Avira URL Cloud	safe	
http://https://prod.msocdn.com/2021.1.28.2/en-US/js/DomainManager.js	0%	Avira URL Cloud	safe	
http://https://prod.msocdn.com/images/scrollbar/arrow_staticup_16.png	0%	Avira URL Cloud	safe	
http://https://acctcdn.msauth.net/images/	0%	Avira URL Cloud	safe	
http://https://prod.msocdn.com/en-US/css/webfonts/SegoeUI-SemiBold-final.eot?iefix	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cs1100.wpc.omegacdn.net	152.199.23.37	true	false	• 0%, Virustotal, Browse	unknown
sni1gl.wpc.alphacdn.net	152.199.21.175	true	false	• 0%, Virustotal, Browse	unknown
FRA-efz.ms-acdc.office.com	52.97.250.242	true	false		high
www.office.com	unknown	unknown	false		high
signup.live.com	unknown	unknown	false		high
r4.res.office365.com	unknown	unknown	false		high
aadcdn.msftauth.net	unknown	unknown	false	• 0%, Virustotal, Browse	unknown
prod.msocdn.com	unknown	unknown	false	• 0%, Virustotal, Browse	unknown
assets.onestore.ms	unknown	unknown	false		unknown
account.live.com	unknown	unknown	false		high
ajax.aspnetcdn.com	unknown	unknown	false		high
acctcdn.msauth.net	unknown	unknown	false		unknown
outlook.office365.com	unknown	unknown	false		high
secure.aadcdn.microsoftonline-p.com	unknown	unknown	false		unknown
portal.microsoftonline.com	unknown	unknown	false		high
zauthxcovidtestinnt0kajxktkatak0jtt0a0jnkowauath.fra1.cdn.digitaloceanspaces.com	unknown	unknown	false		high
clientlog.portal.office.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://zauthxcovidtestinnt0kajxktkatak0jtt0a0jnkowauath.fra1.cdn.digitaloceanspaces.com/index.htm?=en-US&username=martha.rodriguez@schulergroup.com	false		high

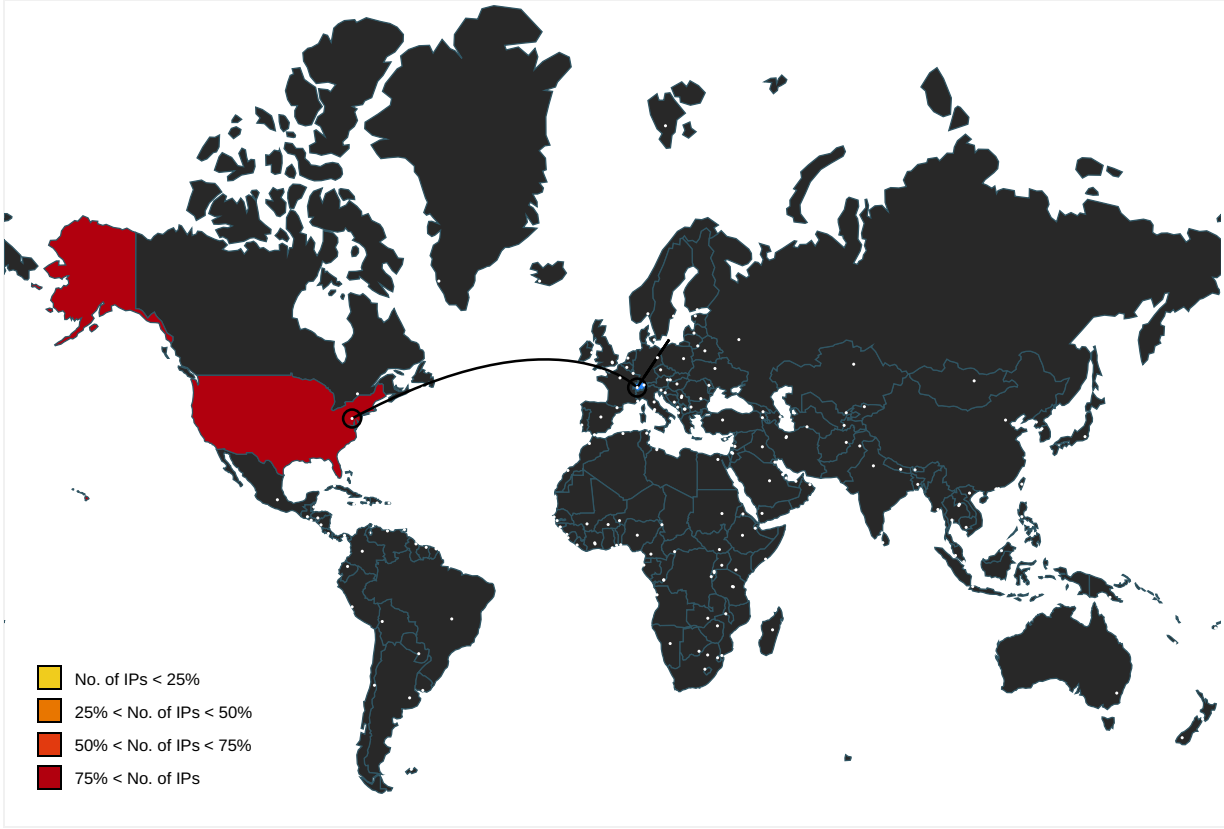
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://ncuillery.github.io/angular-breadcrumb	AngularExtensions[1].js.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://prod.msocdn.com/2021.1.28.2/en-US/WebControls/JS/ProductKeyControl.js	Prefetch[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://prod.msocdn.com/2021.1.28.2/en-US/JS/NetPerf.js	Prefetch[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://aadcdn.msftauth.net/ests/2.1/content/images/backgrounds/2_bc3d32a696895f78c19df6c717586a5d.s	index[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.youradchoices.ca/fr	privacystatement[1].htm.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://purl.eligrey.com/github/Blob.js/blob/master/Blob.js	AngularExtensions[1].js.2.dr	false		high
http://www.asp.net/ajaxlibrary/CDN.ashx.	privacystatement[1].htm.2.dr	false		high
http://https://prod.msocdn.com/images/scrollbar/arrow_staticdown_16.png	Prefetch[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://prod.msocdn.com/en-US/css/webfonts/SegoeUI-Regular-final.ttf	EmbeddedFonts[1].css.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://prod.msocdn.com/2021.1.28.2/en-US/css/EmbeddedFonts.css	Prefetch[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.xbox.com/en-US/Legal/CodeOfConduct	servicesagreement[1].htm.2.dr	false		high
http://https://prod.msocdn.com/2021.1.28.2/en-US/JS/PasswordStrengthMeter.js	Prefetch[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://prod.msocdn.com/2021.1.28.2/en-US/JS/SearchBox.js	Prefetch[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://aka.ms/taxservice	servicesagreement[1].htm.2.dr	false		high
http://https://prod.msocdn.com/2021.1.28.2/en-US/js/reporting.js	Prefetch[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://prod.msocdn.com/Shell/Images/header_wizard_hl_mos.jpg	Prefetch[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://acctcdn.msauth.net/wlivepackagefull_gkQfr3DPKXxDWQ1F0WVujA2.js?v=1	ResetPassword[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://prod.msocdn.com/2021.1.28.2/en-US/JSC/ControlBundle.js	Prefetch[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://prod.msocdn.com/en-US/css/webfonts/SegoeUI-Light-final.eot	EmbeddedFonts[1].css.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://github.com/asafdav/ng-csv/commit/ae479f7099573a05807f55f51fbd1d799c5ed00a	AngularExtensions[1].js.2.dr	false		high
http://https://skype.com/go/myaccount	servicesagreement[1].htm.2.dr	false		high
http://https://www.skype.com	servicesagreement[1].htm.2.dr	false		high
http://getbootstrap.com)	admin[1].css.2.dr	false	• Avira URL Cloud: safe	low
http://https://mindblog.com.ng/zltmworld/yhost.php	index[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://r4.res.office365.com/owa/prem/16.3809.0.3214099/resources/styles/0/boot.worldwide.mouse.css	prefetch[2].htm.2.dr	false		high
http://https://blobs.officehome.msocdn.com/bundles/app-bundle-916fcbf3c234b31aac35.js	prefetch[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://r4.res.office365.com/owa/prem/16.3809.0.3214099/scripts/boot.worldwide.2.mouse.js	prefetch[2].htm.2.dr	false		high
http://https://prod.msocdn.com/en-US/css/webfonts/SegoeUI-SemiLight-final.eot?iefix	EmbeddedFonts[1].css.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://prod.msocdn.com/en-US/css/webfonts/SegoeUI-SemiLight-final.woff	EmbeddedFonts[1].css.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://prod.msocdn.com/2021.1.28.2/en-US/JS/mscorlib.js	Prefetch[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://prod.msocdn.com/en-US/css/webfonts/SegoeUI-Regular-final.woff	EmbeddedFonts[1].css.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://prod.msocdn.com/Images/transparent.gif	Prefetch[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://github.com/jquery/globalize	boot.worldwide.0.mouse[1].js.2.dr	false		high
http://https://prod.msocdn.com/Shell/Images/pagelayout_nav_highlight.jpg	Prefetch[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.xbox.com/managedatacollection	privacystatement[1].htm.2.dr	false		high
http://https://signup.live.cotinnt0kajxktkatak0jtt0a0jnkowauath.fra1.cdn.digitaloceanspaces.com/index.htm?=	{9B7B6C5E-67CC-11EB-90E4-ECF4BB862DED}.dat.1.dr	false		high
http://https://www.xbox.com/legal/codeofconduct	privacystatement[1].htm.2.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://acctcdn.msauth.net/images/microsoft_logo_7lyNn7YkjJOP0NwZNw6QvQ2.svg	ResetPassword[1].htm.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://prod.msocdn.com/en-US/css/webfonts/SegoeUI-SemiBold-final.ttf	EmbeddedFonts[1].css.2.dr	false	• Avira URL Cloud: safe	unknown
http://purl.eligrey.com/github/FileSaver.js/blob/master/FileSaver.js	AngularExtensions[1].js.2.dr	false		high
http://www.mpegla.com).	servicesagreement[1].htm.2.dr	false	• Avira URL Cloud: safe	low
http://https://aka.ms/kinectprivacy/	privacystatement[1].htm.2.dr	false		high
http://https://acctcdn.msauth.net/jquerypackage_1.10_5V7LAuc3bNAQx2QQfr1RPw2.js?v=1	ResetPassword[1].htm.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://acctcdn.msauth.net/bootstrap_3.3.0_B68S-_daR6nLiLVZsh4XiA2.js?v=1	ResetPassword[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protectio	privacystatement[1].htm.2.dr	false		high
http://https://secure.aadcdn.microsoftonline-p.com/ests/2.1.8576.13/content/cdnbundles/converged.v2.login.m	index[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://github.com/douglascrockford/JSON-js	ResetPassword[1].htm.2.dr	false		high
http://https://prod.msocdn.com/2021.1.28.2/en-US/css/AssistancePanel.css	Prefetch[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://prod.msocdn.com/2021.1.28.2/en-US/css/conciergehelper.css	Prefetch[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://prod.msocdn.com/2021.1.28.2/en-US/js/AssistancePanel.js	Prefetch[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://prod.msocdn.com/en-US/css/webfonts/SegoeUI-Light-final.eot?iefix	EmbeddedFonts[1].css.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://portal.microsoftonline.com/Prefetch/Prefetch.aspx	index[1].htm.2.dr, {9B7B6C5E-67CC-11EB-90E4-ECF4BB862DED}.dat.1.dr	false		high
http://https://prod.msocdn.com/Images/list_bullet_5x5.gif	Prefetch[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://acctcdn.msauth.net/converged_ux_v2_RfnRCrmapm3W_OFn994CMA2.css?v=1	ResetPassword[1].htm.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.opensource.org/licenses/mit-license.php)	knockout_3.3.0_X1BYS2jZMbi7hfUj8VuqFA2[1].js.2.dr	false		high
http://https://prod.msocdn.com/en-US/css/webfonts/FabMDL2.4.05.woff	admin[1].css.2.dr	false	• Avira URL Cloud: safe	unknown
http://fontello.comiconsRegulariconsiconsVersion	icons[1].eot.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.skype.com/go/legal	servicesagreement[1].htm.2.dr	false		high
http://https://mixer.com/about/tos	servicesagreement[1].htm.2.dr	false		high
http://https://www.microsoft.	{9B7B6C5E-67CC-11EB-90E4-ECF4BB862DED}.dat.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://github.com/twbs/bootstrap/blob/master/LICENSE)	admin[1].css.2.dr	false		high
http://https://aadcdn.msftauth.net/ests/2.1/content/images/ellipsis_grey_5bc252567ef56db648207d9c36a9d004.p	index[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://prod.msocdn.com/en-US/css/webfonts/SegoeUI-SemiLight-final.eot	EmbeddedFonts[1].css.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://support.xbox.com/help/friends-social-activity/community/use-safety-settings	privacystatement[1].htm.2.dr	false		high
http://https://www.xbox.com/Legal/ThirdPartyDataSharing	privacystatement[1].htm.2.dr	false		high
http://https://prod.msocdn.com/Shell/Images/O365SharedClusteredImage.png	Prefetch[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://signin.kissmetrics.com/privacy/#controls	privacystatement[1].htm.2.dr	false		high
http://https://account.live.c	{9B7B6C5E-67CC-11EB-90E4-ECF4BB862DED}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://login.skype.com/login	privacystatement[1].htm.2.dr	false		high
http://https://blobs.officehome.msocdn.com/bundles/staticscripts-d40cc02c2c.js	prefetch[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://acctcdn.msauth.net	ResetPassword[1].htm.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://github.com/angular/angular.js/pull/10764	AngularExtensions[1].js.2.dr	false		high
http://https://www.optimizely.com/legal/opt-out/	privacystatement[1].htm.2.dr	false		high
http://https://prod.msocdn.com/2021.1.28.2/en-US/css/home.css	Prefetch[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://prod.msocdn.com/2021.1.28.2/en-US/JSC/HeadBundle.js	Prefetch[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://prod.msocdn.com/images/servicestatus.png	Prefetch[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://prod.msocdn.com/shell/images/o365_gallatin_logo.png	Prefetch[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://api.jquery.com/offset/	AngularExtensions[1].js.2.dr	false		high
http://https://prod.msocdn.com/en-US/css/webfonts/SegoeUI-Regular-final.eot?iefix	EmbeddedFonts[1].css.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://prod.msocdn.com/2021.1.28.2/en-US/css/commonhealthdashboard.css	Prefetch[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://prod.msocdn.com/domains/images/Domain_Purchase_16x16.png	Prefetch[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.appsflyer.com/optout	privacystatement[1].htm.2.dr	false		high
http://https://acctcdn.msauth.net/images/Microsoft_Logotype_White_4MYDQRab31HKDWWN-1HafA2.svg	ResetPassword[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://aka.ms/redeemrewards).	servicesagreement[1].htm.2.dr	false		high
http://https://zauthxcovidtestinnt0kajxktkatak0jtt0a0jnkowauath.fra1.cdn.digitaloceanspaces.com/index.htm?=	{9B7B6C5E-67CC-11EB-90E4-ECF4BB862DED}.dat.1.dr, ~DF64D1AB08A7862898.TMP.1.dr	false		high
http://https://rn00dfrr0f0rfdrnddrdr00n.azurewebsites.net/handler.php	index[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://prod.msocdn.com/Shell/Images/pagelayout_mos_background_right.jpg	Prefetch[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.youradchoices.ca	privacystatement[1].htm.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://chieffancypants.github.io/angular-hotkeys	AngularExtensions[1].js.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://blobs.officehome.msocdn.com/bundles/app-bundle-98c3925f7b2d1a4dbc40.css	prefetch[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://secure.aadcdn.microsoftonline-p.com/ests/2.1.8576.13/content/cdnbundles/convergedloginpagina	index[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://secure.aadcdn.microsoftonline-p.com/ests/2.1.8576.13/content/cdnbundles/oldconvergedlogin_pc	index[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://prod.msocdn.com/2021.1.28.2/en-US/js/DomainManager.js	Prefetch[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.here.com/)	privacystatement[1].htm.2.dr	false		high
http://https://prod.msocdn.com/images/scrollbar/arrow_staticup_16.png	Prefetch[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.skype.com/go/store.reactivate.credit	servicesagreement[1].htm.2.dr	false		high
http://https://acctcdn.msauth.net/images/	ResetPassword[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://developer.yahoo.com/flurry/end-user-opt-out/	privacystatement[1].htm.2.dr	false		high
http://https://prod.msocdn.com/en-US/css/webfonts/SegoeUI-SemiBold-final.eot?iefix	EmbeddedFonts[1].css.2.dr	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
52.97.250.242	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
152.199.21.175	unknown	United States		15133	EDGECASTUS	false
152.199.23.37	unknown	United States		15133	EDGECASTUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	349041
Start date:	05.02.2021
Start time:	08:09:16
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 22s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://zauthxcovidtestinnt0kajxktkatak0jtt0a0jnkowauath.fra1.cdn.digitaloceanspaces.com/index.htm?=en-US&username=martha.rodriguez@schulergroup.com
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	12
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 • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL

Copyright null 2021

Classification:	mal68.phis.win@3/140@16/3
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browsing link: https://login.live.com/oauth20_authorize.srf?response_type=code&client_id=51483342-085c-4d86-bf88-cf50c7252078&scope=openid+profile+email+offline_access&response_mode=form_post&redirect_uri=https%3a%2f%2flogin.microsoftonline.com%2fcommon%2ffederation%2foauth2&state=rQIIAeNisNLJKCkpKLbS1y_ILypJzNHLzUwuyi_OTyvJz8vJzEvVS87P1csvSs9MAbGKhLgE5N-HsRnaz3GZ3Nb0o0aAj2MWI2d8TmYZWOUqRmXCxulfYGR8wch4i0nQvyjdMyW82C01JbUosSQzP-8Ci8ArFh4DZisODi4BBgkGBYYfLIyLWIG2Rik0X16_dbXTrqAUuYQeZ4ZTrPpRVd4W-b7mmV4ppv5hlW6-lqaluRYWHrl5XtppBkXhQUUhmQElZWVGAaGBtqZWhhPYhCawMZ1iY_jAxtjBznCAk_EWl4iRgaGlroGRroGJgoGllZGRlbFRFAA1&estsfed=1&uaid=0656ef1f3f31449c938682f87c100e08&signup=1&lw=1&fl=easi2&fci=https%3a%2f%2fportal.microsoftonline.com.orgid.com • Browsing link: https://account.live.com/ResetPassword.aspx?wreply=https://login.live.com/oauth20_authorize.srf%3frespons e_type%3dcode%26client_id%3d51483342-085c-4d86-bf88-cf50c7252078%26scope%3dopenid%2bprofile%2bemail%2boffline_access%26response_mode%3dform_post%26redirect_uri%3dhttps%253a%252f%252flogin.microsoftonline.com%252fcommon%252ffederation%252foauth2%26state%3drQIIAeNisNLJKCkpKLbS1y_ILypJzNHLzUwuyi_OTyvJz8vJzEvVS87P1csvSs9MAbGKhLgEOhzkFBYXR3m11Zle3FvBmjCLkTM-J7MMrHIVozJh4_QvMDK-YGS8xSToX5TumRJe7JaaklqUWJKZn3eBReAVC48BsxUHB5cAgwSDAsMPFsZFrEBb40pDQg3r0t0nbto2zWOTN8MpVv2oKm-LfF_zTK8UU_-wSjdfS9PSXAsLj9w8L-00g6LwoKKQzICSsjKjgNBAWwsrwwlsQhPYmE6xMXxgY-xgZzjAyXiLS8TlwNBS18BI18BEwcDCysTCytgkCgA1%26estsfed%3d1%26uaid%3d201e408873a34a5a867e35d1bd780560%26fci%3dhttps%253a%252f%252fportal.microsoftonline.com.orgid.com%26username%3d%26contextid%3d34A42CC81359F79A%26bk%3d1549270157&id=293577&uiflavor=web&client_id=1E00004417ACAE&mkt=EN-US&lc=1033&bk=1549270157 • Browsing link: https://www.microsoft.com/en-US/servicesagreement/ • Browsing link: https://privacy.microsoft.com/en-US/privacystatement

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, ielowutil.exe, SgrmBroker.exe, svchost.exe • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • Excluded IPs from analysis (whitelisted): 40.88.32.150, 104.43.139.144, 88.221.62.148, 205.185.216.42, 205.185.216.10, 92.123.151.195, 152.199.19.160, 52.109.88.54, 95.101.47.88, 13.107.6.156, 92.122.146.12, 40.126.9.66, 20.190.137.14, 20.190.137.73, 40.126.9.73, 40.126.9.6, 20.190.137.75, 40.126.9.8, 20.190.137.98, 13.107.42.22, 52.114.32.25, 92.122.145.53, 92.122.144.200, 92.122.213.194, 92.122.213.240, 13.107.246.13, 92.122.213.247, 152.199.19.161, 84.53.167.109 • Excluded domains from analysis (whitelisted): assets.onestore.ms.edgekey.net, www.tm.lg.prod.aadmsa.akadns.net, e13678.dscb.akamaiedge.net, browser.events.data.trafficmanager.net, i.s-microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, www.tm.a.prd.aadg.trafficmanager.net, a1945.g2.akamai.net, e11290.dspg.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, www.microsoft.com-c-3.edgekey.net, ams2.next.a.prd.aadg.trafficmanager.net, login.live.com, star-azurefd-prod.trafficmanager.net, statics-marketingsites-eus-ms-com.akamaized.net, watson.telemetry.microsoft.com, acctcdnvzeuno.azureedge.net, acctcdnvzeuno.ec.azureedge.net, e10583.dspg.akamaiedge.net, fs.microsoft.com, secure.aadcdn.microsoftonline-p.com.edgekey.net, aadcdnoriginneu.azureedge.net, skypedataprdcolcus16.cloudapp.net, cds.b5g9b8e4.hwcdn.net, assets.onestore.ms.akadns.net, c-s.cms.ms.akadns.net, t-0003.t-msedge.net, wildcard.msocdn.com.edgekey.net, e14579.dspg.akamaiedge.net, blobcollector.events.data.trafficmanager.net, account.msa.akadns6.net, c.s-microsoft.com-c.edgekey.net, privacy.microsoft.com.edgekey.net, cs9.wpc.v0cdn.net, home-office365-com.b-0004.b-msedge.net, i.s-microsoft.com, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, acctcdn.trafficmanager.net, www.microsoft.com-c-3.edgekey.net.globalredir.akadns.net, iecvlist.microsoft.com, go.microsoft.com, mscomajax.vo.msecnd.net, e13761.dscg.akamaiedge.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, geo.portal.microsoftonline.akadns.net, skypedataprdcoljpe05.cloudapp.net, cs22.wpc.v0cdn.net, e1875.dscg.akamaiedge.net, ie9comview.vo.msecnd.net, b-0004.b-msedge.net, e1723.g.akamaiedge.net, Edge-Prod-FRAr3.ctrl.t-0003.t-msedge.net, login.msa.msidentity.com, aadcdnoriginneu.ec.azureedge.net, browser.events.data.microsoft.com, c.s-microsoft.com, privacy.microsoft.com, go.microsoft.com.edgekey.net, l-0013.l-msedge.net, eur.portal.microsoftonline.akadns.net, e13678.dscg.akamaiedge.net, www.microsoft.com, e13678.dspb.akamaiedge.net, r4.res.office365.com.edgekey.net, wcpstatic.microsoft.com • Report size getting too big, too many NtCreateFile calls found. • Report size getting too big, too many NtDeviceIoControlFile calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{9B7B6C5C-67CC-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8548204209289596
Encrypted:	false
SSDEEP:	192:rGZRZLM2LK9WLatLQEfLQpZRMLWpeLcpeLcV6fLcV+cX:rC3L7LKULyLhLJLVL7L1LQ
MD5:	3698B506662427D7F2A985A037FBCE13
SHA1:	4B5CB47413CD0735E8D800B795FDD044A6BD78CD
SHA-256:	B3C5D20CA8F3F8724FDD122D1A101EE6D3D75D0ACA44F986363D3F24830CCD2F
SHA-512:	868EE8AA9C36429619106C289E7FF32E36BD63CA58CBB012E2CF9EE00EC9C908FE904985AA7CF6619834BEA0EE2D06AFE50DEEB6227B916CF20E972B7FDA155D
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\{9B7B6C5E-67CC-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	125188
Entropy (8bit):	3.304454365151571
Encrypted:	false
SSDEEP:	768:0aAE4XGHjAE4XGHgvvmUwH2HDvvmUVuvvmUwHYvvmUwH2vvmUwHEvvmUwH83+xv7:0axJxW+WTXG+g+++s+cu/7+syW
MD5:	DF7E15DD2F1042F19E627404806F80D5
SHA1:	E5B73AB1B2391F67BACC0B54BBE0FB87CB98622A
SHA-256:	52CD019BB3175E820D40107D1D2E2485D8CF8D36041E27F49557B7501D41E9E6
SHA-512:	47CFF1B1EBE43011CC5C6C9F16E2AF3303425C3508855D42E7DA2B2C7263484BFA2BA5267A844B1FE8A30AD463E1B2AF1BDF0104386F4CA4843514F476362A2
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{9B7B6C5E-67CC-11EB-90E4-ECF4BB862DED}.dat	
Preview:	....R.o.o.t. .E.n.t.r. y..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{A28BE40F-67CC-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5660704298977235
Encrypted:	false
SSDEEP:	48:IwNGcprsGwpaVG4pQgGrapbSDorGQpKeG7HpRXsTGIpG:rTZEQH6+BSDoFAZTX4A
MD5:	12ACB243C14EBBEDB857A13BB725AB34
SHA1:	08828651D8068443F723636EEA39A2895D4E2FA1
SHA-256:	06A7934136B34C6776FDE42A254B944947EBF21EFECC2061A65A338D93C07179
SHA-512:	123297C96BE368938028B7E306856E101E518CA303F374D81A4F1D323430F20F6BB775E7F08CB0C69FDF63B7FF047B79B4C2627E2710C83B4F92AD396EF06EA4
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):	54720
Entropy (8bit):	3.1035881998138235
Encrypted:	false
SSDEEP:	96:MMsbMVbMVbMkbMtbM9QQQQQ4HQQQQQ4QQQQQ1:UcEJsUY
MD5:	8A70B77CF37E0901EDC366389770077B
SHA1:	987DCA7A30289C54DEDC570D02CC3D29971510C5
SHA-256:	7C8DED5B107871F301FD4044CDB4C4517E32DC523DEEFA40F7E1B11B92717364
SHA-512:	26F53DF1FFA8CD3EF30D701D9F0D1BE592FDD657DC00354797B75640FFA7657BB76F818AF5BED7D17B5D3135F150379DA4717ACED2AB9FF54093BD22FEA52B9
Malicious:	false
Reputation:	low
Preview:	q.h.t.t.p.s.:././.s.e.c.u.r.e...a.a.d.c.d.n...m.i.c.r.o.s.o.f.t.o.n.l.i.n.e.-.p...c.o.m./.e.s.t.s./.2...1...8.5.7.6...1.3./.c.o.n.t.e.n.t./.i.m.a.g.e.s./.f.a.v.i.c.o.n._.a._.e.u.p.a.y.f.g.g.h.q.i.a.i. 7.k.9.s.o.l.6.l.g.2...i.c.o.~(................h(......(....................(....................................."P..."""""""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""""""" ...3333333333333333333333333333333""

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):	133618
Entropy (8bit):	5.224557040823137
Encrypted:	false
SSDEEP:	3072:1f/HuFVppxvIeJ0i9d1EwgXA9JKi5DCE4t:1f/Hu/FIeRgt
MD5:	04ECF0CF6CBC75F16F34D42554CB4C9D
SHA1:	16DFBFEFBD6BB75FD61E7D678693C7C3998677E9
SHA-256:	06B2E0143CA1583C507056D1BC66A4024530340BA5582682180D3E2DCE56D163
SHA-512:	4CEE973A807DB3FE44D7623388087B0293869A539CC5062F0B9EDC33E4CFE98B9D969A4D987F739769C56D058BC55DDEBAB1B38E9C2A2303AE30E35870CBAB2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.microsoft.com/onerfstatics/marketingsites-eus-prod/shell/_scrf/js/themes=default/54-af9f9f/c0-247156/de-099401/e1-a50eee/e7-954872/d8-97d509/f0-251fe2/46-be1318/77-04a268/11-240c7b/63-077520/a4-34de62/bb-d7480b/db-bc0148/dc-7e9864/6d-c07ea1/29-1ec5a9/23-c64e70/cd-23d3b0/6d-1e7ed0/b7-cadaa7/c4-898cf2/ca-40b7b0/4e-ee3a55/3e-f5c39b/c3-6454d7/f9-7592d3/92-10345d/79-499886/7e-cda2d3/b2-7087f0/e5-08f1c0/e0-3c9860/91-97a04f/1f-100dea/33-abe4df/17-f90ef1?ver=2.0&iife=1

Copyright null 2021

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\17-f90ef1[1].js	
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\2_vD0yppaJX3jBnfbHF1hqXQ2[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	1864
Entropy (8bit):	5.222032823730197
Encrypted:	false
SSDEEP:	48:yvswNIBLBpJawmMH44log6gw/MHm7pJroog6gwkMH9Xog6gwdMHdqdyqog7C:ykfXYx+odPcs9B
MD5:	BC3D32A696895F78C19DF6C717586A5D
SHA1:	9191CB156A30A3ED79C44C0A16C95159E8FF689D
SHA-256:	0E88B6FCBB8591EDFD28184FA70A04B6DD3AF8A14367C628EDD7CABA32E58C68
SHA-512:	8D4F38907F3423A86D90575772B292680F7970527D2090FC005F9B096CC81D3F279D59AD76EAFCA30C3D4BBAF2276BBAA753E2A46A149424CF6F1C319DED5A6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://acctcdn.msauth.net/images/2_vD0yppaJX3jBnfbHF1hqXQ2.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="1920" height="1080" fill="none"><g opacity=".2" clip-path="url(#E)"><path d="M1466.4 1795.2c950.37 0 1720.8-627.52 1720.8-1401.6S2416.77-1008 1466.4-1008-254.4-380.482-254.4 393.6s770.428 1401.6 1720.8 1401.6z" fill="url(#A)"/><path d="M394.2 1815.6c746.58 0 1351.8-493.2 1 351.8-1101.6S1140.78-387.6 394.2-387.6-957.6 105.603-957.6 714-352.38 1815.6 394.2 1815.6z" fill="url(#B)"/><path d="M1548.6 1885.2c631.92 0 1144.2-417.45 1144. 2-932.4S2180.52 20.4 1548.6 20.4 404.4 437.85 404.4 952.8s512.276 932.4 1144.2 932.4z" fill="url(#C)"/><path d="M265.8 1215.6c690.246 0 1249.8-455.595 1249.8-10 17.6S956.046-819.6 265.8-819.6-984-364.005-984 198-424.445 1215.6 265.8 1215.6z" fill="url(#D)"/></g><defs><radialGradient id="A" cx="0" cy="0" r="1" gradientUn its="userSpaceOnUse" gradientTransform="translate(1466.4 393.6) rotate(90) scale(1401.6 1720.8)"><stop stop-color="#107c10"/><stop offset="1" stop-color="#c4c4c4" stop-opacity="0"/></radialGradient><r

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\AngularLib[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	159601
Entropy (8bit):	5.229945756171655
Encrypted:	false
SSDEEP:	1536:WgFAhcPyCrbqhRtFV1l0UBVHyfN+e/KOoF07JWwhmbkxXnFRGvTWlGWLwD3CyYzp:W0SCUbyfMe/KOwNDgxVRGvTgGWCG
MD5:	8767203359915C72F6502D16BE998D8C
SHA1:	0072A67738BDDC41EBE993A2F710B6ACDEF8FB9E
SHA-256:	E8423C91CA39502391841C89A77533F4C4B8AD3AA678A67A8ED4986ED673D989
SHA-512:	5702C4F0CEB339FB7368A9E1210A7A4935ED78056B4FAFD6418C90D93FC3A1FCF55ED79087317FC389E1E0C75DD040D8F3CA3D2D5C2EDC58583A60EFDF4186 3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://prod.msocdn.com/2021.1.28.2/en-US/JSC/AngularLib.js
Preview:	/*!. AngularJS v1.3.15. (c) 2010-2014 Google, Inc. http://angularjs.org. License: MIT.*/.(function(n,t,i){'use strict';;function v(n){return function(){for(var i=arguments[0],u,t,r=" ["+(n?n+":":"")+i+"] http://errors.angularjs.org/1.3.15/"+(n?n+"/":"")+i,i=1;i<arguments.length;i++)r=r+(1==i?"?":"&")+"p"+(i-1)+"=",u=encodeURIComponent,t=arguments[i] ,t="function"==typeof t?t.toString().replace(/ \{[\s\S]*$/,""):"undefined"==typeof t?"undefined":"string"!=typeof t?JSON.stringify(t):t,r+=u(t);return Error(r)}}function wr(n){if(n ull==n||vr(n))return!1;var t=n.length;return n.nodeType===at&&t?!0:l(n)||s(n)||0===t||"number"==typeof t&&0<t&&t-1 in n}function r(n,t,i){var u,f,e;if(n)if(o(n))for(u in n)"prototype"==u||"length"==u||"name"==u||n.hasOwnProperty&&!n.hasOwnProperty(u)||t.call(i,n[u],u,n);else if(s(n)||wr(n))for(e="object"!=typeof n,u=0,f=n.length;u<f;u++)(e||u in n)&&t.call(i,n[u],u,n);else if(n.forEach&&n.forEach!==r)n.forEach(t,i,n);else for(u in n)n.hasOwnProperty(u)&&t.call(i,n[u

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\ControlBundle[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):	94910
Entropy (8bit):	5.202004077183847
Encrypted:	false
SSDEEP:	1536:x7cx5Yu0kcI4OtiiB2ZaJUx3qVnS8auwqme2cumAaUmE4Y/rHww1erw5L+Hfx07q:+QROIiB2ZAYuwtjR1eU5L+y7imfg
MD5:	CEC9CD4A6EE299E7656F5DA8F21055D8
SHA1:	CCB46614BE6E905BF647D0542C2F4246406BEDC5
SHA-256:	59E1433729FE7B02F06538C8C389FB640AEB3F99CE45C0D2744BF748A527D27B
SHA-512:	932E43C7B0C4732630AA3C8F2C82015A6B82AABB05A189E96CE388E01DFDA879D4D8E5675DDA26054B364D6809BFF4EF12515FBC2F397C6438303ED1863C8A5
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\ControlBundle[1].js	
IE Cache URL:	http://https://prod.msocdn.com/2021.1.28.2/en-US/JSC/ControlBundle.js
Preview:	var TextBox=window.TextBox||function(){var r=function(i){var u=t(i),r=n(i),f=i.value;return r&&f.length-u.length>=r?!1:!0},u=function(t){var i=n(t);return i?!1:!0},f=function(r){var u;if(window.clipboardData&&(u=n(r),u)){var f=r.value,e=t(r),o=u-f.length+e.length,s=window.clipboardData.getData("Text").substr(0,o);return i(r,s),!1}return!0},e=function(t){var i=n(t),r=t.value;i&&r.length>i&&(t.value=r.substring(0,i))},n=function(n){var t=n.attributes.multilineMaxLength;return t?parseInt(t.value):null},t=function(n){var t,i;return n.document?(i=n.document.selection.createRange(),t=i.text):t=n.value.substring(n.selectionStart,n.selectionEnd),t},i=function(n,t){var r,i;n.document?(i=n.document.selection.createRange(),i.text=t):n.value=n.value.substring(0,n.selectionStart)+t+n.value.substring(n.selectionEnd)};return{OnKeypressHandler:r,OnBeforePasteHandler:u,OnPasteHandler:f,OnBlurHandler:e,GetMultilineMaxLength:n,GetSelectedText:t,SetSelectedText:i}};var HelpCallout=window.HelpCallout||fu

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\HeadBundle[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):	139371
Entropy (8bit):	5.324565469087667
Encrypted:	false
SSDEEP:	1536:dQ1MdLE9ANSk/X8LUYxuDoYOXMHvpLw/sirjVbGWnUXgIZ1XcgiHN:2WpoUYxukww/XU3
MD5:	01393734CE8C609DEDAFB5D859B39566
SHA1:	B25D39BCBDE4EC3CEA263644745386374B74F84A
SHA-256:	4BAF4CA64D7F5AAF54F617D12DE5E27927462B37786737D3C4ACD2846E023CFB
SHA-512:	E83E751D3DDB54B57A4E1383EA68A8F98890307B180C114E0D6A4E1714F13BEB9227A2BECF14CB240E7E72F725D90412C93ED1F8EDDA6000169E86AA1FF44E53
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://prod.msocdn.com/2021.1.28.2/en-US/JSC/HeadBundle.js
Preview:	var Namespace={Register:function(n){for(var r=!1,t="",u=n.split(".\"),i=0;i<u.length;i++)t!=""&&(t+="."),t+=u[i],r=this.Exists(t),r||this.Create(t)},Create:function(n){for(var i=n.split('.'),r=window,t=0;t<i.length;t++)("undefined"==typeof r[i[t]]||null===r[i[t]])&&(r[i[t]]={}),r=r[i[t]]},Exists:function(n){for(var i=n.split('.'),r=window,t=0;t<i.length;t++)if("undefined"!=typeof r[i[t]]&&null!==r[i[t]])r=r[i[t]];else return!1;return!0}},Shared;Namespace.Register("Microsoft.Online.BOX.JS.Shared"),Microsoft.Online.BOX.JS.Shared=new function(){function n(n){var r=window.location.hostname.toUpperCase(),u=n.origin.toUpperCase(),t,i;if(u.indexOf(r)!=-1&&n.data){t=null;try{t=JSON.parse(n.data)}catch(f){return}if(t&&t.eventId){if(t.eventId==="abtSignOutEventForHostUserGenerated")try{i="/estslogout",window.open(i,'_self')}catch(f){O365.Instrument.ClientInstrument.getInstance().logMessage(504151,"Failed to handle event abtSignOutEventForHostUserGenerated with data : ",n.data)}if(t.eventId==="abt

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\MicrosoftAjaxCombined[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	228581
Entropy (8bit):	5.223873821636117
Encrypted:	false
SSDEEP:	3072:H7b73vmxkXfmzDLk6Pp/en4CYjd+Lo5QIeQ0H:b33vekXKk2p/eHYILo5Qd
MD5:	84B399257C7078B6C8051DA088694690
SHA1:	1219498C3CAF8229F5B22EC8DFAC409995808ED2
SHA-256:	2E8859F136956CE2AE0C5330BF402A9CF673B6A5191E394232FA2CC6364C3C43
SHA-512:	4BB038DC7C07AD69E109A27A5ABD8FB9B22EADECA72BB8C0FB35ABE0DDC56F3FDA358064E1FE0425EDABC7303D9AC99A66A88A28D9CA58B031BF6D7A3F9DBEED
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://prod.msocdn.com/2021.1.28.2/en-US/JSC/MicrosoftAjaxCombined.js
Preview:	var $get,$create,$addHandler,$addHandlers,$clearHandlers,$common,CommonToolkitScripts,$AA;(function(n,t){function vt(){function ru(n,i){function l(n){if(typeof f!==h)throw Error.argument("value",String.format(t.Res.enumInvalidValue,n,this.__typeName));}var r=this,u,f,c,o,s,y;if(i){if(u=r.__lowerCaseValues,!u){r.__lowerCaseValues=u={},o=r.prototype;for(s in o)u[s.toLowerCase()]=o[s]}}else u=r.prototype;if(r.__flags){for(var a=(i?n.toLowerCase():n).split(dt),v=0,e=a.length-1;e>=0;e--)y=a[e].trim(),f=u[y],typeof f!==h&&l.call(r,n.split(dt)[e].trim()),v|=f;return v}return c=i?n.toLowerCase():n,f=u[c.trim()],typeof f!==h&&l.call(r,n),f}function uu(n){var u=this,e,t,r,s,h,c,o;if(typeof n===f||n===i)return u.__string;if(e=u.prototype,u.__flags&&n!==0){if(r=u.__sortedValues,!r){r=[];for(t in e)r.push({key:t,value:e[t]});r.sort(function(n,t){return n.value-t.value}),u.__sortedValues=r}for(s=[],h=n,t=r.length-1;t>=0;t--)if((c=r[t],o=c.value,o!==0)&&(o&n)===o&&(s.push(c.key),h-=o,h===0))break;if(

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\RE1Mu3b[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 216 x 46, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	4054
Entropy (8bit):	7.797012573497454
Encrypted:	false
SSDEEP:	48:zICvnyRHJ3BRZPcSPQ72N2xoiR4fTJX/rj4sFNMkk5/p1k2lPUmbm39o4aL7V9XH:10nvE724xoiRQJPrjpLKSFl9oX31Z1d
MD5:	9F14C20150A003D7CE4DE57C298F0FBA
SHA1:	DAA53CF17CC45878A1B153F3C3BF47DC9669D78F
SHA-256:	112FEC798B78AA02E102A724B5CB1990C0F909BC1D8B7B1FA256EAB41BBC0960
SHA-512:	D4F6E49C854E15FE48D6A1F1A03FDA93218AB8FCDB2C443668E7DF478830831ACC2B41DAEFC25ED38FCC8D96C4401377374FED35C36A5017A11E63C8DAE5C87

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\RE1Mu3b[1].png	
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://img-prod-cms-rt-microsoft-com.akamaized.net/cms/api/am/imageFileData/RE1Mu3b?ver=5c31
Preview:	.PNG.....IHDR.....J.....tEXtSoftware.Adobe ImageReadyq.e<...(iTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c132 79.159284, 2016/04/19-13:13:40 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpMM:DocumentID="xmp.did:A00BC639840A11E68CBEB97C2156C7FD" xmpMM:InstanceID="xmp.iid:A00BC638840A11E68CBEB97C2156C7FD" xmp:CreatorTool="Adobe Photoshop CC 2015.5 (Windows)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:A2C931A470A111E6AEDFA14578553B7B" stRef:documentID="xmp.did:A2C931A570A111E6AEDFA14578553B7B"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>.....DIDATx..\..UU.>.7..3....h.L..& j2...h.@.."........`U.....R"..Dq.&.BJR 1.4`$.200...l.....wg.y.[k/

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\ResetPassword[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	154569
Entropy (8bit):	5.504739614881644
Encrypted:	false
SSDEEP:	3072:Xf4RW2Jem/ZtvegpjK7AqkcCab4bF5LHTXun7ewbBN8isv55VzdgOy:Xf4RW2smtpe0qkU4bF5/cdBNvsv55Zly
MD5:	6E3A59BBF78B4580464D6EC638B56C0C
SHA1:	C27C5534207098D6039032CE98875B22847856A8
SHA-256:	7AA183CBE0570BA4FEB475AD6342CBBE3129A2B19FCE7E3AD379E0C00FC323B6
SHA-512:	CFC663D88C3777AFBEBD529F42FA828D1EF541084E5AEEA3B8823D3329528CFFF2F06AE8B81850D083E5B5ED5A1C4AEAC8541F1CC1970FDC1883CBF472FDD4A
Malicious:	false
Reputation:	low
Preview:	.. Copyright (C) Microsoft Corporation. All rights reserved. -->....<!DOCTYPE html>..<html lang="en" xml:lang="en" class="m_ul" dir="ltr" style="">.. <head>.. <link rel="preconnect" href="https://acctcdn.msauth.net" crossorigin>..<link rel="preconnect" href="https://acctcdn.msauth.net" crossorigin>..<meta http-equiv="x-dns-prefetch-control" content="on">..<link rel="dns-prefetch" href="//acctcdn.msauth.net">..<link rel="dns-prefetch" href="//acctcdn.msftauth.net">..<link rel="dns-prefetch" href="//acctcdnmsftuswe2.azureedge.net">..<link rel="dns-prefetch" href="//acctcdnvzeuno.azureedge.net">.... <title>Reset your password</title>.. <meta http-equiv="Content-Type" content="text/html;charset=utf-8"/><meta name="referrer" content="origin"/><meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=2.0, minimum-scale=1.0, user-scalable=yes"/><meta name="format-detection" content="telephone=no"/>.. <link rel="shortcut icon" href="https://acctcdn.ms

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\accountcorepackage_ugsPz17NG3A8-KfxIO31oA2[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	52933
Entropy (8bit):	5.351100385160471
Encrypted:	false
SSDEEP:	1536:Wwr2X/amFvFSpN5COh97LDc/Kjt//u72Yp:Wwr2X/Dyjt/m72Yp
MD5:	BA0B0FCF5ECD1B703CF8A7F120EDF5A0
SHA1:	37B0E3E50081524E47E2DFC0750F40DB06932241
SHA-256:	341CE71CE7FB6B3A2351C6A706272F3532A2A1959A7AF1949EEF122F2C002DD9
SHA-512:	AF27AD18A4082B2352A7DD3C79918B47A54E845A683184197107C11B5CAF88A820EADD7C7069245E54AA85B3CAF1C4E7DE9B2C0E36CDA0EC37070C4CC115015
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://acctcdn.msauth.net/accountcorepackage_ugsPz17NG3A8-KfxIO31oA2.js?v=1
Preview:	!function(){function e(){}function t(t){var n=d.Animations;return!n||e.$forcejQuery||t?!1:n.Enabled||!1}function n(e,t,n){if($B.IE){try{e[0].style.removeAttribute("filter")}catch(i){}}o(e,t,n)}function o(e,t,n){e&&(t?(e.show(),e.css("opacity","1")):(e.css("opacity","0"),e.hide())),n&&n()}function i(e,t,n){setTimeout(function(){o(e,t,n)},0)}function a(){var e=$PageHelper.byId("identityBanner");return e&&e.length>0?e:null}function r(){var e,t=document.createElement("div"),n={"animation":"animationend","OAnimation":"oAnimationEnd","MozAnimation":"animationend","WebkitAnimation":"webkitAnimationEnd"};.for(var o in n){if(void 0!==t.style[o]){return e=n[o],n[o]}}return""}function l(t,n){var o=$PageHelper.byId("inner");if(o.length>0){if(!t){return void o.removeClass("zero-opacity")}o.hasClass("zero-opacity")?(o.one(e.animationEndEventName,function(){o.removeClass("zero-opacity"),n&&n()}),o.addClass("fade-in-lightbox")):n&&n()}}function s(){var e=!1,t=["Webkit","Moz","O"],n=document.createElem

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\adoption[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	18845
Entropy (8bit):	5.128348921406134
Encrypted:	false
SSDEEP:	192:UlxdkcwG9qyC6homLcjMKyhzja8iVXaSWRgajoaGB:kfLoI3hzj7iVXaSWS8oaGB
MD5:	B89215CF3658A1D3AAD846694D6E88AD
SHA1:	63223E964C83A2C81357DE51F2D09EEB80371286
SHA-256:	9F00A847B64F6D6C669BE4D0C726C9EFB2F0E21574B7E64E4F538CE6AC47E429

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\adoption[1].css	
SHA-512:	4ED209597F6CF48578C9DDE3972E58B48584F4618D345292E1D3F1A805D2A7241EA42C3E7994D163D98D4DC2B8C8531614BD558BCEB5C15867C00A83895080EI
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://prod.msocdn.com/2021.1.28.2/en-US/css/adoption.css
Preview:	.padding{bottom:-29px}div.PageLayout td.Content{width:100%;padding:0;vertical-align:top}#ShellContainer{display:none}.left-nav{height:auto}.nomaxwidth{max-width:none}.background{overflow:visible}h1.offertitle{color:#fff;padding-top:170px;padding-right:15px;padding-bottom:10px;padding-left:25px}h1.content-title{font-size:72px;font-family:"SegoeUI-Light-final","Segoe UI Light","Segoe UI",Segoe,Tahoma,Helvetica,Arial,Sans-Serif;line-height:80px;margin-bottom:0;padding-bottom:5px}.screen{min-height:0}.norightpadding{padding-right:0}.noleftpadding{padding-left:0}.spaceforbanner{margin-top:40px;margin-bottom:0}select{width:auto;border:1px solid #a3aeaf;border-image:none;font-size:17px}#CountrySelection_SelectedRegion{min-width:260px}.Year{width:120px}.Month{width:140px}.Day{width:70px}.screen .content{width:600px;padding-left:0;padding-top:60px}.black{color:#000}h2.black{color:#000}h2.listitem{color:#000;margin-top:10px}ul.description{padding-left:28px}li.description{list-style-type:disc}.da

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\bootstrap_3.3.0_B68S-_daR6nLiLVZsh4XiA2[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	37431
Entropy (8bit):	5.2074072548864425
Encrypted:	false
SSDEEP:	768:4YApOpkHNjkaTqUftZ2lz5+BAUGy2K7fIs9sKMgZVBm27RE:4Y41Nft9+BAxKzM
MD5:	07AF12FBF75A47A9CB88B559B21E1788
SHA1:	18C081E65B1E93C3FFE4E342895BA8E9C6C0C08A
SHA-256:	2D37191A3FF388D282C09350ECF39A3EB9E6DA48296B9EA35BECCBFF92D1725B
SHA-512:	8F137FD094B57BA529CAA09D8B289FF322A3DB5284673BA178130A15720F3D0E25D67719A6836DAB26B7B439B8E976EAD66C1AABB91A15729EE1CC863F7D301E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://acctcdn.msauth.net/bootstrap_3.3.0_B68S-_daR6nLiLVZsh4XiA2.js?v=1
Preview:	/*!.--- START OF THIRD PARTY NOTICE ---..This file is based on or incorporates material from the projects listed below (Third Party IP). The original copyright notice and the license under which Microsoft received such Third Party IP, are set forth below. Such licenses and notices are provided for informational purposes only. Microsoft licenses the Third Party IP to you under the licensing terms for the Microsoft product. Microsoft reserves all other rights not expressly granted under this agreement, whether by implication, estoppel or otherwise. .//----------.twbs-bootstrap-sass (3.3.0).//----------..The MIT License (MIT)..Copyright (c) 2013 Twitter, Inc..Permission is hereby granted, free of charge, to a person obtaining a copy.of this software and associated documentation

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\commonhealthdashboard[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	4189
Entropy (8bit):	5.10186054799555
Encrypted:	false
SSDEEP:	96:DqMruZD919+9rf9Q959S9X9T9j9O9w9S9P9gKto9wXlraRNvZ5neN9/vFo:DBK1GUvvm
MD5:	D44B66A9A76B043107AF4E9E077F7E8E
SHA1:	D7F26721B5EC0561C8E19A40498E147BC0CEA931
SHA-256:	BFE8E35907D77DD95BD17FFFB1E84F6CEF9D3928AD6DF43072FC6E93A87D2FA0
SHA-512:	D563F5F62F23535A96EF79B0CE63910F5390B9E63C3162D51FD76463200B44BD344B5B56DE4EB58A173196B8499D53E4ADEF7D554CC6BDE6FCA7DD88B3C4910C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://prod.msocdn.com/2021.1.28.2/en-US/css/commonhealthdashboard.css
Preview:	.DataTable{width:100%}.DataTable td,.DataTable th{padding-left:12px;padding-right:12px;font-size:9pt;line-height:normal;padding-bottom:4px;padding-top:4px;border-color:#fff;border-right:solid 1px transparent;border-bottom:solid 1px transparent}.DataTable th{font-size:10pt;padding-top:0;border-bottom-width:0}.DataTable td.Header{font-size:10pt}.DataTable .TabelTitle{font-weight:bold}.DataTable tr.odd>td{background-color:#f7fbfe}.DataTable tr.odd+tr>td{background-color:#edf6fd}.DataTable tr:first-child>th{border-bottom:solid 0 transparent;padding-bottom:0}.DataTable TH.LeftRoundCorner B,.DataTable TH.LeftRoundCorner I,.DataTable TH.LeftRoundCorner U{line-height:0;display:block;height:0;font-size:1px;color:#b2e6f9}.Page-Modern .DataTable TH.LeftRoundCorner B,.Page-Modern .DataTable TH.LeftRoundCorner I,.Page-Modern .DataTable TH.LeftRoundCorner U{display:none}.DataTable TH.LeftRoundCorner B{border-bottom:1px solid;margin:0 0 0 2px}.Page-Modern .DataTable TH.LeftRoundCorner B{display:none}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\converged.v2.login.min_xu7km3oxm4bwp2b-mqyozg2[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	102261
Entropy (8bit):	5.304993895573072
Encrypted:	false
SSDEEP:	1536:QpHDglHuhw+E3mazA/PWrF7qvEAFiQcpmNtpHzyJRr:lB4byJZ
MD5:	5EEEE49B73979B86F0A7607E32ACA866

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\converged.v2.login.min_xu7km3oxm4bwp2b-mqyozg2[1].css	
SHA1:	75329D55D86E0D1B803BA5A641203A37C8B9C5B7
SHA-256:	6013F9292BBF154CD978A519E9BA6D501C57C50118E1535A374B0E6473FEC91C
SHA-512:	AE55F8C8C5AADFB1795A2E2BDA9E76F5845A56C79B70A69870726BA5F68A613045AD564B2AD312EE59F993EE5A6CD5D5DCE2D986B1EA3EA5D289B87D578CF 73
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://secure.aadcdn.microsoftonline-p.com/ests/2.1.8576.13/content/cdnbundles/converged.v2.login.min_xu7km3oxm4bwp2b-mqyozg2.css
Preview:	/*! Copyright (C) Microsoft Corporation. All rights reserved. *//*!.--- START OF THIRD PARTY NOTICE ---..This file based on or incorporates material from the projects listed below (Third Party IP). The original copyright notice and the license under which Microsoft received such Third Party IP, are set forth below. Such licenses and notices are provided for informational purposes only. Microsoft licenses the Third Party IP to you under the licensing terms for the Microsoft product. Microsoft reserves all other rights not expressly granted under this agreement, whether by implication, estoppel or otherwise...//-------------------------- ---.twbs-bootstrap-sass (3.3.0).//--..The MIT License (MIT)..Copyright (c) 2013 Tw Inc..Permission is hereby granted, free of charge, to any person

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\datarequestpackage_h-_7C7UzwdefXJT9njDBTQ2[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	8111
Entropy (8bit):	5.339313763115951
Encrypted:	false
SSDEEP:	192:nEAKv577D9kgT/xwj9O8hFNFxgLdQ0Eoxr:E177Dj+yt
MD5:	87EFFB0BB533C1D79F5C94FD9E30C14D
SHA1:	4E4F5F3CDDDDBFDDB46A1626D7CE579A639DE389
SHA-256:	617E32CA57507098771FD30AF6B9DCAB063448F6D7E0BC6D6557DD1895F80543
SHA-512:	CB107C09F9A32D85BF2AF714EE9BF7CE2649AA33E63C2255D4BBD281E3CDA8FBDFA2E58212E8004AEEAAB4DD8C94543F82187C7673189CACBDD5CD8C26C5 3F7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://acctcdn.msauth.net/datarequestpackage_h-_7C7UzwdefXJT9njDBTQ2.js
Preview:	!function(){function e(e){function t(e){return e&&e.state==l&&(e.prev&&(e.prev.next=e.next),e.next&&(e.next.prev=e.prev),D==e&&(D=e.next),$==e&&($=e.prev),e.state=u,e.prev=e.next=null,y--),e}function a(e){if(e&&e.state==u){var r=$;r?(r.next=e,e.prev=r):D=e,$=e,e.state=l,y++}}function f(){!q&&!b&&y&&x>w&&(b=window.setTimeout(g,s))}function v(e){var r=(new Date).getTime()-e<i;return r}function g(){var e=(new Date).getTime();for(b=0,q=!0;y>0&&x>w;){var r=D;if(r&&x>w?(o.assert(r.state===l,"Task was not in a pending state and we were just about to execute it."),r=m(t(r))):r=null,r&&!v(e)){break.}}q=!1,f()}function m(e){if(e){o.assert(void 0!=e.id&&!A[e.id],"Task didn't have an id or was already active!"),w++,A[e.id]=e,e.startTime=(new Date).getTime(),e.state=c;var r=e.exec(function(r){T(e,r)});r||T(e)}return e}function T(e,r){e.state===c&&(w--,o.assert(A[e.id],"A task is being completed without being in the active task list."),delete A[e.id],r&&"number"==typeof r?(e.state=d,e.timeoutId=wind

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
Reputation:	low
IE Cache URL:	http://https://www.microsoft.com/favicon.ico?v2
Preview:	.............h(..f...HH..........(..00......h....6.. ....=..............@.........(....A..(...................(...................................."P......................................"""""""""""""""""""""""" ...3 3333333333333333333333333333"""""""""""""""""""""""" ...333333333333333333333333333"""""""""""""""""""""""" ...3333333333333333333333333333"""" """""""""""""""""""" ...3333333333333333333333333333"""""""""""""""""""""""" ...3333333333333333333333333333"""""""""""""""""""""""" ...33333333333 33333333333333333"""""""""""""""""""""""" ...3333333333333333333333333333"""""""""""""""""""""""" ...3333333333333333333333333333"""""""""""""""""""""""""" """""""" ...3333333333333333333333333333"""""""""""""""""""""""" ...3333333333333333333333333333"""""""""""""""""""""""" ...33333333333333333333 333333333"""""""""""""""""""""""" ...3333333333333333333333333333"""""""""""""""""""""

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\icons[1].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), icons family
Category:	downloaded
Size (bytes):	4388
Entropy (8bit):	5.568378803379191
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\icons[1].eot	
SSDEEP:	96:2WZx42qACoApC6do8MPOGiN4mER38GTDfO/fv:1x42qAHAo6VMPi6mcTy
MD5:	77E1987DF3A0274C5A51E3C55CEE7C98
SHA1:	9B0FE96AF141AB09183F386F65BC627B8C396460
SHA-256:	EF04649D4D068673CF0FA47EF4C45C8BE291E703F4EC5FC0E507F17839120AA2
SHA-512:	B1E0CFB515FF2298799BA54574899D27B1FC043F66CC4E9591C504F88273B98697B99ED25955DB84986B39ED9F51864611833DC88064B14C29ADC020FBF6E295
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.onestore.ms/cdnfiles/external/oneui/oneui1.16.2/dist/fonts/icons/icons.eot?
Preview:	$.....LP.....G.....i.c.o.n.s.....R.e.g.u.l.a.r.....V.e.r.s.i.o.n. .1...0.....i.c.o.n.s..... OS/2@.Mn...(...Vcmap.1.....Jglyf.....dhead.9.....6hhea.$.....$hmtx@.....loca". h...L...Bmaxp.3.`..... name.....post{NK..... .....G..._.<.....|.....|..... .T.....D.l...H.D.l.....PfEd.@.....D.....(....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\jquery-1.11.2.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	95931
Entropy (8bit):	5.394232486761965
Encrypted:	false
SSDEEP:	1536:5P1vk7i6GUHdXXeyQazBu+4HhiO2AEeLNFoqqhJ7SerN5sVI6xcBgPv7E+nzms9d:A4Ud4qhJvNPqcB47MfWWca98HrB
MD5:	5790EAD7AD3BA27397AEDFA3D263B867
SHA1:	8130544C215FE5D1EC081D83461BF4A711E74882
SHA-256:	2ECD295D295BEC062CEDEBE177E54B9D6B19FC0A841DC5C178C654C9CCFF09C0
SHA-512:	781ACEDC99DE4CE8D53D9B43A158C645EAB1B23DFDFD6B57B3C442B11ACC4A344E0D5B0067D4B78BB173ABBDED75FB91C410F2B5A58F71D438AA6266D048 98A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ajax.aspnetcdn.com/ajax/jQuery/jquery-1.11.2.min.js
Preview:	/*! jQuery v1.11.2 | (c) 2005, 2014 jQuery Foundation, Inc. | jquery.org/license */!function(a,b){"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a document");return b(a)}:b(a)}("undefined"!=typeof window?window:this,function(a,b){var c=[],d=c.slice,e=c.concat,f=c.push,g=c.indexOf,h={},i=h.toString,j=h.hasOwnProperty,k={},l="1.11.2",m=function(a,b){return new m.fn.init(a,b)},n=/^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g,o=/^-ms-/,p=/-([\da-z])/gi,q=function(a,b){return b.toUpperCase()};m.fn=m.prototype={jquery:l,constructor:m,selector:"",length:0,toArray:function(){return d.call(this)},get:function(a){return null!=a?0>a?this[a+this.length]:this[a]:d.call(this)},pushStack:function(a){var b=m.merge(this.constructor(),a);return b.prevObject=this,b.context=this.context,b},each:function(a,b){return m.each(this,a,b)},map:function(a){return this.pushStack(m.map(this,function(b,c){ret

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\jquery-1_10_2_min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	93263
Entropy (8bit):	5.266897951658619
Encrypted:	false
SSDEEP:	1536:gvFVsQpvCipiGzxaUCZaq0s6DPINAx+DmLhgfYscDBqV9lNd1m8aZ3lv7fb:Gs1NiuBHsazfb
MD5:	CC2255710C7637FF58CB53B3B3576930
SHA1:	43A9736602454573C563CCB7A44743F3C8F0403B
SHA-256:	55476BB72FD6EDEA704C754CB080EAA78301AC372AB3AF1E9E075A4EA8FE4FB0
SHA-512:	667A1120D94C3F7F72F6F2B952E2A485B2A8AB0CE38BF3E2DFA16093226C647AA8D0CE7A87188CD227F939C0C90FA5F460F5B2792580EBC75CB702550548FD4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://prod.msocdn.com/2021.1.28.2/en-US/JS/jQuery/jquery-1_10_2_min.js
Preview:	/*! jQuery v1.10.2 with a fix integrated from v1.12.2 and 3.4.0 | (c) 2005, 2013 jQuery Foundation, Inc. | jquery.org/license */.(function(n,t){function wi(n){var t=n.length,r=i.type(n);return i.isWindow(n)?!1:1===n.nodeType&&t?!0:"array"===r||"function"!==r&&(0===t||"number"==typeof t&&t>0&&t-1 in n)}function fe(n){var t=pi[n]={};return i.each(n.match(s)||[],function(n,i){t[i]=!0}),t}function ru(n,r,u,f){if(i.acceptData(n)){var h,o,c=i.expando,l=n.nodeType,s=l?i.cache:n,e=l?n[c]:n[c]&&c;if(e&&s[e]&&(f||s[e].data)||u!==t||"string"!=typeof r)return e||(e=l?n[c]=b.pop()||i.guid++:c),s[e]||(s[e]=l?{}:{toJSON:i.noop}),("object"==typeof r||"function"==typeof r)&&(f?s[e]=i.extend(s[e],r):s[e].data=i.extend(s[e].data,r)),o=s[e],f||(o.data||(o.data={}),o=o.data),u!==t&&(o[i.camelCase(r)]=u),"string"==typeof r?(h=o[r],null==h&&(h=o[i.camelCase(r)])):h=o,h}}function u u(n,t,r){if(i.acceptData(n)){var e,o,s=n.nodeType,u=s?i.cache:n,f=s?n[i.expando]:i.expando;if(u[f]){if(t&&(e=r?u[f]:u[f].data)){fo

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\knockout_GJ62c6D9R5HuKFdkoO8XYw2[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):	78311
Entropy (8bit):	5.421676443255173
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\knockout_GJ62c6D9R5HuKFdkoO8XYw2[1].js	
SSDEEP:	1536:yOWjonYwd51CleWm3vTJhFR0aXBo1nuQvEODDRLmutNnbt:xP5Cf5/bt
MD5:	189EB673A0FD4791EE285764A0EF1763
SHA1:	13273A13087F0B15C2D9E8C72EA1CAF2E1256B07
SHA-256:	C58E92C3ABAC24575F36960372E39F10AC0E20B3C33B605F2B3D3E1498ACF025
SHA-512:	C59597872F1A972D6F2E08B51C95F1E497B4765BC468086F0AA98F8F9D31504E17349EE114D17C35BE31B2784ED3F3D4097954142E7D9A6CC75C97CC3FAA0838
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://acctcdn.msauth.net/knockout_GJ62c6D9R5HuKFdkoO8XYw2.js?v=1
Preview:	/*!---------- START OF THIRD PARTY NOTICE ----------....This file is based on or incorporates material from the projects listed below (Third Party IP). The original copyright notice and the license under which Microsoft received such Third Party IP, are set forth below. Such licenses and notices are provided for informational purposes only. Microsoft licenses the Third Party IP to you under the licensing terms for the Microsoft product. Microsoft reserves all other rights not expressly granted under this agreement, whether by implication, estoppel or otherwise. .... * Knockout JavaScript library v3.2.0.. * (c) Steven Sanderson - http://knockoutjs.com/.. * License: MIT (http://www.opensource.org/licenses/mit-license.php)....Provided for Informational Purposes Only....MIT License ....Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the Software)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\lightweightsignuppackage_fo7wvnccA0cj8u_fEx_M5w2[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):	182823
Entropy (8bit):	5.3881965733523405
Encrypted:	false
SSDEEP:	3072:6KXp81D/3gWVS2XuiwU4m99VDzTef290EL:tnPU4mNZ
MD5:	7E8EF0BE771C034723F2EFDF131FCCE7
SHA1:	07F8BCDC4DA23A46FE9C40EE5243C0F96A90CD6B
SHA-256:	6E470108B86A13F62935CD948A53E5FF098A4448FA5FF93E38F2F03C0410920C
SHA-512:	0D07783EB7F6A344BD40578B5755D5918AB2EB504CA47B5CE12067C4FE19114739AABC0D051A5D4BDEA4C94105820B03B9D7CCB507C5699447715315585B65D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://acctcdn.msauth.net/lightweightsignuppackage_fo7wvnccA0cj8u_fEx_M5w2.js?v=1
Preview:	function Encrypt(e,t,n,a){var i=[];switch(n.toLowerCase()){case"chgsqsa":if(null==e||null==t){return null}i=PackageSAData(e,t);break;case"chgpwd":if(null==e||null==a){return null}i=PackageNewAndOldPwd(e,a);break;case"pwd":if(null==e){return null}i=PackagePwdOnly(e);break;case"pin":if(null==e){return null}i=PackagePinOnly(e);break;case"proof":if(null==e&&null==t){return null}i=PackageLoginIntData(null!=e?e:t);break;case"saproof":if(null==t){return null}i=PackageSADataForProof(t);break;case"newpwd":if(null==a){return null.}i=PackageNewPwdOnly(a)}if(null==i||"undefined"==typeof i){return i}if("undefined"!=typeof Key&&void 0!==parseRSAKeyFromString){var r=parseRSAKeyFromString(Key)}var o=RSAEncrypt(i,r,randomNum);return o}function PackageSAData(e,t){var n=[],a=0;n[a++]=1,n[a++]=1,n[a++]=0;var i,r=t.length;for(n[a++]=2*r,i=0;r>i;i++){n[a++]=255&t.charCodeAt(i),n[a++]=(65280&t.charCodeAt(i))>>8}var o=e.length;for(n[a++]=o,i=0;o>i;i++){n[a++]=127&e.charCodeAt(i)}return n}function PackagePwdOn

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\lwsignupstringscountrybirthdate_en-us_VxjLzmQAiLRyhA2ROX72uQ2[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	26140
Entropy (8bit):	5.069224830328935
Encrypted:	false
SSDEEP:	384:Z3EReHg2sQhdCdcPxZebPrmuex3dmac3zirs7rOubUrUA/4RkG:lQAg2sQrGbPrmjx3dmac3ziarbnAY
MD5:	5718CBCE640088B472840D91397EF6B9
SHA1:	3C83F10E5CC8B453E7BE23EC594CE7883CE035D8
SHA-256:	F73506F457BD65E70E276E763582735DFF572124815CC1EEC10E1A235F7D4F73
SHA-512:	3F8785D72725EEFF7635CA955DB621DAD8D946DD72BE0C5DAE3B93CE867298E39929AEC0FC3F132452C29FDCA395284264036D60293B36C253B4567FF6880DA
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://acctcdn.msauth.net/lwsignupstringscountrybirthdate_en-us_VxjLzmQAiLRyhA2ROX72uQ2.js?v=1
Preview:	!function(){registerNamespace("$Config"),$Config.sharedStrings={"errors":{"required":"This information is required.","emailRequired":"An email address is required","phoneRequired":"A phone number is required","passwordRequired":"A password is required","invalidEmailFormat":"Enter the email address in the format someone@example.com.","invalidPhoneFormat":"The phone number you entered isn't valid. Your phone number can contain numbers, spaces, and these special characters: ( ) [ ] . - */","emailMustStartWithLetter":"Your email address needs to start with a letter. Please try again.","memberNameAvailable":"{0} is available.","memberNameAvailableasi":"After you sign up, we'll send you a message with a link to verify this user name.","memberNameExistsPhone":"If you own a Microsoft account with this number, go back and sign in.","proofAlreadyExistsError":"This is already part of your security info.","signupBlocked":"{0} isn't available.","memberNameTakenPhone":"The phone number you typed i

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\microsoft_logo_ee5c8d9fb6248c938fd0dc19370e90bd[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	3651
Entropy (8bit):	4.094801914706141

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\microsoft_logo_ee5c8d9fb6248c938fd0dc19370e90bd[1].svg	
Encrypted:	false
SSDEEP:	96:wO4DZ+Stb/jY+eo4hAryAes9mBYYQgWLDm9:wToSBjlevudl9nO
MD5:	EE5C8D9FB6248C938FD0DC19370E90BD
SHA1:	D01A22720918B781338B5BBF9202B241A5F99EE4
SHA-256:	04D29248EE3A13A074518C93A18D6EFC491BF1F298F9B87FC989A6AE4B9FAD7A
SHA-512:	C77215B729D0E60C97F075998E88775CD0F813B4D094DC2FDD13E5711D16F4E5993D4521D0FBD5BF7150B0DBE253D88B1B1FF60901F053113C5D7C1919852D5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://secure.aadcdn.microsoftonline-p.com/ests/2.1.8576.13/content/images/microsoft_logo_ee5c8d9fb6248c938fd0dc19370e90bd.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="108" height="24" viewBox="0 0 108 24"><title>assets</title><path d="M44.836,4.6V18.4h-2.4V7.583H42.4L38 .119,18.4H36.531L32.142,7.583h-.029V18.4H29.9V4.6h3.436L37.3,14.83h.058L41.545,4.6Zm2,1.049a1.268,1.268,0,0,1,.419-.967,1.413,1.413,0,0,1,1-.39,1.392, 1.392,0,0,1,1.02.4,1.3,1.3,0,0,1,.4.958,1.248,1.248,0,0,1-.414.953,1.428,1.428,0,0,1-1.01.385A1.4,1.4,0,0,1,47.25,6.6a1.261,1.261,0,0,1-.409-.948M49.41,18.4H47. 081V8.507H49.41Zm7.064-1.694a3.213,3.213,0,0,0,1.145-.241,4.811,4.811,0,0,0,1.155-.635V18a4.665,4.665,0,0,1-1.266.481,6.886,6.886,0,0,1-1.554.164,4.707,4.707,0, 0,1-4.918-4.908,5.641,5.641,0,0,1,1.4-3.932,5.055,5.055,0,0,1,3.955-1.545,5.414,5.414,0,0,1,1.324.168,4.431,4.431,0,0,1,1.063.39v2.233a4.763,4.763,0,0,0-1.1-.61 1,3.184,3.184,0,0,0-1.15-.217,2.919,2.919,0,0,0-2.223.9,3.37,3.37,0,0,0-.847,2.416,3.216,3.216,0,0,0,.813,2.338,2.936,2.936,0,0,0,2.209.837M65.4,8.343a2.952,2.9 52,0,0,1,.5.039,2.1,2.1,0,0,1,.375.1v2.358a2.04,2.04,0,0,0-.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\print-icon[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGB, non-interlaced
Category:	downloaded
Size (bytes):	173
Entropy (8bit):	5.970149697517944
Encrypted:	false
SSDEEP:	3:yionv//thPl9vtt+NTl0qRthwkBDsTBZtqmA73Fs+rQx33npdtnoypZh9Dicl2up:6v/lhPmNp0WnDspBAzqPnpdiyTh9Fp
MD5:	023F5AC6E0114AF1F781BE5D3C956385
SHA1:	C166284B8541F1DE32DC5C4DEC635C296BF85C98
SHA-256:	75D637BF6B6DFF2525095D0BE7E0C90F012BB118C2EF19099AFDCBC630ADFC79
SHA-512:	DAFA49056E3D3014DB392410685CC05773C09938E2E700657727928EDCFF8EA2D7C769D377539C52DA70321B94F4E8F045F565EC51BC2B701D95BB3213CC220
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/print-icon.png?version=60ebb5de-511c-db20-3795-563c739c5e12
Preview:	.PNG.....IHDR.....h6....tEXtSoftware.Adobe ImageReadyq.e<...OIDATx.b...?..0222`..jX..a5...D0.50.....k.....:...X=....'..(..I.....K..... .....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\privacystatement[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	330955
Entropy (8bit):	4.858738085049129
Encrypted:	false
SSDEEP:	3072:zY698dd87wNHDmdS9v+6WjUiPryCGZN9ruekUIx4z7ZV/BdQZyNdkugyZCqTDHwu:zO87yjftCrYNb8yQZyZCSDH+ekA
MD5:	6DDFEFC7D53AA143D3EEA75B4EB77264
SHA1:	2F3D989575E48956A1F7DF03AB0DCF44978C624C
SHA-256:	A12A68087E7B6546A0BFCA1D7FB47215DE431387FC6BF1A82B26FA0610CC0A82
SHA-512:	BDA6E85238D9017B72BC8778967E760DBBEC970A2D935C0C7C4CE4D9C9ADB110A2892DA6F67E0639A1FD17D88DB4691BC17FC275035BE12C4779279F3A0954 A
Malicious:	false
Reputation:	low
Preview:	.<!DOCTYPE html ><html xmlns:mscom="http://schemas.microsoft.com/CMSvNext" xmlns:md="http://schemas.microsoft.com/mscom-data" lang="en-us" xmlns="http ://www.w3.org/1999/xhtml"><head><meta http-equiv="X-UA-Compatible" content="IE=edge" /><meta charset="utf-8" /><meta name="viewport" content="width=device-width, initial-scale=1.0" /><link rel="shortcut icon" href="https://www.microsoft.com/favicon.ico?v2" /><script type="text/javascript" src="https://ajax.aspnetcdn.com/ajax/jQuery/jquery-1.11.2.min.js">...// Third party scripts and code linked to or referenced from this website are licensed to you by the parties that own such code, not by Microsoft. See ASP.NET Ajax CDN Terms of Use - http://www.asp.net/ajaxlibrary/CDN.ashx... </script><script type="text/javascript" language="javascript">/*<![CDATA[*/if($(document).bind("mobileinit",function(){$.mobile.autoInitializePage=!1}),navigator.userAgent.match(/IEMobile\/10\.0/)){var msViewportStyle=document.createElement ("style");msViewpo

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\resetpasswordpackage_I2DMdH8ooiCXVl6e3pVpWw2[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):	105427
Entropy (8bit):	5.393098665541043
Encrypted:	false
SSDEEP:	3072:RxnHnkgdaZjlkV2XkV14C2XVj2XR1zPXGCPXFUoQ29uZG/i6:3daVlS7Uobs6
MD5:	2360CC747F28A22097565E9EDE95695B

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\resetpasswordpackage_I2DMdH8ooiCXVl6e3pVpWw2[1].js	
SHA1:	739A28639C5168E76B111A072A716AFB3AF4544E
SHA-256:	2B3783F558AA8BB4D855AA009BA62E4A8297302D8DF847BB19366B4DD15ABCAD
SHA-512:	A69FD054805F33045172B0DDBE27B7A3FFB5BBE038FE7250C46384477AFCA8728731F18D80E6553D12FD35A1FC638DE24CD48475FFFCE1BC9CC48528C8EBAF6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://acctcdn.msauth.net/resetpasswordpackage_I2DMdH8ooiCXVl6e3pVpWw2.js?v=1
Preview:	function Encrypt(e,n,t,o){var r=[];switch(t.toLowerCase()){case"chgsqsa":if(null==e||null==n){return null}r=PackageSAData(e,n);break;case"chgpwd":if(null==e||null==o){return null}r=PackageNewAndOldPwd(e,o);break;case"pwd":if(null==e){return null}r=PackagePwdOnly(e);break;case"pin":if(null==e){return null}r=PackagePinOnly(e);break;case"proof":if(null==e&&null==n){return null}r=PackageLoginIntData(null!=e?e:n);break;case"saproof":if(null==n){return null}r=PackageSADataForProof(n);break;case"newpwd":if(null==o){return null.}r=PackageNewPwdOnly(o)}if(null==r||"undefined"==typeof r){return r}if("undefined"!=typeof Key&&void 0!==parseRSAKeyFromString){var a=parseRSAKeyFromString(Key)}var i=RSAEncrypt(r,a,randomNum);return i}function PackageSAData(e,n){var t=[],o=0;t[o++]=1,t[o++]=1,t[o++]=1,t[o++]=0;var r,a=n.length;for(t[o++]=2*a,r=0;a>r;r++){t[o++]=255&n.charCodeAt(r),t[o++]=(65280&n.charCodeAt(r))>>8}var i=e.length;for(t[o++]=i,r=0;i>r;r++){t[o++]=127&e.charCodeAt(r)}return t}function PackagePwdOn

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\script[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):	30250
Entropy (8bit):	5.330396235509644
Encrypted:	false
SSDEEP:	384:ekorlyUMfQ8sW5hXDiWiQRKKwoOdo/r4nqdRy/dRyWhtyFhtyYKQys05DU7BS5ha:0olDi2RKQOOwqjE2l/3FJ1C/n+NYiKq
MD5:	79493518F253F3F74970CF43C8A3FEEE
SHA1:	E0CC16264EA44A55C17766A5E0F0F4DB7DD8AAF2
SHA-256:	BD041981B6512D6DA32A6AE752EFE67DD0BA22FACFA9A534B0F5B08651B7852A
SHA-512:	D204999F215BA5A837391AD447F3A26461439EF4FBBF39CEC22CE970F7F86EC908FD3CF4C0500F6A529FCDF5C0707214896ECACC15FB0B04259E7EBEFF749D5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSScripts/script.jsx?k=8c27a4b8-356f-dd50-ddb2-9e2c834bf9c4
Preview:	function ShowSelectedComponentKeyPress(n,t){if(window.event.keyCode==13)return ShowSelectedComponent(n,t),!1}function SetRightSideNavigationMenuHeight(){$("[id^=dvModuleGroup_]").hide();window.location.search.toLowerCase().indexOf("bookmarkid")!=-1&&SelectBookMark();window.location.search.toLowerCase().indexOf("componentid")!=-1&&LoadSelectedInternalLink();$(".div_side_comp").length>0&&$(".div_content").css("min-height",$(".div_side_comp").height()-27)}function ShowSelectedComponent(n,t){var i=$("#"+t).attr("data-parentModule");return i!=undefined&&i!=null&&($("[data-parentmodule="+i+"]").show(),$("#"+i+" [id$=_LongDescription]").length>0?(document.getElementById(i+"_LongDescription").style.display="block",document.getElementById(i+"_ShortDescription").style.display="none",ShowText($("#"+i+".learnMoreLabel"),"long")):ShowText($("#"+i+".learnMoreLabel"),"long"),DisplayTopNavigation(i)),$("html, body").animate({scrollTop:$("#"+t).offset().top-1},800),!1}function ShowToolTip(){var n,i,t;w

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\signup16[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	20719
Entropy (8bit):	5.259688018215077
Encrypted:	false
SSDEEP:	192:IYVTebI38CI2hpE++Gv30v5z6X/PfGIR2Mh4fZqZXY+iSvkDDx9+8EFJ:pV80DhpnMUAMq6XpJ
MD5:	36A1960131BFA5384E2C4F1D94CE711B
SHA1:	27FCDE78119CA9CF4EE06E65885E098EBB54BDB0
SHA-256:	61DE99CCA945D6EDF0BC4670F04129D792829CD1E5B63BBFA103522A8804F5C1
SHA-512:	A6FDFF99136A7EA1D97A34B584A5257E75E0FF21E2331A791C348303A05FC178600148C751F40E94197E45055BD06421814E0BC436250814F64D29F245782F59
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://prod.msocdn.com/2021.1.28.2/en-US/content/css/signup16.css
Preview:	@font-face{font-family:'SegoeUI-SemiLight-final';src:url('https://prod.msocdn.com/en-US/css/webfonts/SegoeUI-SemiLight-final.eot');src:url('https://prod.msocdn.com/en-US/css/webfonts/SegoeUI-SemiLight-final.eot?iefix') format('embedded-opentype'),url('https://prod.msocdn.com/en-US/css/webfonts/SegoeUI-SemiLight-final.woff') format('woff'),url('https://prod.msocdn.com/en-US/css/webfonts/SegoeUI-SemiLight-final.ttf') format('truetype'),url('https://prod.msocdn.com/en-US/css/webfonts/SegoeUI-SemiLight-final.svg#web') format('svg');font-style:normal;font-weight:normal}html,body{height:100%}body{font-family:'SegoeUI-Regular-final','Segoe UI','Segoe WP',Tahoma,Arial,sans-serif}.hiddenImportant{display:none!important}.hidden{display:none}a{color:#da3b01;text-decoration:none}a:hover{color:#b22a0f}.container{min-height:100%;height:auto!important;height:100%;margin:0 auto -80px}.content{width:1245px;margin:0 auto;position:relative}.background{background-size:cover;position:absolute;width:100%;he

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\sprite1.mouse[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	7604
Entropy (8bit):	5.077380918925341
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\sprite1.mouse[1].css	
SSDEEP:	96:3pcJGwDdfjyFPhC4yM5FmLxip1DKfcFCIr2l:3p4GwDdfjyFPd712l
MD5:	E9BA472D2DDB09FB3EC536DC240B1976
SHA1:	99DAF55408B077F6F56DAAF6CAE4E54DC0FC0CFA
SHA-256:	461F87E55BBA34C4D9248D1B45685EA832EBA56C15EBF6CCCF75D49F1547B502
SHA-512:	CB3EE5C0DA9C69B77894BE4941B3C2DD3290D2BF00C6528CC92927038B6B593F9808AE5B33B732C9B9BAB4DDECB8FF7425CF7060D7688170AE087AF18D7122 7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://r4.res.office365.com/owa/prem/16.3809.0.3214099/resources/images/0/sprite1.mouse.css
Preview:	.image-adchoices_icon-png{background:url('adchoices_icon.png');width:12px;height:12px}.image-olk_logo_white_cropped-png{background:url('olk_logo_white_cropped.p ng');width:265px;height:310px}.image-owa_brand-png{background:url('owa_brand.png');width:160px;height:30px}.image-readingpane_recipientwell_callout-png{backgrou nd:url('readingpane_recipientwell_callout.png');width:370px;height:245px}.image-loading_blackbg-gif{background:url('loading_blackbg.gif');width:16px;height:16px}.image- loading_whitebg-gif{background:url('loading_whitebg.gif');width:16px;height:16px}.image-thinking16_blue-gif{background:url('thinking16_blue.gif');width:16px;heigh t:16px}.image-thinking16_grey-gif{background:url('thinking16_grey.gif');width:16px;height:16px}.image-thinking16_white-gif{background:url('thinking16_white.gif');width:16 px;height:16px}.image-thinking24-gif{background:url('thinking24.gif');width:24px;height:24px}.image-thinking32_blue-gif{background:url('thinking32_blue.gif');width:32px;h eight:32px

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\wlivepackagefull_gkQfr3DPKXxDWQ1F0WVujA2[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	59841
Entropy (8bit):	5.357773103890131
Encrypted:	false
SSDEEP:	1536:nxw+iAMQc2KFMj4L6fscctZtdIy+dzpqKJns+BGoK7wJ5CAJSE6gfi+585dMIS:SQtK16fwhczOj1+4MZ
MD5:	82441FAF70CF297C43590D45D1656E8C
SHA1:	B7ED8263AA1DFB72EA2039B9830CAA8AE5F70665
SHA-256:	CF5238E1F3DC27E3653F17CC6E5B9490D804D3DD7616E65556642EED8EBC9E98
SHA-512:	391BD4FF04668C5D79661576F7534950C7AE5355E232EC5B3241D68B7E3DB3781863BF85CBAEF1564AA18C1975D3591A7A8130C0CABD18EEADEF9F36863AC4E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://acctcdn.msauth.net/wlivepackagefull_gkQfr3DPKXxDWQ1F0WVujA2.js?v=1
Preview:	!function(){var e=window,t=e.$Debug;t.assert(e.$Config,"ConfigBurner should output: $Config");var n=e.$Config;if(n.handlerBaseUrl=n.handlerBaseUrl||"",!n.sd){var i=document.domain,r=i.split(".");n.sd=1===r.length?"":"."+r[r.length-2]+".com"}t.assert(n.mkt,"ConfigBurner should output: $.$Config.mkt"),n.mkt=n.mkt||"na",n.prop=n.pr op||"Account","undefined"!=typeof window.SymRealWinOpen&&(window.open=window.SymRealWinOpen)}(),function(){function e(){var e=document.title,t=documen t.location.hash;e!=r&&t&&e.indexOf(t)==e.length-t.length&&(document.title=r),r=document.title.}var t=window,n=t.wLive;t.$Debug||(t.$Debug={"enabled":!1,"trace": function(){}});var i=t.document;t._d=i,t._ce=function(e){return i.createElement(e)},t._ge=function(e){return i.getElementById(e)},t._get=function(e){return i.getElementsB yTagName(e)},t._dh=i.head=i.head||t._get("head")[0],n.dh=$PageHelper.byId("head")[0]||t._dh;var r;$PageHelper.get(document).bind("propertychange",e)}(),function() {function _objectMap(e,t){fo

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\2_bc3d32a696895f78c19df6c717586a5d[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	1864
Entropy (8bit):	5.222032823730197
Encrypted:	false
SSDEEP:	48:yvswNIBLBpJawmMH44log6gw/MHm7pJroog6gwkMH9Xog6gwdMHdqdyqog7C:ykfXYx+odPcs9B
MD5:	BC3D32A696895F78C19DF6C717586A5D
SHA1:	9191CB156A30A3ED79C44C0A16C95159E8FF689D
SHA-256:	0E88B6FCBB8591EDFD28184FA70A04B6DD3AF8A14367C628EDD7CABA32E58C68
SHA-512:	8D4F38907F3423A86D90575772B292680F7970527D2090FC005F9B096CC81D3F279D59AD76EAFCA30C3D4BBAF2276BBAA753E2A46A149424CF6F1C319DED5A6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://aadcdn.msftauth.net/ests/2.1/content/images/backgrounds/2_bc3d32a696895f78c19df6c717586a5d.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="1920" height="1080" fill="none"><g opacity=".2" clip-path="url(#E)"><path d="M1466.4 1795.2c950.37 0 1720.8-627.52 1720.8-1401.6S2416.77-1008 1466.4-1008-254.4-380.482-254.4 393.6s770.428 1401.6 1720.8 1401.6z" fill="url(#A)"/><path d="M394.2 1815.6c746.58 0 1351.8-493.2 1 351.8-1101.6S1140.78-387.6 394.2-387.6-957.6 105.603-957.6 714-352.38 1815.6 394.2 1815.6z" fill="url(#B)"/><path d="M1548.6 1885.2c631.92 0 1144.2-417.45 1144. 2-932.4S2180.52 20.4 1548.6 20.4 404.4 437.85 404.4 952.8s512.276 932.4 1144.2 932.4z" fill="url(#C)"/><path d="M265.8 1215.6c690.246 0 1249.8-455.595 1249.8-10 17.6S956.046-819.6 265.8-819.6-984-364.005-984 198-424.445 1215.6 265.8 1215.6z" fill="url(#D)"/></g><defs><radialGradient id="A" cx="0" cy="0" r="1" gradientUn its="userSpaceOnUse" gradientTransform="translate(1466.4 393.6) rotate(90) scale(1401.6 1720.8)"><stop stop-color="#107c10"/><stop offset="1" stop-color="#c4c4c4" stop-opacity="0"/></radialGradient><r

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\2_vD0yppaJX3jBnfbHF1hqXQ2[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	1864

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\2_vD0yppaJX3jBnfbHF1hqXQ2[1].svg	
Entropy (8bit):	5.222032823730197
Encrypted:	false
SSDEEP:	48:yvswNIBLBpJawmMH44log6gw/MHm7pJroog6gwkMH9Xog6gwdMHdqdyqog7C:ykfXYx+odPcs9B
MD5:	BC3D32A696895F78C19DF6C717586A5D
SHA1:	9191CB156A30A3ED79C44C0A16C95159E8FF689D
SHA-256:	0E88B6FCBB8591EDFD28184FA70A04B6DD3AF8A14367C628EDD7CABA32E58C68
SHA-512:	8D4F38907F3423A86D90575772B292680F7970527D2090FC005F9B096CC81D3F279D59AD76EAFCA30C3D4BBAF2276BBAA753E2A46A149424CF6F1C319DED5A6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://signup.live.com/Resources/images/2_vD0yppaJX3jBnfbHF1hqXQ2.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="1920" height="1080" fill="none"><g opacity=".2" clip-path="url(#E)"><path d="M1466.4 1795.2c950.37 0 1720.8-627.52 1720.8-1401.6S2416.77-1008 1466.4-1008-254.4-380.482-254.4 393.6s770.428 1401.6 1720.8 1401.6z" fill="url(#A)"/><path d="M394.2 1815.6c746.58 0 1351.8-493.2 1351.8-1101.6S1140.78-387.6 394.2-387.6-957.6 105.603-957.6 714-352.38 1815.6 394.2 1815.6z" fill="url(#B)"/><path d="M1548.6 1885.2c631.92 0 1144.2-417.45 1144.2-932.4S2180.52 20.4 1548.6 20.4 404.4 437.85 404.4 952.8s512.276 932.4 1144.2 932.4z" fill="url(#C)"/><path d="M265.8 1215.6c690.246 0 1249.8-455.595 1249.8-1017.6S956.046-819.6 265.8-819.6-984-364.005-984 198-424.445 1215.6 265.8 1215.6z" fill="url(#D)"/></g><defs><radialGradient id="A" cx="0" cy="0" r="1" gradientUnits="userSpaceOnUse" gradientTransform="translate(1466.4 393.6) rotate(90) scale(1401.6 1720.8)"><stop stop-color="#107c10"/><stop offset="1" stop-color="#c4c4c4" stop-opacity="0"/></radialGradient><r

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\2_vD0yppaJX3jBnfbHF1hqXQ2[2].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	1864
Entropy (8bit):	5.222032823730197
Encrypted:	false
SSDEEP:	48:yvswNIBLBpJawmMH44log6gw/MHm7pJroog6gwkMH9Xog6gwdMHdqdyqog7C:ykfXYx+odPcs9B
MD5:	BC3D32A696895F78C19DF6C717586A5D
SHA1:	9191CB156A30A3ED79C44C0A16C95159E8FF689D
SHA-256:	0E88B6FCBB8591EDFD28184FA70A04B6DD3AF8A14367C628EDD7CABA32E58C68
SHA-512:	8D4F38907F3423A86D90575772B292680F7970527D2090FC005F9B096CC81D3F279D59AD76EAFCA30C3D4BBAF2276BBAA753E2A46A149424CF6F1C319DED5A6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://account.live.com/Resources/images/2_vD0yppaJX3jBnfbHF1hqXQ2.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="1920" height="1080" fill="none"><g opacity=".2" clip-path="url(#E)"><path d="M1466.4 1795.2c950.37 0 1720.8-627.52 1720.8-1401.6S2416.77-1008 1466.4-1008-254.4-380.482-254.4 393.6s770.428 1401.6 1720.8 1401.6z" fill="url(#A)"/><path d="M394.2 1815.6c746.58 0 1351.8-493.2 1351.8-1101.6S1140.78-387.6 394.2-387.6-957.6 105.603-957.6 714-352.38 1815.6 394.2 1815.6z" fill="url(#B)"/><path d="M1548.6 1885.2c631.92 0 1144.2-417.45 1144.2-932.4S2180.52 20.4 1548.6 20.4 404.4 437.85 404.4 952.8s512.276 932.4 1144.2 932.4z" fill="url(#C)"/><path d="M265.8 1215.6c690.246 0 1249.8-455.595 1249.8-1017.6S956.046-819.6 265.8-819.6-984-364.005-984 198-424.445 1215.6 265.8 1215.6z" fill="url(#D)"/></g><defs><radialGradient id="A" cx="0" cy="0" r="1" gradientUnits="userSpaceOnUse" gradientTransform="translate(1466.4 393.6) rotate(90) scale(1401.6 1720.8)"><stop stop-color="#107c10"/><stop offset="1" stop-color="#c4c4c4" stop-opacity="0"/></radialGradient><r

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\54-41a2a0[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):	168646
Entropy (8bit):	5.043929314140671
Encrypted:	false
SSDEEP:	3072:jzCPZkTP3bDLH0tfRqQ0xtLfj4ZDSIpTt813viY8R1j35Ap7LQZLPPJH7PAbOCxu:jlZACLkeedh
MD5:	55A2B9AD102C59D9946DF38A108FBF84
SHA1:	65CE0F627FF9508C4DDDEBCBF7332B3D5DE1DB17
SHA-256:	CCB734F5ED4702B8E95450889F1A9B5A5FB86B697C2B2B390C608B466D8FADFB
SHA-512:	A5ECFFF6C3909513522AF8396C48050FD76631DF44CFAFF81986150A481B6B6A1ADD29150DEBFA8FE43F32397E13218845B1EFAAEF1F70E5D78E6EE415CD7AAB
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.microsoft.com/onerfstatics/marketingsites-eus-prod/west-european/shell/_scrf/css/themes=default.device=uplevel_web_pc/c2-fe9af7/b9-ae4fa3/fe-321a68/42-1cb85f/3e-dcc204/a1-352ee3/fa-ea79ed/54-41a2a0?ver=2.0
Preview:	@charset "UTF-8";./*! | Copyright 2017 Microsoft Corporation | This software is based on or incorporates material from the files listed below (collectively, "Third Party Code"). Microsoft is not the original author of the Third Party Code. The original copyright notice and the license under which Microsoft received Third Party Code are set forth below together with the full text of such license. Such notices and license are provided solely for your information. Microsoft, not the third party, licenses this Third Party Code to you under the terms in which you received the Microsoft software or the services, unless Microsoft clearly states that such Microsoft terms do NOT apply for a particular Third Party Code. Unless applicable law gives you more rights, Microsoft reserves all other rights not expressly granted under such agreement(s), whether by implication, estoppel or otherwise.*/./*! normalize.css v3.0.3 | MIT License | github.com/necolas/normalize.css */.body{margin:0}.context-uh

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\AssistancePanel[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\AssistancePanel[1].css	
Category:	downloaded
Size (bytes):	11413
Entropy (8bit):	5.022653834837725
Encrypted:	false
SSDEEP:	192:kyDKVoxucWNZdCjt0NwVkipcB+X3tHedw6yVGLJXa:kyDKVoxOZdCjt/VjpV3t+a9Y4
MD5:	3304BEC91700E40CAF7507B5BBE44C8A
SHA1:	943D9F3D8AD445481E1D9D7F9C15D55C6A94F47F
SHA-256:	14224B8810F81D0974F6F284DE197ACA928D56F967669ADF797C77DA5B039BF5
SHA-512:	AE71E8363F3D6AFEDE20BD30FB6A913A2CB2CDB6C2A8D2399807509AC82DE8DEA7E75CEBBE61213AD56C9A84E82F85563C3133A24B5820D0D04C8873FA334AD0
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://prod.msocdn.com/2021.1.28.2/en-US/css/AssistancePanel.css
Preview:	.sidepanel01{display:block;padding:0;position:absolute;right:-280px;top:5px;bottom:5px;z-index:2;pointer-events:auto}.sidepanel_wrapper{min-height:550px;width:0;padding:5px;overflow:visible;position:absolute;top:5px;bottom:5px;right:0;pointer-events:none;z-index:1}.sidepanel_wrapper div{pointer-events:auto}.sidepanel01_default{width:30px;right:0}.panel_peek{width:40px;right:0}.sidepanel01 h1{margin:18px 0}.sidepanel01 ul,.sidepanel01 ul li{padding-left:0;list-style:none}#popular-answers ul{padding-top:10px}.sidepanel_open,.sidepanel01 .sidepanel-wide-panels_closed{width:310px;right:0}.sidepanel_wide{width:480px;right:0}.sidepanel_extra_wide{width:600px;right:0}.sidepanel_wide input[type="text"],.sidepanel_wide textarea{width:360px}.sidepanel_wide textarea{padding-bottom:20px}.sidepanel-arrow{width:30px;min-height:200px;height:100%;float:left;position:relative}.sidepanel-info,.sidepanel-info-post-question,.sidepanel-info-firstrun,.sidepanel-info-status,.sidepanel-info-retry,.sidepanel-w

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\MasterStyles15MVC[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	15742
Entropy (8bit):	5.036748732006646
Encrypted:	false
SSDEEP:	192:VlxxgkrOOIrUC8ZvLtqiZ30EEAizFM62TUOtq/P0DRcjKjRDJgVXH4/HU:Vlx3IIciP1jKjRDJgx3
MD5:	A69F60B0C5E4DA5367E37F82190C6E18
SHA1:	AFB121329EA9B646F950B443044C45D0DA62B630
SHA-256:	BC5A8DFFDB985886C5124B568646CF19E4718720AB8F9DD701B040423C323AF5
SHA-512:	619A98FE3883A667C4CDE33445396EBEF9F93CB02C6042795FEB01E13BD0209B6FFBC98AC9F5F3E813133D861AD72E8E8238D11DA8402B6E271CB0B93E10EEEA
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://prod.msocdn.com/2021.1.28.2/en-US/css/MasterStyles15MVC.css
Preview:	.pl-shell-footer-hide{display:none}.pl-padding-hide{display:none}.mvc-validator>.field-validation-error{border:1px solid red}.adminScoped input[type=submit]{min-width:100px;display:inline-block;margin-right:10px;margin-left:0;margin-top:5px;text-transform:lowercase;vertical-align:baseline;border:1px solid;color:#fff;text-align:center;line-height:normal;font-size:13px;padding:0 0 0 0}.mpl-layout{margin-left:50px;margin-right:50px;line-height:normal}.mpl-layout.gemini{font-family:"SegoeUI-Light-final","Segoe UI Light","Segoe UI",Segoe,Tahoma,Helvetica,Arial,Sans-Serif;-webkit-font-smoothing:antialiased;font-size:16px;line-height:20px}.mpl-layout.gemini *{box-sizing:border-box}.mpl-layout-table{width:100%}.mpl-banner-box.gemini{position:absolute;top:0;padding-top:17px;padding-bottom:17px;padding-left:30px;padding-right:42px}.mpl-banner-box-text.gemini{font-size:36px;line-height:36px}.mpl-banner-box-hidden{display:none}.mpl-header-td{min-width:300px}.mpl-header-td{vertical-align:middle}.mp

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\MasterStyles15[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	93254
Entropy (8bit):	5.5580645228571575
Encrypted:	false
SSDEEP:	1536:EIRhm83ObH7N2nf4u/5CaBzeo5oauC2zvE:EIRhm37NnkeYqC2zvE
MD5:	5A27F456E68893EACD2B447797CCE7F5
SHA1:	5F35E5C6480E5299F8884070C9096260813A8CEE
SHA-256:	F515FD92BC8503C768FD94BFAF6AE7495529069679202629DEAF186F0E1FF4C3
SHA-512:	04C2AE2450E3B15B41D669C278C33A4770C2B6761C69DD70F507348783CBDC64F8AF2FBED5523820F22DAA25FA35BB1E415E5355FC47C2B2DB07BCB172556BE7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://prod.msocdn.com/2021.1.28.2/en-US/css/MasterStyles15.css
Preview:	.adminScoped *{line-break:strict}.o15table,.o15table2{width:100%;margin-bottom:30px;border-collapse:separate;border-spacing:1px}.o15table th,.o15table2 th{font-weight:normal;white-space:nowrap;width:25%;font-size:11px}.o15table th,.o15table td{padding:5px 12px;vertical-align:top;text-align:left}.adminScoped h4{line-height:normal}.adminScoped h5{line-height:normal}.adminScoped h6{line-height:normal}.adminScoped a:hover{text-decoration:underline;cursor:pointer}.adminScoped a[disabled]{color:#666!important}.adminScoped a[disabled]:hover{cursor:default;text-decoration:none}.adminScoped p{margin:1ex 0 1ex 0}.adminScoped img{border-style:none}.adminScoped hr{border:solid 1px #505050;margin:8px 0 8px 0}.DropdownList-disabled,.TextBox-disabled{opacity:.4;filter:alpha(opacity=40)}.adminScoped th{font-weight:normal;text-align:left}.adminScoped select:disabled{color:#c3cdd2;background-color:#fff;border:solid 1px #d5dee2}.adminScoped option{padding-left:10px}.adminScoped option:disabled{color:#c3c

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\O365ThemeDefault[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	7600
Entropy (8bit):	4.755347264022592
Encrypted:	false
SSDEEP:	96:gTJ0Z6QYvW81oyLEfqSorX5Kjb6tk63LA5D287sq5pY+0dnk3P54aaoJ99orOoY0:S0dYjueAynT8js
MD5:	BC6A941A872D57146E13823F6935A7F2
SHA1:	E648D16D68417B81616454539EDD8303E04DBEC7
SHA-256:	D132D49C1C8945F5C43AE470BADF2B6EDCD584297E84E59DD2034FFB7DC863B3
SHA-512:	F9629A3E82E24FC48DEA4C677491235AAB0098CEDF40DB9F98E53CA430B5DD105A2D9F092E007351AFE2BCCCD2A430C9020EDAE55665E3F3517703A3D00CDE71
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://prod.msocdn.com/2021.1.28.2/en-US/css/O365ThemeDefault.css
Preview:	.o365-theme-base,.o365-theme-base input,.o365-theme-base textarea,.o365-theme-base select{background-color:#fff;color:#333;border-color:#666}.o365-theme-base h1,.o365-theme-base h3,.o365-theme-base h4,.o365-theme-base h5,.o365-theme-base h6{color:#333}.o365-theme-base h2{color:#666}.o365-theme-base a{color:#0078d7}.o365-theme-base input:focus,.o365-theme-base input:hover,.o365-theme-base textarea:focus,.o365-theme-base textarea:hover,.o365-theme-base select:hover,.o365-theme-base select:focus{border-color:#2b88d8}.o365-theme-base a[disabled],.o365-theme-base a[disabled]:hover{color:#666!important}.o365-theme-base input[disabled],.o365-theme-base textarea[disabled]{background-color:#f4f4f4;border-color:#eaeaea;color:#a6a6a6}.o365-theme-base input:disabled,.o365-theme-base textarea:disabled{background-color:#f4f4f4;border-color:#eaeaea;color:#a6a6a6}.o365-theme-base input[type=submit]{background-color:#0078d7;border-color:#0078d7}.o365-theme-base .DataTable td,.o365-theme-base .DataTable

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\Prefetch[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	9781
Entropy (8bit):	5.507773835298488
Encrypted:	false
SSDEEP:	96:MJbTEjSpNnMv8iP0IDNyS4xc82euY3U3O3z7WkYBL/V6DcRDJpclHCkEMJYfqrU:+bu0Mki17L/V6De9pclCmJYfqrU
MD5:	A4D2997B99AFF0F6CEB9E170BE636E45
SHA1:	62B38D3C3CCB72FE727CB3647999C25CF6A4DB13
SHA-256:	310B9C25EE954CAE9368B54509807E37EFA74F2711505611BE0B444D6269EA58
SHA-512:	34B835315B85B7176B58A4D8AE51EFEE5908C719F942911BB37F56F1826254BCE17AC7F7B12EC5FC0537989A3BB1230AD16B26A388D2748016A84CBFC5A10048
Malicious:	false
Reputation:	low
Preview:	.<!DOCTYPE html>.<html>.<head>. <meta name="robots" content="noindex">. <script type="text/javascript">. window.O365={CID:"ce397afab595428b9ca8517f94604e18",PID:"Prefetch.aspx",LURL:"https\x3a\x2f\x2fclientlog.portal.office.com\x2fpp.l\x2f"};. </script>. <script type='text/javascript'>var O365;(function(n){n.Perf={},n.Perf.M={S:new Date};var t=!1,i=function(i){var u,f;t||(t=!0,u=n.Perf.M,u[i]=new Date,f=u[i].getTime(),window.setTimeout(function(){var e="",s,l,t,a,v;try{for(s=["L","U","M"],e+="{B:{S:'"+i+"',",t=0;t<s.length;t++)e+=r(s[t],u.S,u[s[t]],t===s.length-1);if(e+="}",window.performance&&performance.timing){var o=window.performance.timing,y=o.fetchStart,p=u.M?u.M.getTime():-1,h=["E","O","D","C","R","S","M","L"],c=o.loadEventStart;for(c&&(f=c),l=[o.redirectStart,o.domainLookupStart,o.domainLookupEnd,o.connectEnd,o.responseStart,o.responseEnd,p,c],e+=",A:{",t=0;t<h.length;t++)e+=r(h[t],y,l[t],t===h.length-1);e+="}"}e+=",C:{LT:"+f+"}}"}catch(w){e+="!E

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\admin[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):	1382145
Entropy (8bit):	5.1968022469302015
Encrypted:	false
SSDEEP:	6144:mZ18TNwHUqPb4QOv3VZ4x8PIQplhDe6RVHc4Rqt/6QYIED7PWMtyJk7eOMT+8EI:/TGPuZ7IWT/6QYR6Mt5eOMT+8u
MD5:	A622AF0C85EF92ADF2C7C2974B4D641E
SHA1:	2A423C3B3CEB6BE98726B262A86B500BF91D7064
SHA-256:	7F6B6E9F6F421073014D14D6822EF38A6922D5A7F24565FA20E0781A71476368
SHA-512:	4A2C405FFF5B8BC34F3FB9C63A069684098EC12FE94F29C5B8B9795F2C7E9DEB9EC095746563E9BAE7D15424FFD7B756155CEA1F5D89DAB6D9BD4886751062
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://prod.msocdn.com/2021.1.28.2/en-US/admin/css/admin.css
Preview:	.fake{color:red}.k-reset{margin:0;padding:0;border:0;outline:0;text-decoration:none;font-size:100%;list-style:none}.k-floatwrap:after,.k-slider-items:after,.k-grid-toolbar:after{content:"";display:block;clear:both;visibility:hidden;height:0;overflow:hidden}.k-floatwrap,.k-slider-items,.k-grid-toolbar{display:inline-block}.k-floatwrap,.k-slider-items,.k-grid-toolbar{display:block}.k-block,.k-button,.k-header,.k-grid-header,.k-toolbar,.k-grouping-header,.k-tooltip,.k-pager-wrap,.k-tabstrip-items .k-item,.k-link.k-state-hover,.k-textbox,.k-textbox:hover,.k-autocomplete,.k-dropdown-wrap,.k-picker-wrap,.k-numeric-wrap,.k-autocomplete.k-state-hover,.k-dropdown-wrap.k-state-hover,.k-picker-wrap.k-state-hover,.k-numeric-wrap.k-state-hover,.k-draghandle{background-repeat:repeat;background-position:0 center}.k-link:hover{text-decoration:none}.k-state-highlight>.k-link{color:inherit}.k-textbox>input,.k-input[type="text"],.k-input[type="number"],.k-textbox,.k-picker-wrap .k-input,.k-button{font-si

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\app[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF, LF line terminators
Category:	downloaded
Size (bytes):	262641
Entropy (8bit):	4.9463902181496096
Encrypted:	false
SSDEEP:	3072:u+Vd0pBbqPLYoyjFkxD2hAYwJb8ILm731Ss:u+Vd0DePLYoyjFkxD2hAYwJbZLM31Ss
MD5:	7C593B06759DB6D01614729D206738D6
SHA1:	0D4F76D10944933B8DDECFFE9691081439A77A3C
SHA-256:	F7D9FB0479DE843CF3FB0B78FC56BBB9E30BF0A238C6F79D9209FA8B22EFB574
SHA-512:	EF91B610CF17A17AAFB48984B4403EF175EB86096E3F12E23AE8D4C7C96EF60ED14DA3F69721E095CD2ACE3F0A06190186D000992823814BB906F7FB3576C2C1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.onestore.ms/cdnfiles/external/oneui/oneui1.16.2/dist/css/app.css
Preview:	@font-face {. font-family: "wf_segoe-ui_normal";. src: url("//i.s-microsoft.com/fonts/segoe-ui/west-european/normal/latest.eot");. src: url("//i.s-microsoft.com/fonts/segoe-ui/west-european/normal/latest.eot?#iefix") format("embedded-opentype"), url("//i.s-microsoft.com/fonts/segoe-ui/west-european/normal/latest.woff") format("woff"), url("//i.s-microsoft.com/fonts/segoe-ui/west-european/normal/latest.ttf") format("truetype"), url("//i.s-microsoft.com/fonts/segoe-ui/west-european/normal/latest.svg#web") format("svg");. font-weight: normal;. font-style: normal; }..@font-face {. font-family: "wf_segoe-ui_light";. src: url("//i.s-microsoft.com/fonts/segoe-ui/west-european/light/latest.eot");. src: url("//i.s-microsoft.com/fonts/segoe-ui/west-european/light/latest.eot?#iefix") format("embedded-opentype"), url("//i.s-microsoft.com/fonts/segoe-ui/west-european/light/latest.woff") format("woff"), url("//i.s-microsoft.com/fonts/segoe-ui/west-european/light/latest.ttf") format("truetype

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\conciergehelper[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	5200
Entropy (8bit):	5.00329299691644
Encrypted:	false
SSDEEP:	96:l5L28mnjvnjtnEnkqVEtVgGMVTO7j6yBnlcL6zitcTzDk:l5LjmDZE2gGwOv6yBnW6fA
MD5:	54599D7C2AC4C08C1B52A1BF953B2080
SHA1:	C15251DF5BCEA1B665E401B5C73935157CB5B361
SHA-256:	E3DD3D2EB577E0976C6C3BB2A597839A4B50019E6F34767D692B371AA6A87DD7
SHA-512:	107669750D308F1E2FEB2F739A749350ACCDF0998AD113F2B437EA6577EDEAECFC1190AB3FA3E9EDBD51B0F1F9F9DB0E3AF3031D231C8F67A4AE260A7011A3C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://prod.msocdn.com/2021.1.28.2/en-US/css/conciergehelper.css
Preview:	.freelance-panel-flow{margin-top:30px;width:320px;border-width:1px;border-style:solid;border-radius:5px;top:50px}.freelance-panel-home{margin-top:30px;width:320px;border-width:1px;border-style:solid;border-radius:5px;position:fixed!important;postion:absolute;bottom:30px;top:50px}.freelance-panel-docked{margin-top:30px;width:320px;border-width:1px;border-style:solid;position:fixed;bottom:0;right:30px;border-top-left-radius:5px;border-top-right-radius:5px;background-color:#fff;z-index:100}.freelance-panel-docked-noBorder{margin-top:30px;width:320px;border-width:0;border-style:solid;position:fixed;bottom:0;right:30px;border-top-left-radius:5px;border-top-right-radius:5px;background-color:#fff;z-index:10000}.freelance-panel-docked-shellHome{margin-top:30px;margin-left:20px;width:320px;border-width:1px;border-style:solid;position:fixed;bottom:0;left:30px;border-top-left-radius:5px;border-top-right-radius:5px;background-color:#fff}.freelance-panel-docked-shellHome-noBorder{margin-top:30px;ma

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\converged_ux_v2_RfnRCrmapm3W_OFn994CMA2[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	95459
Entropy (8bit):	5.292153801820765
Encrypted:	false
SSDEEP:	1536:QpHDIqBBw+T6azA/PWrF7qvEAFiQcpmKboBdiyMUWC8ErpH/TVTDrwCGNJZ3yU0P:IBFNyUM
MD5:	45F9D10AB99AA66DD6FCE167F7DE0230
SHA1:	D443993E7ADB3108167BCD94E5D3126A2E3EE7EE
SHA-256:	D72952FC8950D26C08C6BAD73D389C35D0EAF164CB73503183A2966DEFAAD991
SHA-512:	0DBCCCB37A3A249C7DBB948AC756FD332298DD8A742E92DF6A767FD565C925768058C05AF182106F8DA29979C0D23BD3E9ECE9E41C1EA931F4F198CBDCE8B3F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://acctcdn.msauth.net/converged_ux_v2_RfnRCrmapm3W_OFn994CMA2.css?v=1
Preview:	/*! Copyright (C) Microsoft Corporation. All rights reserved. *//*!---------- START OF THIRD PARTY NOTICE ----------..This file based on or incorporates material from the projects listed below (Third Party IP). The original copyright notice and the license under which Microsoft received such Third Party IP, are set forth below. Such licenses and notices are provided for informational purposes only. Microsoft licenses the Third Party IP to you under the licensing terms for the Microsoft product. Microsoft reserves all other rights not expressly granted under this agreement, whether by implication, estoppel or otherwise. ..//----------.twbs-bootstrap-sass (3.3.0).//----------..The MIT License (MIT)..Copyright (c) 2013 Twitter, Inc..Permission is hereby granted, free of charge, to any perso

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
Reputation:	low
IE Cache URL:	http://https://signup.live.com/Resources/images/favicon.ico
Preview:	.............h(..f...HH...........(..00......h....6.. ....=..............@..........(....A..(...................(....................................."P..."""""""""""""""""""""""""""""""""""" ...3 3333333333333333333333333333"""""""""""""""""""""""""""""""""" ...3333333333333333333333333333"""""""""""""""""""""""""""""""""" ...3333333333333333333333333333"""" """""""""""""""""""""""""""""" ...3333333333333333333333333333"""""""""""""""""""""""""""""""""" ...3333333333333333333333333333"""""""""""""""""""""""""""""""""" ...3333333333 333333333333333333"""""""""""""""""""""""""""""""""" ...3333333333333333333333333333"""""""""""""""""""""""""""""""""" ...3333333333333333333333333333"""""""""""""""""""""""""""" """""""" ...3333333333333333333333333333"""""""""""""""""""""""""""""""""" ...3333333333333333333333333333"""""""""""""""""""""""""""""""""" ...3333333333333333333 333333333"""""""""""""""""""""""""""""""""" ...3333333333333333333333333333""""""""""""""""""""""""""""""

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\favicon[2].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 6 icons, 128x128, 16 colors, 72x72, 16 colors
Category:	downloaded
Size (bytes):	17174
Entropy (8bit):	2.9129715116732746
Encrypted:	false
SSDEEP:	24:QSNTmTFxg4lyyyyyyyyyyyyyio7eeeeeeeeekzgsLsLsLsLsLsQZp:nfgyyyyyyyyyyyyynzQQQQQO
MD5:	12E3DAC858061D088023B2BD48E2FA96
SHA1:	E08CE1A144ECEAE0C3C2EA7A9D6FBC5658F24CE5
SHA-256:	90CDAF487716184E4034000935C605D1633926D348116D198F355A98B8C6CD21
SHA-512:	C5030C55A855E7A9E20E22F4C70BF1E0F3C558A9B7D501CFAB6992AC2656AE5E41B050CCAC541EFA55F9603E0D349B247EB4912EE169D44044271789C719CD0
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://account.live.com/Resources/images/favicon.ico
Preview:	.............h(..f...HH...........(..00......h....6.. ....=..............@..........(....A..(...................(....................................."P..."""""""""""""""""""""""""""""""""""" ...3 3333333333333333333333333333"""""""""""""""""""""""""""""""""" ...3333333333333333333333333333"""""""""""""""""""""""""""""""""" ...3333333333333333333333333333"""" """""""""""""""""""""""""""""" ...3333333333333333333333333333"""""""""""""""""""""""""""""""""" ...3333333333333333333333333333"""""""""""""""""""""""""""""""""" ...3333333333 333333333333333333"""""""""""""""""""""""""""""""""" ...3333333333333333333333333333"""""""""""""""""""""""""""""""""" ...3333333333333333333333333333"""""""""""""""""""""""""""" """""""" ...3333333333333333333333333333"""""""""""""""""""""""""""""""""" ...3333333333333333333333333333"""""""""""""""""""""""""""""""""" ...3333333333333333333 333333333"""""""""""""""""""""""""""""""""" ...3333333333333333333333333333""""""""""""""""""""""""""""""

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\home15[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	1723
Entropy (8bit):	5.133944657348725
Encrypted:	false
SSDEEP:	24:72pY29zhE6Ayu21CrXlqYC8hEvjzMr33lyfaS4KnQaq8Nuh2a:m9EraDYC8hEvjz0nlyfaS4eQaq8Nuh2a
MD5:	E2465EDA10BB4EF428723F3D9AA59E7D
SHA1:	D1B8639FDB47321A9730840FC55F3D6719B291DC
SHA-256:	D9CF25F06485765D98CD21B392729518E43B994252E41F11DBA6DCB777D6F580
SHA-512:	C646A57F76F369F581896D35D7EDE17D967900F2D75D9FFC2A680C8EB77017909198C729D3DFE4143EF5F8C8BCF6B23F6B17350D5C701FFF76C5C3CE201F5AD
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://prod.msocdn.com/2021.1.28.2/en-US/css/home15.css
Preview:	.HomeMainHeader{font-family:"Segoe UI Light","Segoe UI",Segoe,Tahoma,Helvetica,Arial,Sans-Serif,SegoeUI-Light-final;font-size:48px;line-height:normal;letter-spa cing:normal;margin-top:60px}.HomeSubHeader{font-family:"Segoe UI Light","Segoe UI",Segoe,Tahoma,Helvetica,Arial,Sans-Serif,SegoeUI-Light-final;font-size:22px;line- height:normal;letter-spacing:normal;margin-top:6px}#DivIsLicensed,#AdminTasks{margin-bottom:50px}#AdminTasks{margin-top:50px}.AdminTasks A{color:#0072c6;font- family:"Segoe UI Light","Segoe UI",Segoe,Tahoma,Helvetica,Arial,Sans-Serif,SegoeUI-Light-final;font-size:18px;line-height:normal;letter-spacing:normal;display:inline-blo ck;margin-bottom:9px}Div.ProfessionalTilePage{min-width:1000px}.ProfessionalTilePage td{padding:0}Div.LinkHeader{margin-bottom:30px;margin-top:5px}.AdminStart-O uterDiv{height:415px;margin-top:2px;overflow:hidden;min-width:1200px}.AdminStart-InnerDiv{height:330px;left:10px;position:relative;top:58px;width:1200px}.AdminStart- InnerDiv h1.BOX-HeaderSup

Copyright null 2021

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\home[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	4254
Entropy (8bit):	5.163271433365275
Encrypted:	false
SSDEEP:	96:+r2ZPOc0PHpSHrhwelTSjgjfIND428194:+MGHpSLh/l5fE4R4
MD5:	62E59A034C97AB0ACE0DAFBDE33F2D4F
SHA1:	8B9424DF77D6A6176A0D40BF13182CCCF9274FF9
SHA-256:	186F50FAA1743EF888F3762B5A2D7164C6094AB8807CDA66B3435F9C9582C8B8
SHA-512:	3DB5CF84F0C8004DC8BE72A1DDEFD00323F14F0779FDFFDD32FC08540F02A1C3216E9ABD3ECCBA63EFDAB7328207D0809F36835FE5C62EA701351DD563F5FE FA
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://prod.msocdn.com/2021.1.28.2/en-US/css/home.css
Preview:	.Home-Content-Container{max-width:625px}.Home-RightColumn-Bottom{height:30px}.Administrator-Control-RowValue{padding-left:10px}.Home-SearchControl-Container{width:100%;padding-top:4px;padding-bottom:26px}.Page-Modern .Home-SearchControl-Container{width:200px;padding-bottom:30px}.Home-SearchControl-Table{border:1px solid #c6dff3;background-color:#fff}.Page-Modern .Home-SearchControl-Table{border:1px solid;background-color:transparent;min-width:200px;min-height:24px}.Home-SearchControl-Table input[type="image"]{vertical-align:middle}.Page-Modern .Home-SearchControl-Table>tbody>tr>td>span{margin-right:8px}.Home-SearchControl-Table input[type="text"]{margin:0;padding-top:0;float:left;height:18px;vertical-align:middle;border:solid 0 red;padding-bottom:3px;padding-top:3px;padding-left:4px;color:#aaa;width:100%}.Page-Modern .Home-SearchControl-Table input[type="text"]{padding-left:8px}.Home-SearchControl-Container input[type="text"]:focus{color:#43515b}#AdminHomeContentPanels>div{margin-botto

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\jquery-1.7.2.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	94840
Entropy (8bit):	5.372946098601679
Encrypted:	false
SSDEEP:	1536:8YRKUfAjtledhTmtaFyQHGvCXsedOgRc9izzr4yff8teLvHHEjam7W5X3yzSiLnM:VUb6GvCu09s2o2skAieW
MD5:	B8D64D0BC142B3F670CC0611B0AEBCAE
SHA1:	ABCD2BA13348F178B17141B445BC99F1917D47AF
SHA-256:	47B68DCE8CB6805AD5B3EA4D27AF92A241F4E29A5C12A274C852E4346A0500B4
SHA-512:	A684ABBE37E8047C55C394366B012CC9AE5D682D29D340BC48A37BE1A549AECED72DE6408BEDFED776A14611E6F3374015B236FBF49422B2982EF18125FF47DC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ajax.aspnetcdn.com/ajax/jQuery/jquery-1.7.2.min.js
Preview:	/*! jQuery v1.7.2 jquery.com | jquery.org/license */.(function(a,b){function cy(a){return f.isWindow(a)?a:a.nodeType===9?a.defaultView||a.parentWindow:!1}function cu(a){if(!cj[a]){var b=c.body,d=f("<"+a+">").appendTo(b),e=d.css("display");d.remove();if(e==="none"||e===""){ck||(ck=c.createElement("iframe"),ck.frameBorder=ck.width=ck.height=0),b.appendChild(ck);if(!cl||!ck.createElement)cl=(ck.contentWindow||ck.contentDocument).document,cl.write((f.support.boxModel?"<!doctype html>":"")+"<html><body>"),cl.close();d=cl.createElement(a),cl.body.appendChild(d),e=f.css(d,"display"),b.removeChild(ck)}cj[a]=e}return cj[a]}function ct(a,b){var c={};f.each(cp.concat.apply([],cp.slice(0,b)),function(){c[this]=a});return c}function cs(){cq=b}function cr(){setTimeout(cs,0);return cq=f.now()}function ci(){try{return new a.ActiveXObject("Microsoft.XMLHTTP")}catch(b){}}function ch(){try{return new a.XMLHttpRequest}catch(b){}}function cb(a,c){a.dataFilter&&(c=a.dataFilter(c,a.dataType));var d=a.dataTyp

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\jquerypackage_1.10_5V7LAuc3bNAQx2QQfr1RPw2[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):	96649
Entropy (8bit):	5.297804550899051
Encrypted:	false
SSDEEP:	1536:G+6LPOpumEEni7iU2e25CxgjDb60nkN8h1utK0Dv+9G1LDrjsNyw5yn/dFZ75Tym:xH7pDuVUNB0lmEGWf
MD5:	E55ECB02E7376CD010C764107EBD513F
SHA1:	FA6D184DF01EC535628DC8FAF38211591BAADFC8
SHA-256:	5776881753B95A0ABE5D1F6EFE3ABE7B83A3265EACCD117DD948E523C044600C
SHA-512:	099C665E1CEE8DF9C5D5C340A14170341BD29E0321875FF08E594B750CFDBF2CA8C9B45B584FCA21F87CBE6CD8A170918CECFF8C9796AAFA3D89F0AA97509ABD
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://acctcdn.msauth.net/jquerypackage_1.10_5V7LAuc3bNAQx2QQfr1RPw2.js?v=1

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\jquerypackage_1.10_5V7LAuc3bNAQx2QQfr1RPw2[1].js	
Preview:	/*!. * jQuery JavaScript Library v1.10.2. * http://jquery.com/. *. * Includes Sizzle.js. * http://sizzlejs.com/. *. * Copyright 2005, 2013 jQuery Foundation, Inc. and other contrib utors. * Released under the MIT license. * http://jquery.org/license. *. * Date: 2013-07-03T13:48Z. */.!function(e,t){function n(e){var t=e.length,n=ct.type(e);return ct. isWindow(e)?!1:1===e.nodeType&&t?!0:"array"===n||"function"!==n&&(0===t||"number"==typeof t&&t>0&&t-1 in e)}function r(e){var t=kt[e]={};return ct.each(e.match(pt)|| [],function(e,n){t[n]=!0}),t}function i(e,n,r,i){if(ct.acceptData(e)){var o,a,s=ct.expando,u=e.nodeType,l=u?ct.cache:e,c=u?e[s]:e[s]&&s;if(c&&l[c]&&(i||l[c].data)||r!==t||"str ing"!=typeof n){return c||(c=u?e[s]=tt.pop()||ct.guid++:s),l[c]||(l[c]=u?{}:{"toJSON":ct.noop}),("object"==typeof n||"function"==typeof n)&&(i?l[c]=ct.extend(l[c],n):l[c].data=ct.e xtend(l[c].data,n)),a=l[c],i||(a.data||(a.data={}),a=a.data),r!==t&&(a[ct.camelCase(n)]=r),"string"==typeof n?(o=a[n],null==o&&(o=

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\knockout_3.3.0_X1BYS2jZMbi7hfUj8VuqFA2[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):	80144
Entropy (8bit):	5.421376219099593
Encrypted:	false
SSDEEP:	1536:vZ2N4/PzS0zdqm4NVmVtfB6aTJDIO5XxV7FyTDQIp8a+fNNnbt:Ay+0LmmBt7c1+Rfbt
MD5:	5F50584B68D931B8BB85F523F15BAA14
SHA1:	FAF4BD348F40016BCE0ABF54F167C7923B303ABB
SHA-256:	3C829DCF48768082A6177B77AE4E499337ED4C8BD056705CDB1E979F7B6EFCE5
SHA-512:	EB01573B9152D93400C7BCDC0C3746B58E8F5F8BA7A4C033D3A30D688E307543979402CAD4A19249391BA3113466F562D20A521BBEFFB7864AEBEB18FDB79BC 1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://acctcdn.msauth.net/knockout_3.3.0_X1BYS2jZMbi7hfUj8VuqFA2.js?v=1
Preview:	/*!---------- START OF THIRD PARTY NOTICE ----------....This file is based on or incorporates material from the projects liste below (Third Party IP). The original copyright notice and the license under which Microsoft received such Third Party IP, are set forth below. Such licenses and notices are provided for informational purposes only. Microsoft licenses the Third Party IP to you under the licensing terms for the Microsoft product. Microsoft reserves all other rights not expressly granted under this agreement, whether by implication, estoppel or otherwise. .... * Knockout JavaScript library v3.3.0.. * (c) Steven Sanderson - http://kn ockoutjs.com/.. * License: MIT (http://www.opensource.org/licenses/mit-license.php)....Provided for Informational Purposes Only....MIT License ....Permission is hereby gr anted, free of charge, to any person obtaining a copy of this software and associated documentation files (the Software)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\latest[1].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), Segoe UI Light family
Category:	downloaded
Size (bytes):	28315
Entropy (8bit):	7.9724193003797
Encrypted:	false
SSDEEP:	384:+R0Z7+bHAtrQ1yBFbgqLct7rJhhPLLkHsrvSzaJu4mI3n5o+MmKCxDg6iT7jdVye:+uNUAtE3phPLLFTiMu+pxCjHyGEQ9zL
MD5:	17DFE73CB9C64527F7248B0A24DB317D
SHA1:	345198B9239FCDAF038FB2D3A919E4724037DBAA
SHA-256:	AD75FB92B2EBCE6C37640F03E1AB96A752F388BCE60C877ADE4780B13839E8C4
SHA-512:	421B56D93E9BD5E4B4449DD0FCDEE8D531087FD484C91530AAF0A67EDEA33D5AC2F14A7F4966C528C0F130F17F26629FCAB9F8AB47E950CEB5B9F1A827EA07 28
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://i.s-microsoft.com/fonts/segoe-ui/west-european/light/latest.eot?
Preview:	.n...m.....LP#...B..... .....S.e.g.o.e. .U.l. .L.i.g.h.t.....R.e.g.u.l.a.r.....V.e.r.s.i.o.n. .5...3.2.....S.e.g.o.e. .U.l. .L.i.g.h.t.....K..e..66.....U.D.-.. iu...4P\..GLFM..C?.;..-...~|...P..\.(..)RI.....>.>..CE..SsV.jPR...H.....].R..&.n.hT.....x.....q .....wA[....F.....c."....Zed..>.?...`..3...B..W....R....F.j....v..'?.5.k^.....+..a...).. _].x.#QSi.....|<t....k.;..Hv1.G...L$.9....5.t.:...V.Y.....\|.@....B.....P`..2.Z.0....2`.FR.MF8.x....GP0..$:.....PYm.22..."S."1.*j[=.=.mR.*.....j....&.4...k..].1@..y$....."y..C..g7..k.B*. ..V..F\...G.m.jK ...O....b.Qlo...!.N.V....t.[..p.N..~@1d...YX.."....R_i.4.$j.P..U....u9...<..6..4%.....9`.....S...N.Y..L..B$2\.E.vhe...n..h..5..Z..K?.H..S...2..=R..x.....EX.2.....$."..... It8..z.+.h ..$.2*T....}Z../....p..b0ae.qq.(-v1..E.!.l".a..p.).:,.8t..7..^..W...4A.D\eOb$.....b.NI.Pe.#$.O38....,....g..&|...B{...].....9..u.8..~Y...3.X..ff.,.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\latest[2].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), Segoe UI family
Category:	downloaded
Size (bytes):	35047
Entropy (8bit):	7.975792390307888
Encrypted:	false
SSDEEP:	768:l6ibzTDpOGuAJ63YB9eSzDtQEspfAzyNyuBmOfAJYCM:/iPMYJ4GEAZoTyglcM
MD5:	CAD76E4816AF6890C9BFD02A6D1EA899
SHA1:	9EDC91541C31034FCE0D83AABBAAD4C314CD3D33
SHA-256:	D5794223D1A062E5DBE6C34C1994C8CE3792B24AFD5218D0644CB1F53DA4BE58
SHA-512:	24983A5856C2B4D8CBE2A4BD233A93B266A03D4218942E1D1733B33B65AB7A504AF0AC31DE2F1E69F6FF8CCD7A169CD4555539D34FFF8DE4CB8C98DB2DB2C 63
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\latest[2].eot	
IE Cache URL:	http://https://i.s-microsoft.com/fonts/segoe-ui/west-european/normal/latest.eot?
Preview:	...=.....LP#...B..... .....S.e.g.o.e. .U.I.....R.e.g.u.l.a.r.....V.e.r.s.i.o.n. .5...3.2.....S.e.g.o.e. .U.I.....RV.z..;~.....U.D.-..iu...N4P\..GLFM .Y.?.;..-...~~....Ox.M..".$..._.....g..sC*2..4W.....9AGc.[a..*.rCl,..@..U_..L...e..Ru.J.-.f..3.....S`.A.....K<;...n.Y...rli.....([...W...5k.....^K.G...U.@....2H..B.)N0w.....C..9..... ....#.l2,4..6y.3$b....K.wx...I.$E..?3.8.c...,x..t.wa.O....4.c...!..+.<EM...2T.>\..]4.A.H.;..G.....W.:.?...Z".....e....8....84.L,.)0..y.Xdd.Pa.@.&.o(.I.q.yF...[.y.m(D...(....T.....,A.;q.... .w.$..C..a.. .Y.O?{..0...'1.;C.,.....W..Q-..'.5tD@9..U...E4e.&_...S.Y...\)b.s.rIR.....%..R..KU O..{.0(.....^Q\^!.et...Kf%..K...}.1...S.{.....3p..]...|Y...w..|JeS$..k.....>(8 .ZlV..N.). c...Z.K.\..q....'S.j.....9...._..E.#s*'#.....[.....DJ^.L7../1...+U.qG.....-...MM..q....L..c...^...:e....<h...:..`.jz..fb.Ha.....k.....e\)g..\."..M

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\latest[3].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), Segoe UI Semibold family
Category:	downloaded
Size (bytes):	30643
Entropy (8bit):	7.976822258863597
Encrypted:	false
SSDEEP:	768:UOtV1asJ9G0dAdnVrKX/HkVJRPvkgxYZ4Zoe:bLasJ9G0u0fk/RnkgxGof
MD5:	E812BA8B7E2A657F2B70CFACE93C7682
SHA1:	2F02CDDBB483F9B11BBBE74C3CA917A4C345FBAD
SHA-256:	3330C1DEAC468874238DD0C6BF902179A8731EDA8A208C7D01DAC0AB1EAE1BC9
SHA-512:	354B2DB12BC1D67F26F94352B0B663DAD64C46C107454FC19CFEA01C54BB09340BC26C06DE1B96FF826F5287CE246A6317722BAE41B72B63BA86FDAF844BA94 E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://i.s-microsoft.com/fonts/segoe-ui/west-european/semibold/latest.eot?
Preview:	.w...v.....X.....LP#...B..... .....".S.e.g.o.e. .U.I. .S.e.m.i.b.o.l.d.....R.e.g.u.l.a.r.....V.e.r.s.i.o.n. .5...3.2...".S.e.g.o.e. .U.I. .S.e.m.i.b.o.l.d.....H .P..lb.7^.....U.D.-..iu...:4P\..GLFM.Y.#?.;..-...~}_).z{.rmD.1".$.....{.t.....=...!cK...%.~.....g.....j.9S....6. ..n..V.]pz...e.....#X...=,.p.F..6&.VR...k$~J..n....7.....K.8..T.....x..J.....#.J .XaQ.Q%_{3..xr.... 0Dm...k..Ep.....>..?Pk!KB..C...Q.q..1=6<,.S.F.&B..J.....ya2b."S.....6.2.....H.....*..09A...Tb/.&.d..#.E.:.E.(..I5.M..444d.1.....K..I...I.O..VBb....:..:b..Mh.'= 4.d/..o.k.mMm.....bx..!..S.@E.....>@:..k.JCas..7."..uG3hR.h..w..8W>.4.....pX....J..a....}.Y.....(>H^=.`=.mg*.!.....w'...J.<.ob..3A .../.....5%.'....XS0a.....I.Ia....a...=..g..... {V1+.."_)7$2 O..!bb.=..|.s.1..2qm..#.O.....+E(I..1....EgQ.....E)R.m.?.8.q...J.G.@!f..n.F.r#..(..2p.?.9.8..?.d]..s..0.9.f..A...r.iq....x.g.aO....S.....R0i..BT.yl.".<k...:&Ja.\.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\microsoft_logo_7lyNn7YkjJOP0NwZNw6QvQ2[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	3651
Entropy (8bit):	4.094801914706141
Encrypted:	false
SSDEEP:	96:wO4DZ+Stb/jY+eo4hAryAes9mBYYQgWLDm9:wToSBjlevudl9nO
MD5:	EE5C8D9FB6248C938FD0DC19370E90BD
SHA1:	D01A22720918B781338B5BBF9202B241A5F99EE4
SHA-256:	04D29248EE3A13A074518C93A18D6EFC491BF1F298F9B87FC989A6AE4B9FAD7A
SHA-512:	C77215B729D0E60C97F075998E88775CD0F813B4D094DC2FDD13E5711D16F4E5993D4521D0FBD5BF7150B0DBE253D88B1B1FF60901F053113C5D7C1919852D58
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://acctcdn.msauth.net/images/microsoft_logo_7lyNn7YkjJOP0NwZNw6QvQ2.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="108" height="24" viewBox="0 0 108 24"><title>assets</title><path d="M44.836,4.6V18.4h-2.4V7.583H42.4L38 .119,18.4H36.531L32.142,7.583h-.029V18.4H29.9V4.6h3.436L37.3,14.83h.058L41.545,4.6Zm2,1.049a1.268,1.268,0,0,1,.419-.967,1.413,1.413,0,0,1,1-.39,1.392, 1.392,0,0,1,1.02.4,1.3,1.3,0,0,1,.4.958,1.248,1.248,0,0,1-.414.953,1.428,1.428,0,0,1-1.01.385A1.4,1.4,0,0,1,47.25,6.6a1.261,1.261,0,0,1-.409-.948M49.41,18.4H47. 081V8.507H49.41Zm7.064-1.694a3.213,3.213,0,0,0,1.145-.241,4.811,4.811,0,0,0,1.155-.635V18a4.665,4.665,0,0,1-1.266.481,6.886,6.886,0,0,1-1.554.164,4.707,4.707,0, 0,1-4.918-4.908,5.641,5.641,0,0,1,1.4-3.932,5.055,5.055,0,0,1,3.955-1.545,5.414,5.414,0,0,1,1.324.168,4.431,4.431,0,0,1,1.063.39v2.233a4.763,4.763,0,0,0-1.1-.61 1,3.184,3.184,0,0,0-1.15-.217,2.919,2.919,0,0,0-2.223.9,3.37,3.37,0,0,0-.847,2.416,3.216,3.216,0,0,0,.813,2.338,2.936,2.936,0,0,0,2.209.837M65.4,8.343a2.952,2.9 52,0,0,1,.5.039,2.1,2.1,0,0,1,.375.1v2.358a2.04,2.04,0,0,0-.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\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
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\mwfmdl2-v3.54[1].woff	
IE Cache URL:	http://https://www.microsoft.com/mwf/_h/v3.54/mwf.app/fonts/mwfmdl2-v3.54.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\override[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):	1531
Entropy (8bit):	4.797455242405607
Encrypted:	false
SSDEEP:	24:Udf0F+MOu2UOqD3426TKgR2Yyk9696TkMYqdfskeEkeGk/ksuF9qaSm9qags:Ud8FYqTj36TKgR2Yyk9696TkMYO0keEW
MD5:	A570448F8E33150F5737B9A57B6D889A
SHA1:	860949A95B7598B394AA255FE06F530C3DA24E4E
SHA-256:	0BD288D5397A69EAD391875B422BF2CBDCC4F795D64AA2F780AFF45768D78248
SHA-512:	217F971A8012DE8FE170B4A20821A52FA198447FA582B82CF221F4D73E902C7E3AA1022CB0B209B6679C2EAE0F10469A149F510A6C2132C987F46214B1E2BBBC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://statics-marketingsites-eus-ms-com.akamaized.net/statics/override.css?c=7
Preview:	a.c-call-to-action:hover, button.c-call-to-action:hover{box-shadow:none!important}a.c-call-to-action:hover span, button.c-call-to-action:hover span{left:0!important}...c-call-to-action:not(.glyph-play):after { right: 0!important;} a.c-call-to-action:focus,button.c-call-to-action:focus{box-shadow:none!important}a.c-call-to-action:focus span,button.c-call-to-action:focus span{left:0!important;box-shadow:none!important}...theme-dark .c-me .msame_Header_name {color: #f2f2f2;}...pmg-page-wrapper .uhf div, .pmg-page-wrapper .uhf button, .pmg-page-wrapper .uhf a, .pmg-page-wrapper .uhf span, .pmg-page-wrapper .uhf p, .pmg-page-wrapper .uhf input {font-family: Segoe UI, SegoeUI,Helvetica Neue,Helvetica,Arial,sans-serif !important;}..@media (min-width: 540px) {.pmg-page-wrapper .uhf .c-uhfh-alert span, .pmg-page-wrapper .uhf #uhf-g-nav span, .pmg-page-wrapper .uhf .c-uhfh-actions span, .pmg-page-wrapper .uhf li, .pmg-page-wrapper .uhf button, .pmg-page-wrapper .uhf a, .pmg-page-wrapper .uhf #meC

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\servicesagreement[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	209815
Entropy (8bit):	5.164705570714912
Encrypted:	false
SSDEEP:	6144:GMhZaZEzF0a6OGYL0seowg6ehsymCJ2i/T9VTSfaTHgJi7eshMcgGJ3AQ:GOZaZEzX6OGYQseowg6ehsymCJ2i/pV7
MD5:	59386D83AD18E52D7D50EDA49C1B3D69
SHA1:	9E77E95F6052D117515999F2A79269DEC24CDC47
SHA-256:	123D97CB530F6693F8AF1513A6CB7F8D188D862A2C879103B9ED63BA5C9F790B
SHA-512:	F281CE64E60C4B6ED2C51F73746D3DA56BDD2B827D5B4E5A42A72F860E06406B67D5FCEB6F93C273A412D27B53A2CB0E08EB3E570DBD0E426387654A9211F3 7
Malicious:	false
Reputation:	low
Preview:	.<!DOCTYPE html ><html xmlns:mscom="http://schemas.microsoft.com/CMSvNext" xmlns:md="http://schemas.microsoft.com/mscom-data" lang="en-us" xmlns="http ://www.w3.org/1999/xhtml"><head><meta name="viewport" content="initial-scale=1.0, width=device-width" /><meta http-equiv="X-UA-Compatible" content="IE=edge" /><title>Microsoft Services Agreement</title><meta name="Title" content="Microsoft Services Agreement" /><meta name="CorrelationVector" content="X1Am9GXg dUeBHm/g.1" /><meta name="Description" content="" /><meta name="MscomContentLocale" content="en-us" /><link href="https://www.microsoft.com/onerfstatics/marketingsites-eus-prod/west-european/shell/_scrf/css/themes=default.device=uplevel_web_pc/c2-fe9af7/b9-ae4fa3/fe-321a68/42-1cb85f/3e-dcc204/a1-352ee3/fa-ea79ed/54-41a2a0?ver=2.0" rel="stylesheet" type="text/css" media="screen" /><link href="https://statics-marketingsites-eus-ms-com.akamaized.net/statics/override.css?c=7" rel ="stylesheet" type="text/css" media="screen" /><link rel="

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\shell.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	82190
Entropy (8bit):	5.036904170769404
Encrypted:	false
SSDEEP:	1536:tJzwN0CbUTqI34/9w6/Qua+1IGEbjBko230WBYT:vyA
MD5:	1F9995AB937AC429A73364B4390FF6E8
SHA1:	81998DCC6407CEB5CEF236AD52B9F2A3A9528D3B
SHA-256:	49E5166F40D8586714F86E08AB76A977199DF979357147A0E81980A804151C2A
SHA-512:	6669AE352FF46DB734BB8F973D1C0527C3A5EC4119D534AAE4C33F29EFF970168ED5FE200A05D4E1B6A2EC0E090E2207549B926317D489DC7664B0D9C208546
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\shell.min[1].css	
Reputation:	low
IE Cache URL:	http://https://assets.onestore.ms/cdnfiles/onestorerolling-1510-19009/shell/v3/scss/shell.min.css
Preview:	@charset "UTF-8";@font-face{font-family:'wf_segoe-ui_normal';src:local("Segoe UI");src:url("//i.s-microsoft.com/fonts/segoe-ui/west-european/normal/latest.eot");src:url("//i.s-microsoft.com/fonts/segoe-ui/west-european/normal/latest.eot?#iefix") format("embedded-opentype"),url("//i.s-microsoft.com/fonts/segoe-ui/west-european/normal/latest.woff") format("woff"),url("//i.s-microsoft.com/fonts/segoe-ui/west-european/normal/latest.ttf") format("truetype"),url("//i.s-microsoft.com/fonts/segoe-ui/west-european/normal/latest.svg#web") format("svg");font-weight:normal;font-style:normal}@font-face{font-family:'wf_segoe-ui_semilight';src:url("//i.s-microsoft.com/fonts/segoe-ui/west-european/semilight/latest.eot");src:url("//i.s-microsoft.com/fonts/segoe-ui/west-european/semilight/latest.eot?#iefix") format("embedded-opentype"),url("//i.s-microsoft.com/fonts/segoe-ui/west-european/semilight/latest.woff") format("woff"),url("//i.s-microsoft.com/fonts/segoe-ui/west-european/semilight/latest.ttf")

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\signup[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	164921
Entropy (8bit):	5.168918127498864
Encrypted:	false
SSDEEP:	1536:Okf5Pv25eFzlF70UgGZ2qWlem/ZapiBN1SoBFo5AXCCx648tFcDJqMgdmy:Pf4RW2Jem/ZapiBRBkNCx6/tFcvgQy
MD5:	B410E292BAC4AAF8A332936BBDB6C949
SHA1:	57A8534804BBDE1AA2582801DAF75A27A5ED8330
SHA-256:	093815D447FB570461A8DC5E36FEA3ECECE3E6C2BA3654F0696A19C63A895AB7
SHA-512:	419D8C663B7A50AC3F5C04B6F5393CEE4AB7ACE9933D5E26FC77324689D4D696468F3F811029A5F750E7B9C5DF5278A3E4CCE9854F8B6C7A06B99A41ECA61B69
Malicious:	false
Reputation:	low
Preview:	.. Copyright (C) Microsoft Corporation. All rights reserved. -->....<!DOCTYPE html>..<html lang="en" xml:lang="en" class="m_ul" dir="ltr" style="">.. <head>.. <link rel="preconnect" href="https://acctcdn.msauth.net" crossorigin>..<link rel="preconnect" href="https://acctcdn.msauth.net" crossorigin>..<meta http-equiv="x-dns-prefetch-control" content="on">..<link rel="dns-prefetch" href="//acctcdn.msauth.net">..<link rel="dns-prefetch" href="//acctcdn.msftauth.net">..<link rel="dns-prefetch" href="//acctcdnmsftuswe2.azureedge.net">..<link rel="dns-prefetch" href="//acctcdnvzeuno.azureedge.net">.... <title>Microsoft account</title>.. <meta http-equiv="Content-Type" content="text/html;charset=utf-8"/><meta name="referrer" content="origin"/><meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=2.0, minimum-scale=1.0, user-scalable=yes"/><meta name="format-detection" content="telephone=no"/>.. <link rel="shortcut icon" href="https://acctcdn.msau

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\style[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	836
Entropy (8bit):	4.940950417710206
Encrypted:	false
SSDEEP:	24:Cn5ZoK2kNMCJZ4ZVaeao1DphsILHJNM2WXgEXgf0Xgm:u5dxJZ4+BWIIPLQ73/
MD5:	2AC383F4677A1036C8EA4289F99A31E3
SHA1:	E65967B9273029CDDD5A5F8DF9E61DACF89CF11C
SHA-256:	2206A95E6BAC7C185CC54638EBF0B0089CBC27FF729B45AC63C968CFE4991AA4
SHA-512:	9E61D4E2B42A1BC776C5649ECD2E32A1CE1ACEDA929E8C013D20BE95D12B7B56864FD588D6117E6410988331F85E21815E2E135030F49BEA2A244F872570DBE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSStyles/style.csx?k=4627136a-bd68-db6e-30c9-37cf96c98eee
Preview:	body .grid,.body-open .grid,.grid h3,.grid .h3,.grid .header-small,.grid strong,.grid .body-tight-2,.grid h1,.grid .h1,.grid .header-large,.grid .caption{font-family:"Segoe UI"}.grid{max-width:1600px !important}.c-uhfh-actions,.c-uhfh-gcontainer-st .all-ms-nav,.glyph-global-nav-button{display:none !important}.shell-header-wrapper,.shell-footer-wrapper,.shell-category-nav,.shell-notification .shell-notification-grid-row{max-width:1180px !important}.PsTitle{font-family:Segoe UI,sans-serif;margin-right:.3em !important;font-size:2em;display:inline-block;vertical-align:top;margin-left:-.02em}.childModule{margin-left:8% !important}.CollectingYourInfoRightNav{display:none}html[dir=rtl] .m-r-md{margin-right:0;margin-left:10px}html[dir=rtl] .m-l-md{margin-left:0;margin-right:10px}html[dir=rtl] .m-r-bl{margin-right:0;margin-left:40px}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\website[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	19578
Entropy (8bit):	5.243804219387574
Encrypted:	false
SSDEEP:	192:AgBjy+mpx941pAKlVdggX4mFTJF5NuOUz0e1IZKXHMcTTXFX/xNOPlx+x2KnbEGs:AUZm/93kg24mFTJFWOuzIY8lx+x1bExj
MD5:	00F4C8A7128E42589BFA8686199C9B48
SHA1:	BF2F14950AC2FCDBEAFF43C337D30EB7AAD84D1D
SHA-256:	F951AD4D9E13D53094E965DD27ACBCDD4AAC1731DCC4A2E0DB5E39D20EAD92B7
SHA-512:	88BC351A4FFED8E273FE5C96D420A31D785B6FC0CC78020DEB92ADEA5EC3B3F3177885E912D37C0074B0D579CD68890348ED06D4D6481A0CBCC9706E4ECB72A
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\website[1].css	
IE Cache URL:	http://https://prod.msocdn.com/2021.1.28.2/en-US/css/website.css
Preview:	.dirSyncLeftContent{float:left;margin-left:10px;margin-right:5px;width:400px}.dirSyncRightContent{float:left}.itemHeader{font-weight:bold}.itemGroup{clear:both;margin:10px 0;overflow:hidden}.helpGroup{clear:both;margin:3px 0;overflow:hidden;padding-left:12px}.helpLink{float:left;line-height:16px;margin-left:5px;width:275px}.migrateItem{clear:both;overflow:hidden;padding-left:15px}.itemText{float:left;margin:0 3px}.itemControl{clear:left;float:left;margin:0}.resultSuccess{background-color:green}.resultFailure{background-color:red}.resultSkipped{background-color:#ff0}.Admin-ErrorPanel{padding:5px 5px 5px 5px;border:1px solid #a80f22;display:block;margin-bottom:10px}.Admin-ErrorTextBox{padding:5px!important;border:1px solid #a80f22!important;display:block!important;margin:0 0 10px!important;opacity:1!important;filter:alpha(opacity=100)!important}.Admin-MessagePanel{padding:5px 5px 5px 5px;border:1px solid #ed8043;display:block;margin-bottom:10px}textarea.Admin-MessagePanel{padding:5px!imp

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\AdminApp[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	2567701
Entropy (8bit):	5.299970276946556
Encrypted:	false
SSDEEP:	49152:9bNNdveYP6BT4GbQGNeQtxRd7njKll4R/7ffXWnOsVQf8E8m8t8E8E8M8m8U08E8:BoeNJ
MD5:	F2354BF60AC0BBA9225B843E03BF13C0
SHA1:	52E805313E8D861EC05A6DC9B07D343E67FC0EC8
SHA-256:	AEF7AA4F966477B38979CD7A98DF3DC1BFB80852500E622D20A356FE98FAC0C4
SHA-512:	A8D7828E98E068CB2E0B280C94E9AEBA6EC74F9897BB8C765C06C30B16C4237D3C54BBA879AA1CCF2B2BB673E2414C75E98F84E197AC83D7D489C3589AF8F8E7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://prod.msocdn.com/2021.1.28.2/en-US/JSC/AdminApp.js
Preview:	Array.prototype.find||Object.defineProperty(Array.prototype,'find',{value:function(n){var i,u,f,t,r;if(this==null)throw new TypeError('"this" is null or not defined');if(i=Object(this),u=i.length>>>0,typeof n!='function')throw new TypeError('predicate must be a function');for(f=arguments[1],t=0;t<u;){if(r=i[t],n.call(f,r,t,i))return r;t++}return undefined},configurable:!0,writable:!0}),Object.entries||(Object.entries=function(n){for(var i=Object.keys(n),t=i.length,r=new Array(t);t--;)r[t]=[i[t],n[i[t]]];return r}),typeof Object.assign!='function'&&Object.defineProperty(Object,"assign",{value:function(n){'use strict';var f,r,i,u;if(n==null)throw new TypeError('Cannot convert undefined or null to object');for(f=Object(n),r=1;r<arguments.length;r++)if(i=arguments[r],i!=null)for(u in i)Object.prototype.hasOwnProperty.call(i,u)&&(f[u]=i[u]);return f},writable:!0,configurable:!0}),String.prototype.startsWith||(String.prototype.startsWith=function(n,t){return this.substr(!t||t<0?0:+t,n.lengt

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\AdminBootstrap[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):	1074668
Entropy (8bit):	5.366116766427001
Encrypted:	false
SSDEEP:	6144:+rsnhwq22Ehxdyw0D1KLYtzkEUZ9aSKv4uUfSw4fTEAv7cRxNjUKWmXPJUaHCL:jchxdyxrtw/MDw4fTEGoWm/WtL
MD5:	B39486710C8382FF9994248603A9F52D
SHA1:	84E174228D1AAC0736948997D0A33ECF40F2ABC3
SHA-256:	3AE4ED30A45821161397424BBA79F6A49BB458235ACE34046A377F790B8C1DBC
SHA-512:	975FD95F447CBDBA0AA6887812860144B3001DBDBC88EE74CE36118589B4654BFA3D9F58C78A1A227EA30E724D4C8F09F890475C57A010B9F28F1905696D088E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://prod.msocdn.com/2021.1.28.2/en-US/JSC/AdminBootstrap.js
Preview:	var AdminApp,Admin;(function(n){'use strict';;n.app=AdminApp=angular.module("AdminSPA",["ngRoute","ngAnimate","ngStorage","ngCookies","ui.bootstrap","ui.router","ngSanitize","ngResource","ncy-angular-breadcrumb","angular-tour","kendo.directives","ngMessages","mgo-angular-wizard","ngCsv","gridster","ngAria","ngCsvImport","ngFileSaver","colorpicker.module","cfp.hotkeys","infinite-scroll","angular-momentjs","LivePerson","ui.select"]).run(["$rootScope","$state","$stateParams","$window","$http","$templateCache","$timeout","ConciergeIntegrationService","HelperService","DomainService","RecommendationService","SFBFrameService",function(t,i,r,u,f,e,o,s,h,c,l,a){function vt(){o(function(){var n=angular.element(document.querySelector('#DelayLoadAdminFooter'));n.length>0&&$('#AdminAppFooter').load("/AdminPortal/Home/adminfooter",function(){o(function(){var u=angular.element(document.querySelector('#AdminFeedbackDiv')),n,t,i,r;u.length>0&&$(u).trigger("AdminFeedbackDiv",!0),n=angular.element(docume

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\AngularExtensions[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):	1059287
Entropy (8bit):	5.67616825829357
Encrypted:	false
SSDEEP:	24576:QIUX3c5h1Z4bJ5XXtlJmPcPnTnHUbhErpWK8E:QIUX3zXtlJmkfTnHUbhErpWK8E
MD5:	28603F46FD399473B7E8BB456ACC53D9
SHA1:	BE6D47669B43C403E0F15906A85F49F20C47AFA9
SHA-256:	699DB0CABC66C2AFB0A696604F055683AF5CD89065640BF1DE31BE246FE9488F
SHA-512:	69D2EB9BD84BE4D6545B28B213125C3639B04E65AF2E39A5C0E8513753335E765C43E6828F787C04F56160CABA9EA664B6232591D8C16D0CE22ACDB74DA0846

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\AngularExtensions[1].js	
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://prod.msocdn.com/2021.1.28.2/en-US/JSC/AngularExtensions.js
Preview:	/*! angular-breadcrumb - v0.3.3-dev-2015-04-21.* http://ncuillery.github.io/angular-breadcrumb.* Copyright (c) 2015 Nicolas Cuillery; Licensed MIT */.!function(n,t,i){"use strict";;function c(n,i){return t.equals(n.length,i.length)?n>i:n.length>i.length}function u(n){var t=n.replace(/\n/g," ").match(/^([^(]+?)\s*(\((.*)\))?$/);if(!t||4!==t.length)throw new Error("Invalid state ref '"+n+"'");return{state:t[1],paramExpr:t[3]\|\|null}}function l(){var n={prefixStateName:null,template:"bootstrap3",templateUrl:null,includeAbstract:!1};this.setOptions=function(i){t.extend(n,i)},this.$get=["$state","$stateParams","$rootScope",function(t,r,f){var e=f;f.$on("$viewContentLoaded",function(n){c(n.targetScope.$id,e.$id)&&(e=n.targetScope)});var s=function(n){var t=n.parent\|\|(/^(.+)\.[^.]+$/.exec(n.name)||[])[1],i="object"==typeof t;return i?t.name:t},o=function(i,f){for(var o,c,s=u(f),l=!1,a=!1,h=0,v=i.length;v>h;h+=1)if(i[h].name===s.state)return;o=t.get(s.state),o.ncyBreadcrumb&&(o.ncyBreadcrumb.fo

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\AssistancePanel[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	27905
Entropy (8bit):	5.141736623285827
Encrypted:	false
SSDEEP:	384:CyBOE54ZAWJZNdZ6t1McvLKwOwpFmtWDiY1HyxvUZ9VKyQgARpRB1ZguiRheZlBG:0E54XJxw1HyRYKIskey0aOBc2TphyLp
MD5:	1C464B916FDF6B04FF983E23B491DC64
SHA1:	27F7D2B90E96CF58B15286458BF3CF430C6E47D5
SHA-256:	9B2344DA5CB380BCCA74351142434E798F9A00DAC87AC5B1AE2F687570D64CDC
SHA-512:	1DBB6561E263AAC7B158F208B3B2FBB95D0D455C84A51E39805876536E1FF3F5F31FBC531187E4DB58135747396496E3CFDA51B7B80E4592CCE0E759688F2FA8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://prod.msocdn.com/2021.1.28.2/en-US/js/AssistancePanel.js
Preview:	var AssistancePanel={};AssistancePanel.ControlId='',AssistancePanel.ContextControlSelectors=[],AssistancePanel.ShowPanel=!1,AssistancePanel.ShowSearch=!1,AssistancePanel.ShowPopularAnswers=!1,AssistancePanel.ShowAskQuestion=!1,AssistancePanel.ShowViewQuestions=!1,AssistancePanel.CommunityIsDown=!0,AssistancePanel.CommunityUserExists=!1,AssistancePanel.ShowSuggestion=!0,AssistancePanel.panel_is_open=!1,AssistancePanel.search_is_open=!1,AssistancePanel.UpdatePopularAnswersCalled=!1,AssistancePanel.onbeforeunloadfired=!1,AssistancePanel.lastLoadedSearchTerm=null,AssistancePanel.SearchText='',AssistancePanel.SearchContextualOnly=!0,AssistancePanel.SearchCurrentPageNum=1,AssistancePanel.MessagePopularAnswers='popular answers',AssistancePanel.MessageHaveIssue='Have a specific question?',AssistancePanel.MessageGetHelp='Get help from Office 365 community experts.',AssistancePanel.MessageHowCanWeHelp='How can we help?',AssistancePanel.MessageGiveUsDetails='Add details:',AssistancePanel.MessageE

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\DomainManager[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	C source, ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	2808
Entropy (8bit):	5.1572741755282765
Encrypted:	false
SSDEEP:	48:sWF91f5mDoDpDy0l7VH5KrRUPV+4HP5lVUrVjpzvUVyQfUV5y3woyUwdTl:sOjSspDy0eVZKlUBTsBgE
MD5:	319F77A87D0974A10ECF31F37341DF76
SHA1:	4F9C6823CDCABBC6D317109C19176498B22E8E1C
SHA-256:	84777EC4B081683D569CBC42B8E2FEA5662B5A0CB8A0F5C0C635F974C4B586C1
SHA-512:	DC68CC64B4F5023154316D3885731E77A7E71FA7D4A3CE6B5D0B665B086EE193E6507A66365ABE2746714741233333BAADA39DA4A89105EDF53843D55A2FD3FF(
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://prod.msocdn.com/2021.1.28.2/en-US/js/DomainManager.js
Preview:	var O365;(function(n){var t;(function(n){var t=function(){function n(){this.ProcessingIsDomainPresentRequest=null}return n.GetInstance=function(){return n.Instance==null&&(n.Instance=new n),n.Instance},n.prototype.Initialize=function(n,t,i){return this.ListGridId=n,this.NeedsToCheckDns=t,this.NeedsToBackfillDomainPurchaseData=i,window.O365Shell&&window.O365Shell.Notifications&&window.O365Shell.Notifications.RefreshSystemNotifications(),this},n.OnFetchDataCompleted=function(){var t=n.GetInstance();return t.SelectFirstRow(),t.NeedsToBackfillDomainPurchaseData&&(t.NeedsToBackfillDomainPurchaseData=!1,Microsoft.Online.BOX.Admin.UI.Domains.Reseller.DomainResellerManager.BackfillDomainPurchaseData(n.BackfillDomainPurchaseDataCallback,n.BackfillDomainPurchaseDataCallback)),t.NeedsToCheckDns&&(t.NeedsToCheckDns=!1,Microsoft.Online.BOX.Admin.UI.Domains.Repository.DomainUIRepository.CheckDns(n.CheckDnsCallback,n.CheckDnsCallback)),!1},n.BackfillDomainPurchaseDataCallback=function(t){t==1&&n.GetI

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\Domain_Add_16x16[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):	1008
Entropy (8bit):	6.082804268439566
Encrypted:	false
SSDEEP:	24:f1hpgyWwjx82lY2T3/VJ4mY4CTmYayJ3VJNmYMmCFSmYfGV8:t/ENn2DAJ3ybQi8
MD5:	84DEE654C2C6E5185D8B78C0C23E45EB
SHA1:	CB1A7AF4904865A035BFA41A85F42F5E1E2FA515
SHA-256:	7085C708C1C708DC07E17F067E8F850B9018AF2DB6321610F42CBDA9F7F83AB8

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\Domain_Add_16x16[1].png	
SHA-512:	ECFDF476F69D7526C8E9669881A766ECFB3C987B72AB1150B8678A7E3B6C5E51A3347CFB9FCF7C7FE0407D22FC925B84D2A759CEAD8E51B537219D8704A24C D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://prod.msocdn.com/domains/images/Domain_Add_16x16.png
Preview:	.PNG.....IHDR.....a....tEXtSoftware.Adobe ImageReadyq.e<...!iTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.5-c021 79.154911, 2013/10/29-11:47:16 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmp:CreatorTool="Adobe Photoshop CC (Windows)" xmpMM:InstanceID="xmp.iid:78697A5AAED911E39E10D9C59246481D" xmpMM:DocumentID="xmp.did:78697A5BAED911E39E10D9C59246481D"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:78697A58AED911E39E10D9C59246481D" stRef:documentID="xmp.did:78697A59AED911E39E10D9C59246481D"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>.wX....eIDATx.b466f.....\...hv.. .P.@..D.a`..R.....ldp...U..X...T..(.8.....B ..E..X.. `..\jF.."!aM$H........_..@.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\Domain_Purchase_16x16[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):	1119
Entropy (8bit):	6.390115600649757
Encrypted:	false
SSDEEP:	24:f1hpgyWwjx82lY2T3/VSNVYyJ3VfaMZZGamq1GmoFMuycdIzgz:t/ENn2De7J3jtl1GmoFnbtz
MD5:	263666D8119D627871A4D1D61F3E9F13
SHA1:	60E2F5415069391A7CA2A06B20833500CE74D930
SHA-256:	A30CFB98095D8111D201FB41B436D45185752B6DFE88E44D0925E9DA22263BDC
SHA-512:	362AAF93F104C35D9EB4A7AC5426300579D05605002D5199E4FF6C00793CC5828C2AC7C0490F890BA88969C27056D1A9A3BC1EB91AFE58198BBDDB086EBEFDF C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://prod.msocdn.com/domains/images/Domain_Purchase_16x16.png
Preview:	.PNG.....IHDR.....a....tEXtSoftware.Adobe ImageReadyq.e<...!iTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.5-c021 79.154911, 2013/10/29-11:47:16 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmp:CreatorTool="Adobe Photoshop CC (Windows)" xmpMM:InstanceID="xmp.iid:7C0234E5AED911E3845DC91F722A2105" xmpMM:DocumentID="xmp.did:7C0234E6AED911E3845DC91F722A2105"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:7C0234E3AED911E3845DC91F722A2105" stRef:documentID="xmp.did:7C0234E4AED911E3845DC91F722A2105"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>.....IDATx.b...?.%...B.B.b...f u.....3g,XH....-.8.....Aa.4y+.mM..l@..h.2.....HWl....H...l.."R.o .G..G....a.P....M.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\GeminiWizard[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):	9028
Entropy (8bit):	5.2055101815002125
Encrypted:	false
SSDEEP:	192:epfigVSPs7ns7nXpVgAy0/0NxfU/S0fUNRf0QaUax0EUNRf8GKbtOOR74s2:ePVS07nynXpZy0/uxfKS0fORfTaUax0t
MD5:	D66AE4644B136B468507E2E758E2C732
SHA1:	8540307D3EAA68D1540AE501E1D0A65682249B62
SHA-256:	78F204FB7B794AAD7425F3822F1C8C0107F0FA1442369A798AEF0DC6BF35B40D
SHA-512:	1A6564216182A71E63EC83417A3DD5C16FC7AB3AD6DBB5A6EA1957770293D08BB73BE9BE9E185CA55D4CBD3CE529A4373E3F8AE7C1C9FCCA68A40B5D007A7 97
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://prod.msocdn.com/2021.1.28.2/en-US/WebControls/JS/GeminiWizard.js
Preview:	var GeminiWizard=function(n,t,i,r,u,f,e,o,s){this.Id=n,this.NavigationPaneId=t,this.Steps=[],this.ForceValidationOnNext=r,this.EnableAnimationOnTranisition=u,this.LastCompletedIndex=-1,this.StartAtStepIndex=typeof f=="undefined"||f==null?0:f,this.CurrentStep=null,this.IsInAnimation=!1,this.NavigationQueue=[],this.QueuedNavigationTimeout,this.BaseFieldCount=3,this.MinimumScreenPadding=50,this.OrginalItemSpacing=30,this.OnNavigationCompleted=null,this.OrginaScreenPadding=30,this.MinimumFieldSpacing=10,this.StepNotStarted=e,this.StepInProgress=o,this.StepCompleted=s,This=this,GeminiWizard.prototype.FocusAfterNavigate=function(){$("input[type='text']:visible",$("#"+This.CurrentStep.Id)).first().focus()},GeminiWizard.prototype.AdjustMinHeight=function(){if(typeof screenHeight!="undefined"&&screenHeight){var n=screenHeight-$(".footer").height(),t=$('.steps-container').outerHeight(!0)+$('.left-nav h1').outerHeight();$(".screen").css("min-height",(n<t?t:n)+"px"),$(".background").css("height",

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\GridView[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):	7808
Entropy (8bit):	5.229365087117069
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\GridView[1].js	
SSDEEP:	96:L+qs9f6jGaJDM2j/jHHe0Oy6qkmYdcCXiwLPzwL5AcP0F0mqDY3cpS7Z:CCGaG8jrjkmYdcBwLPz4OVvqsMpSd
MD5:	CFAC4D37EBEE0DEB9CA7FF514C67910B
SHA1:	DA0A3FC895086FC6094B24811EC6E494ACACC4C8
SHA-256:	6FEDAE5107F342161BA5B8DC77D5D20A77FEEC58A4417A4CB14C8BAA883D157E
SHA-512:	40DB53C62062B2527DEC3594A669F3A4B32A44F5DF4C0141281EABBCDD0518FA52414C6A862BB1E7A0932C1E9BDB3F13EC5A4BE74C53ADBA73CAC78A460A7 3E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://prod.msocdn.com/2021.1.28.2/en-US/WebControls/JS/GridView.js
Preview:	var GridViewManager={};GridViewManager._gridViewInstanceIds=[],GridViewManager._gridViewInstances=[],GridViewManager.CreateGridViewInstance=function(n,t,i) {var r=n.replace(/_Grid_ListViewUpdatePanel$/i,""),u,f;return GridViewManager._gridViewInstanceIds[r]?null:(u=new GridViewInstance(r,t,i),f=GridViewManager._gridView Instances.length,GridViewManager._gridViewInstances[f]=u,GridViewManager._gridViewInstanceIds[r]=f,u)},GridViewManager.GetGridViewInstanceByID=function(n){var t =GridViewManager._gridViewInstanceIds[n];return GridViewManager._gridViewInstances[t]},GridViewManager.GetGridViewInstance=function(n){var t=null,i,r,u;if(n){fo r(i=/(_Grid_ListViewUpdatePanel)|(_LayoutUpdatePanel)$/i;n&&(!n.id||!n.id.match(i));)n=n.parentElement;n&&n.id&&(r=n.id.replace(i,""),u=GridViewManager._gridVie wInstanceIds[r],t=GridViewManager._gridViewInstances[u])}else t=GridViewManager._gridViewInstances[0];return t},GridViewManager.LoadInit=function(){var t,n;for(Sys.Application.remove_load(GridViewMana

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\HIPControl[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):	38677
Entropy (8bit):	5.2403199684773
Encrypted:	false
SSDEEP:	768:mlxte81WzOZm5eiSPuAAjmFl9+pW4bg1WMG1yKyAIHo7lYSF5bsbMb8jssi1+:ix91WzZYiOuIl9+pW4b7IXSo
MD5:	F0CCEF116CC550152B90DB0EA68D8FB0
SHA1:	1D813F3F06C36AA45AE76A8B5AAD50B24FCC460D
SHA-256:	811E2184ACAC6E3DC10851B5E1DDD6F431AB4FEFF39A4914EE487A961F7761DB
SHA-512:	2105C19E40EE71D0278832B430A9E208606AFE052F6C05A3CE53D5B2F31E114246853E836A971891F1EA9B7165EC08D63F9F4B516D141BC8E7DBC0073240F72A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://prod.msocdn.com/2021.1.28.2/en-US/JSC/HIPControl.js
Preview:	function HipChallenge(){this.LoadingTrials=3,this.CurrentLoadingAttempt=0,this.FailOverMessage='',this.ShouldShowMessageOnFailing=!0,this.IsActive=!1,this.IsUIL ess=!1,this.IsChallengeLoading=!1,this.ChachedLoadingParams=!1,this.CachedLoadParam1=null,this.CachedLoadParam2=null,this.CachedLoadParam3=null,this.C hallengeId='',this.Verified=!1,this.FailOverChallengeId="",this.LoadTimeOut=2e3,this.LoadTimeOutHandle=null,this.UILoaded=!1,this.PrerequisiteChallenge='',this. ConnectionFailed=!1,this.ShowValidation=!1,this.Loaded=!1,this.DependantChallengeId='',this.GradedActionChallenge='',this.ShowErrorPanel=function(){},this.Deact ivate=function(){},this.Activate=function(){},this.ShowConnectivityError=function(){},this.GetVerificationData=function(){this.NotImplementedException()},this.GetUserResp onse=function(){this.NotImplementedException()},this.GetChallengeType=function(){},this.Show=function(){this.UILoaded=!0},this.Hide=function(){this.UILoaded=!1} ,this.Verify=function(){return!0},this.V

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\ListGrid[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	61371
Entropy (8bit):	5.237542510810988
Encrypted:	false
SSDEEP:	384:J66D8dHRGWZMKGrhEDa/Vi7XVl1TqI4iv1SxXlSlE4GYLQ6IgXm0gWtMZAGn6wpL:BmRaI9ahvYsw2DAGn6wppscyO1
MD5:	6D4AD7661B98C4CE3444484CBC068A7E
SHA1:	9A4BC733289A99B8D11D8904B5098EFBE3D98C64
SHA-256:	1461BE81ED64FF3244D8EF01E12F34D0D66D8FD6D5912BBBD2FFF6316AAF0D53
SHA-512:	1026990C1984BA88BC049AB3BE5F051DD314559F52E228DBA0A3F7D76AD208BC45A2228A0E847303AD8B76ED0B3920EE806B41C918282DF8D5BE8E7EE4379B9 1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://prod.msocdn.com/2021.1.28.2/en-US/WebControls/JS/ListGrid.js
Preview:	var NavigatePage,BOX,ListGrid;(function(n){n[n.NoChange=0]="NoChange",n[n.First=1]="First",n[n.Previous=2]="Previous",n[n.Next=4]="Next",n[n.Last=8]="Last",n[n. Direct=16]="Direct"})(NavigatePage||(NavigatePage={})),function(n){var t;(function(n){function i(n){var t=document.createElement("div");return t.appendChild(doc ument.createTextNode(n)),t.innerHTML.replace(/\"/g,""")}function t(n){var t=i(n);return t.replace(/\'/g,"'")}function o(n,t){return t.length?t.length>n.length?!1 :n.substr(0,t.length)==t:!0}function u(n){return n!==null&&n!==undefined&&n!=''}var a,v,s,h,f,c,l,r,e;(function(n){n[n.ascending=0]="ascending",n[n.descending=1]="descend ing"})(a=n.SortOrder||(n.SortOrder={})),function(n){n[n.clientInitiated=0]="clientInitiated",n[n.serverInitiated=1]="serverInitiated"}(v=n.DataFetchMode||(n.DataFetchMode= {})),s=function(){function n(){this.AddButton='AddButton',this.ArrowDown='ArrowDown',this.ArrowUp='ArrowUp',this.CloseButton='CloseButton',this.DeleteButton='D eleteButto

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\NetPerf[1].js	
Size (bytes):	4787
Entropy (8bit):	5.3136178165749515
Encrypted:	false
SSDEEP:	96:5iBUcCRgqJY+ebZFBfquEiwQYGQwnCSo3DijVxlJz/odkFVMhMY7PHYh+O8C:5i/PquEiwQ/QJzDeVnN/odkbMhMY7PHI
MD5:	D4A9893F26D6C6BA6370D1AA877D9530
SHA1:	616E7478F40C2EE6DDE03C7D6AFA35265211EDBD
SHA-256:	329E33E61952A1445BF79F6D073FF443339AA13E6338C568D20A3015C0E7BF9E
SHA-512:	9870638699DD51E0EEF34BCE532E24B585FE02E3BB52AE62F0389E97904EE04A12646D24041F277718938A1EA3AF257BDB6D136514B97AB0790FF1E9C1F40820
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://prod.msocdn.com/2021.1.28.2/en-US/JS/NetPerf.js
Preview:	function NetPerf(){function c(r){var u,l=[],p=["i":30000,"v":3'],o,a,y,s,h,v,c;if(l.push(p),u=[],r=='u')e?(u.push('0'),u.push('1')):(u.push('1'),u.push('0'));else if(r=='l')u.push('0'),u.push('0'),e=!0;else return;for(o=null,y=f.length,s=0;s<y;s++)h=window.performance.timing[f[s]],o==null?o=h:(a=h>0?h-o:-1,u.push(a));if(u.push(""+n.encodeJsonStringLiteral(document.URL)+""),u.push(n.edgeInfo.isEdge?"1":"0"),u.push(""+n.encodeJsonStringLiteral(n.edgeInfo.ds)+""),u.push(""+n.encodeJsonStringLiteral(n.edgeInfo.f.toString())+""),u.push(""+n.encodeJsonStringLiteral(n.edgeInfo.cid)+""),v=[],n.edgeInfo.prop)for(c in n.edgeInfo.prop)n.edgeInfo.prop.hasOwnProperty(c)&&v.push(c+'='+n.edgeInfo.prop[c]);u.push(""+n.encodeJsonStringLiteral(v.join(t))+""),u.push(""+n.encodeJsonStringLiteral(n.edgeInfo.wl)+""),u.push(""+n.encodeJsonStringLiteral(n.edgeInfo.tid)+""),u.push(""+n.encodeJsonStringLiteral(n.edgeInfo.ipv)+""),l.push(""f":['+u.join(t)+']'),i.push('{'+l.join(t)+'}')}function

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\O365SharedClusteredImage[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 296 x 168, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	26186
Entropy (8bit):	7.981535861643487
Encrypted:	false
SSDEEP:	384:AM/GaZ38Yog5DrPgXbRrRO7Tyu7aoiuGkLDYhlILJOZOp+1uHZnyjwJkv2IjHn0H:3ijg5HER4dbehlIOuZy97bvQ
MD5:	AA28125192CC8D2864AF67D09A25C099
SHA1:	11252D6F3BD826C2ED9A48096C580458E58F0127
SHA-256:	FB0F5D0B6B161DBC395A3D1186E6CBCFC6DA62D36CDEC3E4D9FE1F1619B9826D
SHA-512:	E65F31CC1E8126EDE35743F05F610617722AB1D9E9271DBFEAF855C6129DC83C2C1FB211E7F51309F028185A5F08CA6D9B9FCF1CB624FAFF248C5D21155543E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://prod.msocdn.com/Shell/Images/O365SharedClusteredImage.png
Preview:	.PNG.....IHDR...(.....S.su....sRGB.....gAMA.....a...e.IDATx^.].|T..>.....z.E.....(<D,X..`.#*$. O.|.P)6"M.Y..P..l( $.....@B.....}.....T...~g..;w..sgg...&L.0a...&L.]`.M...0 * .^X.Y,..0.....{/UE2a.....O.>A...7...n..h....!..).O.Bw.0a....#...1c.....{..X...Yy.../.Z.M.....j..]...3.}...z.?.....hHH.4.....x.z...A...8.....8.....:....0..d.....x....'g.y..{.(.V.q.....F.....7 ..]..U.K.....Q....c.:to..G[..;V....S..q.....bP..i.u....;<.....G.}.....-.9c.....$..D.....o.;7.=F...hsTw.x.....{ad.o/.[J?.l.....q q.D.3.!..z.`.....#../...."".....y.....]...<.]......!.>[7.....v.g.._.;0.]w.. <.&..7.(4.o..].<...0Z.N..p...q.....`.?.h.....C...\....fPP..h..X.ma.+...gD...c.}4.:D.....}8..a.....|...~@.....x...Q...k..g..F....&.fC~.....+.P./x.e..yJJ.o.e.1v9|..>0./..W!...GC}...F.U.... +.W..x.N ....WL.m...;..{A#..;!.4..2.....r28.....v.....p .....<.G..X...s..... ...w.V....3...+....Y&'.....>..$.].|6.KQG.....~F....3....+.[...~..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\PasswordStrengthMeter[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):	3041
Entropy (8bit):	5.443939715136298
Encrypted:	false
SSDEEP:	48:8/JawL2CDpLGLg0ELdcImwDb3+qoekDYk/GCqpufqv0wgViv9Y+eMNzeRqKb+mpZ:cL5ug3dVf+qpkMkgpufqvFgVi++ecUqK
MD5:	2A29FC3105377608989FDCF710A47554
SHA1:	F6AC20B91A57841A4F84A7DAFA490502FB20D6A4
SHA-256:	8DC4107571BA20983D62DF95A23D5CABC961418C55B75A8CEB1437A83CC7AB3F
SHA-512:	85FFFBC2A8681989E048E9A3E754ADE8D60C9FA603F88747C73C0EC02848EEF34A703EA47F0DCF40B59405B02FBA2C1B3F1700DE8D7710B9DBC6F7291B1EAB A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://prod.msocdn.com/2021.1.28.2/en-US/JS/PasswordStrengthMeter.js
Preview:	var PasswordStrengthMeter=function(){function n(n,t,i){(this.PasswordMeterDiv=document.getElementById(n+"_passwordStrengthMeter"),this.PasswordStrengthMeterId=n,this.PasswordTextBox=document.getElementById(t),this.PasswordTextBox!=null)&&(this.PropertySheetId=i,this.PasswordTextBox.PasswordStrengthManager=this,this.PasswordTextBox.onchange=this.TextChangedHandler,this.PasswordTextBox.onkeyup=this.TextChangedHandler,this.PasswordTextBox.PasswordStrengthManager.EvaluatePassword(!1),this.PasswordStrengthMeterDisplayed=!1)}return n.prototype.EvaluatePassword=function(t){var i='weak',r;this.SetMeterLevel(this.PasswordStrengthMeterId,n.METERLEVEL_URGENT),r=this.PasswordTextBox.value,n.ClientSideStrongPassword(r)?(i='strong',this.SetMeterLevel(this.PasswordStrengthMeterId,n.METERLEVEL_HEALTHY)):n.ClientSideMediumPassword(r)?(i='medium',this.SetMeterLevel(this.PasswordStrengthMeterId,n.METERLEVEL_CAUTION)):n.ClientSideWeakPassword(r)&&(i='weak'),this.PasswordMeterDiv.innerText=i,this.PropertyS

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\PeoplePicker[1].js	
Size (bytes):	11639
Entropy (8bit):	5.192812704605868
Encrypted:	false
SSDEEP:	192:ZHqaIeeago8L9nN0hUNxiHjib9NUhXkop1R1NWS9rCsnZBSVAx8c3ODqbiQ4:4aIee5o8LdN0hUNQW5NiXkYWyrtyAp30
MD5:	68C7188A72C68095DCF664C384BE4A24
SHA1:	44759AF7DA7C068E57D2C68C914CFBB488EF44C6
SHA-256:	A7321F5898D11C794E86F016F4BE7D8355872A94081ADC22D551D5298D1A2900
SHA-512:	CEF7D483D540E7A5B4404A381D25F39FA66DAE81AA58FCE1F42DFB3E03376E31B680BB623EB81ADAE7061A25967F9D196A47E97BDA94AFCCBDEEC422B0BE07F7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://prod.msocdn.com/2021.1.28.2/en-US/WebControls/JS/PeoplePicker.js
Preview:	var PeoplePicker=new function(){var n=this,ft=null,w=null,p=null,y='Too many results, use search.',nt='Total: {0}',k=250,u,c;this.Initialize=function(t,u){var s=$("#"+t);MissingImgUrl=u.MissingImgUrl,w=u.RemoveUserImgUrl,p=u.DeleteUserImgUrl,s.data("GetDataCommand",u.GetDataCommand),s.data("GetAddDataCommand",u.GetAddDataCommand),s.data("AddCommand",u.AddCommand),s.data("DeleteCommand",u.DeleteCommand),s.data("DeleteTooltip",u.DeleteTooltip),s.data("RemoveTooltip",u.RemoveTooltip),s.data("RemoveCommand",u.RemoveCommand),s.data("EmptyListText",u.EmptyListText),s.data("EmptySearchText",u.EmptySearchText),s.data("OnClientAfterGetData",u.OnClientAfterGetData),s.data("OnClientGetDataError",u.OnClientGetDataError),s.data("OnClientAddButtonClick",u.OnClientAddButtonClick),s.data("OnClientSelectionChanged",u.OnClientSelectionChanged),s.data("OnClientBeforeDelete",u.OnClientBeforeDelete),s.data("OnClientAfterDelete",u.OnClientAfterDelete),s.data("AllowMultiSelect",u.AllowMultiSelect),s.data("Sh

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\ProductKeyControl[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):	6094
Entropy (8bit):	5.324866002827835
Encrypted:	false
SSDEEP:	96:AkjE+hfNEr7iDYdcG/e9BibhThrd3NrY/hLzX+IUcDKQEm8mw38dlRRxPWIHA2LU:A+bTEXdcG/e9wbhThrdCdOc+34lR7Weu
MD5:	3EED7BA0DAC5334BBFB37CF020FDBF5E
SHA1:	C50F48EE80602FAD48570D156154611884D96EB0
SHA-256:	C7157A9FC54B34EC8F7CF095F2967B85561168F73D5209A81CAE3148277C3F4A
SHA-512:	655F9EF2813C9D4C73FE1E6FBB3119F87E7C1A64029FBDA90C5C9701B457D10D9B7E15B59BC6B1E66645877D35DF59F1A42AD0AE7072B335DEECB18E138F29BA
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://prod.msocdn.com/2021.1.28.2/en-US/WebControls/JS/ProductKeyControl.js
Preview:	window.O365=window.O365||{},O365.ProductKeyControl=function(n,t,i){var r={Empty:{imgSrc:null,imgAlt:null},Incomplete:{imgSrc:null,imgAlt:null},Complete:{imgSrc:null,imgAlt:null},Validating:{imgSrc:'https://prod.msocdn.com/webcontrols/Images/spinner_16x16.gif',imgAlt:'Validating product key'},Valid:{imgSrc:'https://prod.msocdn.com/Images/GreenCheck_default_16x16_metro.png',imgAlt:'Valid product key'},Invalid:{imgSrc:'https://prod.msocdn.com/Images/Alert_High_default_16x16_metro.png',imgAlt:'Invalid product key'}},ut=function(n){var y="ValFieldError",e=!0,f="",o,s=$(n),w=s.parent(),h=s.attr("id"),i=h+"_v",u=i+"_val",c=i+"_err",r=i+"_err_ClientState",l=i+"_f",a=document.createElement("div"),v,t;a.innerHTML="<input type='hidden' name='"+r+"' id='"+r+"' />",w[0].appendChild(a),v=$("#"+u),t=v[0],t.enabled=!0,t.controltovalidate=h,t.display="None",t.isvalid=!0,t.errormessage=" ",t.evaluationfunction=window.CustomValidatorEvaluateIsValid,t.clientva

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\SearchBox[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):	3176
Entropy (8bit):	5.1874348844684315
Encrypted:	false
SSDEEP:	96:FcRnZncnjnx1nw1nVCon7nlKx/DnvnPwOnpBIRjFZoh/JCZ64qAr1Anp0Opt:FCZWbfS3jlq/7/sjDWUZJR0SK
MD5:	E33609CCD161B2921E3314BB2EA1E57F
SHA1:	C36602903D967B93A6C1FF2327E51337A0F63E18
SHA-256:	5A1670A4BFD961D75281157664AA5EE7247D3236991FEC228CBE950AA63D00A8
SHA-512:	24DA3283F4CA4368A2FFF24F183996363D5D8E39A3C0D9E012DA17751A94497B4D584C395766F196BD83978A23B0C1824FF97597068E33CFCAA43BD71DDC2C9B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://prod.msocdn.com/2021.1.28.2/en-US/JS/SearchBox.js
Preview:	var SearchBox=function(){function n(){}return n.OnLoad=function(t,i,r){if(i?n.Focus(t):n.Blur(t),r){var u=$('#'+t+'_TextBox');u.keydown(function(i){n.OnTextBoxKeyDownHandler(t,i)}),u.keyup(function(i){n.OnTextBoxTextChangedHandler(t,i)}),u.focus(function(){n.OnTextBoxFocusHandler(t)}),u.blur(function(){n.OnTextBoxFocusHandler(t)}),u.bind('cut',function(i){setTimeout(function(){n.OnTextBoxTextChangedHandler(t,i)})}),u.bind('paste',function(i){setTimeout(function(){n.OnTextBoxTextChangedHandler(t,i)})})),$('#'+t+'_SearchButton').click(function(){return n.OnSearchButtonClickHandler(t),!1}),$('#'+t+'_CloseButton').click(function(){return n.OnCloseButtonClickHandler(t),!1})}},n.OnTextBoxFocusHandler=function(t){n.Focus(t)},n.OnTextBoxKeyDownHandler=function(t,i){i&&(i.which==13||i.keyCode==13?(n.OnSearchButtonClickHandler(t),n.KillEvent(i)):(i.which==27||i.keyCode==27)&&(n.OnCloseButtonClickHandler(t),n.KillEvent(i)))},n.OnTextBoxTextChangedHandler=function(t,i){n.OnTextBoxKeyDownHandler(t,i

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\WebResource[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	23063
Entropy (8bit):	4.7535440881548165
Encrypted:	false
SSDEEP:	384:GvUzYI+Vi4g1V5it1ONhA6w+Kv8i/4CYzLKL4DrLU0iTxZTAzIzrwDlTWMClQip9:bkON69kClQq8hDRJHp2tWU25Zt/gREVG
MD5:	90EA7274F19755002360945D54C2A0D7
SHA1:	647B5D8BF7D119A2C97895363A07A0C6EB8CD284
SHA-256:	40732E9DCFA704CF615E4691BB07AECFD1CC5E063220A46E4A7FF6560C77F5DB
SHA-512:	7474667800FF52A0031029CC338F81E1586F237EB07A49183008C8EC44A8F67B37E5E896573F089A50283DF96A1C8F185E53D667741331B647894532669E2C07
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://portal.microsoftonline.com/WebResource.axd?d=MXtg1iJlvcCXUg0psCKY65hv7x5zsNj7b4sWbqT5W_wUKFSsYN5qoOOJ_Meqcbf6zzs2C9ua5Drl7HN_YFKgqnHS0XS42Tompdtccfs-3myddgOcqKbq-Kqbxia_abWD2JCWZxRC12RxfHJ7IYbTqg2&t=637458261053210223
Preview:	function WebForm_PostBackOptions(eventTarget, eventArgument, validation, validationGroup, actionUrl, trackFocus, clientSubmit) {.. this.eventTarget = eventTarget;.. this.eventArgument = eventArgument;.. this.validation = validation;.. this.validationGroup = validationGroup;.. this.actionUrl = actionUrl;.. this.trackFocus = trackFocus;.. this.clientSubmit = clientSubmit;..}..function WebForm_DoPostBackWithOptions(options) {.. var validationResult = true;.. if (options.validation) {.. if (typeof(Page_ClientValidate) == 'function') {.. validationResult = Page_ClientValidate(options.validationGroup);.. }.. }.. if (validationResult) {.. if ((typeof(options.actionUrl) != "undefined") && (options.actionUrl != null) && (options.actionUrl.length > 0)) {.. theForm.action = options.actionUrl;.. }.. if (options.trackFocus) {.. var lastFocus = theForm.elements["__LASTFOCUS"];.. if ((typeo

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\WebTrendsStream[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):	28248
Entropy (8bit):	5.347774117671711
Encrypted:	false
SSDEEP:	384:x/I+Y5l9700WyarU/Ozm3hquCBZGreXA4Q7Mxv2zPKrvTYsQ5VK0evSGw8uxQPCb:x/2h00Wr/m3objR2zPKc3K0eaGikl0uG
MD5:	E8C873D69B9CEB16829EA4F9B376EAD9
SHA1:	A167AE5326588A568EE947F84E4B0A039304CB5A
SHA-256:	8BFC29FC85FDC41C80034BD5346114C794B1C55B1D34CD8243E3B084C86738A7
SHA-512:	EDBD7DF8E98680D337EB5E92CBF3351661C10F9F23F71F4DE3F58F88A1D6D122B80B5E4EDA42CB2332ACF18463CD0C81399CE944BB9DA40BD5CD3C6BFD6579A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://prod.msocdn.com/2021.1.28.2/en-US/JS/WebTrendsStream.js
Preview:	(function(n,t,i,r){function f(n){return n&&(n.forEach||(n.forEach=function(n,t){for(var u=t||window,i=0,r=this.length;i<r;++i)n.call(u,this[i],i,this)}),n.filter||(n.filter=function(n,t){for(var f=t||window,r=[],i=0,u=this.length;i<u;++i)n.call(f,this[i],i,this)&&r.push(this[i]);return r}),n.indexOf||(n.indexOf=function(n,t){for(var t=t||0,i=0;i<this.length;++i)if(this[i]===n)return i;return-1})),n}if(!n.Webtrends){var u={dcss:{},plugins:{},dcssIdx:0,gWtId:{},addEventListener:n.addEventListener?function(n,t,i){n.addEventListener&&n.addEventListener(t,i,!1)}:function(n,t,i){n.attachEvent&&n.attachEvent("on"+t,i,!1)},events:{},version:"10.2.81",qryparams:{},hasLoaded:!1,dcsdelay:25,init:function(){r.search&&(u.qryparams=u.getQryParams(r.search)),n.webtrendsAsyncInit&&!n.webtrendsAsyncInit.hasRun&&(n.webtrendsAsyncInit(),n.webtrendsAsyncInit.hasRun=!0),u.addEventListener(n,'load',function(){u.hasLoaded=!0});var t=new RegExp("MSIE ([0-9]{1,}[\.0-9]{0,})");t.exec(i.userAgent)!=null&&(u.IE=p

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\WebTrends[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	15823
Entropy (8bit):	5.328533457196768
Encrypted:	false
SSDEEP:	384:EsQuqcdrwGmE6Du8dcQQh5zSTD4EOVcEjfjNkc/B0wrl5e9V8DP4a4yv:EsQe6SCEewrCaj
MD5:	91C8676E3292BBA46CC19344F98F2390
SHA1:	D33EE4F46D6D83D56720E9B794A7F39B6B263CA6
SHA-256:	48CE87A451A27B4DF39A619AFE51C62389EF455534982A14DC8357895ABFB9AA
SHA-512:	8BE9476E45BC970618ABA6119B229725E5B53A739C7232D26D49B743FC22B0C55436780AC3554D2B40793DACD079E280703880389EC896CEA48C14F2AB1710A0
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://prod.msocdn.com/2021.1.28.2/en-US/JS/WebTrends.js
Preview:	function WebTrends(){var n=this;this.dcsid="",this.wtid_domain="portal.office.com",this.domain="m.webtrends.com",this.timezone=-8,this.fpcdom="",this.onsitedoms=function(){return window.RegExp?new RegExp("oofice365","i"):""}(),this.downloadtypes="xls,doc,pdf,txt,csv,zip,xlsx,docx,pptx,ppt",this.navigationtag="div,table",this.trimoffsiteparams=!0,this.enabled=!0,this.i18n=!1,this.fpc="WT_O365_FPC",this.paidsearchparams="gclid",this.splitvalue="",this.preserve=!0,this.DCS={},this.DCS.dcscfg=1,this.WT={},this.DCSext={},this.images=[],this.index=0,this.qp=[],this.exre=function(){return window.RegExp?new RegExp("dcs(uri)|(ref)|(aut)|(met)|(sta)|(sip)|(pro)|(byt)|(dat)|(p3p)|(cfg)|(redirect)|(cip)","i"):""}(),this.re=function(){return window.RegExp?n.i18n?{"%25":/\%/g,"%26":/\&/g}:{"%09":/\t/g,"%20":/ /g,"%23":/\#/g,"%26":/\&/g,"%2B":/\+/g,"%3F":/\?/g,"%5C":/\\/g,"%22":/\"/g,"%7F":/\x7F/g,"%A0":/\xA0/g}:""}()}function dcsMultiTrack(){if(typeof _tag!="undefined")return _tag.dcsMultiTrack()}We

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\WebUIValidation[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	26951
Entropy (8bit):	4.514992390210281
Encrypted:	false
SSDEEP:	384:jMgviMjM4if38GmhXeC1QRwweTkBE9wbOY4Jf/JhRZ5h+73hNVt8oC4veONhLYVi:CLEiJSdo11vIYHqb5Klo8v
MD5:	B3D7A123BE5203A1A3F0F10233ED373F
SHA1:	F4C61F321D8F79A805B356C6EC94090C0D96215C
SHA-256:	EF9453F74B2617D43DCEF4242CF5845101FCFB57289C81BCEB20042B0023A192
SHA-512:	A01BFE8546E59C8AF83280A795B3F56DFA23D556B992813A4EB70089E80621686C7B51EE87B3109502667CAF1F95CBCA074BF607E543A0390BF6F8BB3ECD992E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://prod.msocdn.com/2021.1.28.2/en-US/JS/WebUIValidation.js
Preview:	var Page_ValidationVer = "125";..var Page_IsValid = true;..var Page_BlockSubmit = false;..var Page_InvalidControlToBeFocused = null;..var Page_TextTypes = /^(te xt|password|file|search|tel|url|email|number|range|color|datetime|date|month|week|time|datetime-local)$/i;..function ValidatorUpdateDisplay(val) {.. if (typeof(val.display) == "string") {.. if (val.display == "None") {.. return;.. }.. if (val.display == "Dynamic") {.. val.style.display = val.isvalid ? "none" : "inline";.. return;.. }.. }.. if ((navigator.userAgent.indexOf("Mac") > -1) &&.. (navigator.userAgent.indexOf("MSIE") > -1)) {.. val.style.display = "inline";.. }.. val .style.visibility = val.isvalid ? "hidden" : "visible";..}..function ValidatorUpdateIsValid() {.. Page_IsValid = AllValidatorsValid(Page_Validators);..}..function AllValidatorsV alid(validators) {.. if ((typeof(validators) != "undefined") && (validators != null)) {

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\arrow_staticdown_16[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	1042
Entropy (8bit):	5.961534921558674
Encrypted:	false
SSDEEP:	24:g1hpunQWwh82lYSKwPKNuVVET3ZyJ3VyIGIcikQC:+itvnLHunE0J3HbnC
MD5:	ACD4CCC53CCE442FC05BA52FA57574D0
SHA1:	B57C0F07B2B5DE89E5468BC2B2529C1A32011D9E
SHA-256:	69970476B5CEAE80F39C399B901B4F9C1FD6C7222CAACE76DD30DEEDF7BD4128
SHA-512:	2870D6266C2DA443430246607D0CFCBC930EBC4F0760B47081734B47786E2057169E66C65B5CCCC6AC566BB7506249A3EDF72481134D9CC92350725327D59BD4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://prod.msocdn.com/images/scrollbar/arrow_staticdown_16.png
Preview:	.PNG.....IHDR.....(-.S....tEXtSoftware.Adobe ImageReadyq.e<...diTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpme ta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.0-c060 61.134777, 2010/02/12-17:32:00 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http ://ns.adobe.com/xap/1.0/" xmpMM:OriginalDocumentID="xmp.did:0EFFC984A5CAE0119B69D54FE88EB690" xmpMM:DocumentID="xmp.did:BAEF2443CEA011E085EF EF2A2063B3B9" xmpMM:InstanceID="xmp.iid:BAEF2442CEA011E085EFEF2A2063B3B9" xmp:CreatorTool="Adobe Photoshop CS5 Windows"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:D46FCB9FD3CDE011A8229227DED0FB1E" stRef:documentID="xmp.did:0EFFC984A5CAE0119B69D54FE88EB690"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>-k.R....PLTE.....tRNS...0J...$IDATx.b`D..4.`

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\arrow_staticup_16[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	1044
Entropy (8bit):	5.983201449273861
Encrypted:	false
SSDEEP:	24:g1hpunQWwh82lYSKwPqV00T3ZyJ3VyIGNk/mKc:+itvnLTu00J3HYKc
MD5:	D5A0044CCEFBE6DB30E6950B0F082CDE
SHA1:	E6022067497CAF888EBBD70216AF93069BFA99D0
SHA-256:	E82CE250BA44AF6A50D7B7885E7583C200185A1604103B05916A4D10ACDD4F76
SHA-512:	7D3FEDC43BEB9F84B3AC5DB8AFAE877EB0475336A512859D68F5405CD64A3612EBBF285FB93D6ADEB2A647C75C0180A2DA373C044D95F4464309313C2DF7A8 D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://prod.msocdn.com/images/scrollbar/arrow_staticup_16.png
Preview:	.PNG.....IHDR.....(-.S....tEXtSoftware.Adobe ImageReadyq.e<...diTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpme ta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.0-c060 61.134777, 2010/02/12-17:32:00 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http ://ns.adobe.com/xap/1.0/" xmpMM:OriginalDocumentID="xmp.did:0EFFC984A5CAE0119B69D54FE88EB690" xmpMM:DocumentID="xmp.did:E35D2522CEA011E0A747 8353B6D7FCED" xmpMM:InstanceID="xmp.iid:E35D2521CEA011E0A7478353B6D7FCED" xmp:CreatorTool="Adobe Photoshop CS5 Windows"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:D46FCB9FD3CDE011A8229227DED0FB1E" stRef:documentID="xmp.did:0EFFC984A5CAE0119B69D54FE88EB690"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>.b.....PLTE.....tRNS...0J...&IDATx.b`D....`

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\header_bg_signup_office[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, big-endian, direntries=7, orientation=upper-left, xresolution=98, yresolution=106, resolutionunit=2, software=Adobe Photoshop CS4 Windows, dat etime=2010:11:16 08:06:38], baseline, precision 8, 1040x182, frames 3
Category:	downloaded
Size (bytes):	34891
Entropy (8bit):	7.5591958729915705
Encrypted:	false
SSDEEP:	768:0C161HOPBgeEswwjbYtjOUYUU2+Jds7b2GD9OGO:raupBzwwfOjItJdssD
MD5:	4F53BAC7F51CC1BD5EBFF673D6F43389
SHA1:	932F1EDE503DA133B1D05949A2FC69C6EA09473B
SHA-256:	A96EA38F3358290869C5756940A90CD00DEE4396A557857D25B1230F00B0CD28
SHA-512:	A34C42CFFCC83F91F2B8453D9D83675E8ED44EAB80E6A05A18DF4B2002D05B505AC07D52AD3CD5A61DF59411E0A93D817F99DC423F2DF75E934F70ABCE70D6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://prod.msocdn.com/Shell/Images/header_bg_signup_office.jpg
Preview:	......JFIF.....H.H.....TExif..MM.*.....b.....j.(.....1.....r.2.....i.....'.....'.Adobe Photoshop CS4 Windows.2010:11:16 08:06:38.....&.(.....H.....H.....JFIF.....H.H.....Adobe_CM.....Adobe.d.....".....?.....3.....!.1.AQa."q.2.....B#$.R.b34r..C.%.S...cs5....&D.TdE.t6..U.e...u..F'.....Vfv.....7GWgw.....5....!1..AQaq"..2.....B#.R..3$b.r..CS.cs4.%.....&5..D.T..dEU6te....u..F.....Vfv.....'7GWgw.....?..T.I%)$.IJl$.R.'l%1"S..d.K...).....Rpi..Q...G}%4..}.....P.^.5..yN..k.)K..i.....K.q.....$.Q.../.e.d.hP~Sy...a...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\header_wizard_hl_mos[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.02, aspect ratio, density 100x100, segment length 16, baseline, precision 8, 4x60, frames 3
Category:	downloaded
Size (bytes):	344
Entropy (8bit):	3.743705275624063
Encrypted:	false
SSDEEP:	3:nSullBbs1lQQp/yEDpeknmRmi7TWdmMi+Uotkt/KuqslyBzdlR5pkgvbpcT:3ll7QzDkmi76dmMiAW1r3erR5plDST
MD5:	FC45F1EBA15B82E9992C300AA47ADD4C
SHA1:	6AF8F18106C945A643208B201D2BBE6A3C379CFD
SHA-256:	37D366227356992ED64D1B9D2948524F2B628212F575E39AE89CF23C1475BB36
SHA-512:	62BB82B9C31CC3816277E0FCD7F997CD8D022AF4529275C40D00215206AFD4F739694BC7E48A76324800D0EDF064780C2124B5BC83E6F95F0E8F1F7DF44820B6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://prod.msocdn.com/Shell/Images/header_wizard_hl_mos.jpg
Preview:	......JFIF.....d.d.....Ducky.....d.....Adobe.d.....<.....].....Rb.$.....Q.."#.....?.....zJo.6.K.....W..u...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\home[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	14574
Entropy (8bit):	5.295486493716673
Encrypted:	false
SSDEEP:	192:Vzgo0TMbylA12RvdLDqlEAdoUoUbIRh3k3JWhxkyAUlODP313p+P9hA:k3ANEAdoObIhlODPZpd
MD5:	CD64465B3AB78F5A991240B457EDE06B
SHA1:	3AA9821324E2CE46365133CE1BC89D76B25C9EE8
SHA-256:	99B892B0B068F134162F1118AFFA7731F5A91160794E326043ADDDDBDE39ADE9
SHA-512:	D5EAC087270928CFDBC1BA752324DDE09DDD0A70EC565E52521A0FE97B62D4844793E53850881B7D8CF776171C815F14A4E302906F4CC5557BE15BCD56088FD
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://prod.msocdn.com/2021.1.28.2/en-US/js/home.js
Preview:	var SearchControl,TwoColumnControl,EnterpriseHome;Namespace.Register("Microsoft.Online.BOX.JS.Home"),Microsoft.Online.BOX.JS.Home=new function(){this.ShowGetStartedDialog=function(){BOX.JS.DialogManager.get_isBrowserIE7Compatible()?DialogManager.showUrl("/IWGetStarted.aspx","",null,"height:530,width:800"):DialogManager.showUrl("/IWGetStarted.aspx","",null,"height:500,width:800")},this.ShowDate=function(){var n=new Date,t=n.getMonth(),i=n.getDate(),r=n.getDay(),u,f,e;typeof LocalizedMonths!="undefined"&&typeof LocalizedMonths=="object"&&(t=LocalizedMonths[t]),typeof LocalizedDayNumbers!="undefined"&&typeof LocalizedDayNumbers=="object"&&(i=LocalizedDayNumbers[i-1]),typeof LocalizedDays!="undefined"&&typeof LocalizedDays=="object"&&(r=LocalizedDays[r]),u=document.getElementById("todayMonth"),u!=null&&(u.innerHTML=t),f=document.getElementById("todayDate"),f!=null&&(f.innerHTML=i),e=document.getElementById("todayDay"),e!=null&&(e.innerHTML=r)},this.SetupCheckForProvisioning=function(n,t,i)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\image1[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, progressive, precision 8, 1513x1369, frames 3

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\image1[1].jpg	
Category:	downloaded
Size (bytes):	75928
Entropy (8bit):	7.835295454101902
Encrypted:	false
SSDEEP:	1536:FVG8mcfDmWfdepy6GsI2PDtGwhiWntTtZqmBorq6BzKnHxg3tgmlYOlU:Fw8mym+dec6GsrLvPntBZqmBoHzCturK
MD5:	CDFF621572FC19F3A63678B877E15A04
SHA1:	20C78D48FEAD728E047C487DCDE9F7C2AD9C1A9D
SHA-256:	2039C50409DBDBCB63BE1864CE6C110B8E9E27387208C1BA4797E9AB7308DF96
SHA-512:	B9DA71565AECA8D212FA590F3ED8388A256963335FCE2ED8912A5676DD844DA8657372C8F9348175218256DAB4DB16CD1EEC9C7A5ACD5E518D4725E1220C61 3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://prod.msocdn.com/images/backgrounds/image1.jpg
Preview:	......JFIF.....`.`.....C................%.....- ".%5/874/43;BUH;?P?34JdKPWZ_`_9Ghog\nU]_[...C.......+..+[=4=[[......Y...."..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\jquery-3.3.1.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	86927
Entropy (8bit):	5.289226719276158
Encrypted:	false
SSDEEP:	1536:jLiBdiaWLOczCmZx6+VWuGzQNOzdn6x2RZd9SEnk9HB96c9Yo/NWLbVj3kC6t3:5kn6x2xe9NK6nC69
MD5:	A09E13EE94D51C524B7E2A728C7D4039
SHA1:	0DC32DB4AA9C5F03F3B38C47D883DBD4FED13AAE
SHA-256:	160A426FF2894252CD7CEBBDD6D6B7DA8FCD319C65B70468F10B6690C45D02EF
SHA-512:	F8DA8F95B6ED33542A88AF19028E18AE3D9CE25350A06BFC3FBF433ED2B38FEFA5E639CDDFDAC703FC6CAA7F3313D974B92A3168276B3A016CEB28F27DB07 4A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ajax.aspnetcdn.com/ajax/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.hasOwnProperty ,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\PSUEOSZZ\list_bullet_5x5[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 5 x 8
Category:	downloaded
Size (bytes):	48
Entropy (8bit):	4.0692356777594165
Encrypted:	false
SSDEEP:	3:CJpqpwxlClM3j:dpDM3j
MD5:	E0024553CEA3C0E88604FB35D4E3BFE5
SHA1:	5B70B84AF0EB07F4571D6C47268B261055309D0C
SHA-256:	087E9648D868FDBF885A0268763C6AAF2BEE042DAA6559ED12B3EBD0F477F460
SHA-512:	C059D7BDAC4D33925FFD35456F4C1A37DB8E04BAF5F03E6E20D5C799A71F701460F891CADB024E12A6B054174B1FE211CACAF6EF8F6FC42D05D68FEFFD1A0 2F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://prod.msocdn.com/Images/list_bullet_5x5.gif
Preview:	GIF89a...........].!.......,...................;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\mscorlib[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):	24942
Entropy (8bit):	5.213985584208541

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\mscorlib[1].js	
Encrypted:	false
SSDEEP:	384:H3xbuOg4kiHaATrphVIVXxvz0uvcIUwBnAw1Lmbfoi+H9JT59gpHb:HtXnaAphSxhz0uvc2BnAbf9+HfTgRb
MD5:	4542D764783C82BD784326FB357F0C62
SHA1:	FC5619DAD451C77794AB8759C404D3233F5FA1A8
SHA-256:	965993B2B2C5B69E0AAF3C76372CC5D1494E638C79AF67F2FEFA0AECF67572A1
SHA-512:	51A469D84B7064CA03259E443C776FB208168AE4240F76553331F806F5D9A11BD3B55D5B5BA8257BBF66CD7116CB5B4AACA1E1754AD96656FB011E297E1CC70
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://prod.msocdn.com/2021.1.28.2/en-US/JS/mscorlib.js
Preview:	(function(){function f(t){n?n.push(t):setTimeout(t,0)}function i(){var i,t,r;if(n)for(i=n,n=null,t=0,r=i.length;t<r;t++)i[t]()}var u={version:"0.7.2.0",isUndefined:function(n){return n===undefined},isNull:function(n){return n===null},isNullOrUndefined:function(n){return n===null||n===undefined},isValue:function(n){return n!==null&&n!==undefined}},e=!1,n=[],t,r;document.addEventListener?document.readyState=="complete"?i():document.addEventListener("DOMContentLoaded",i,!1):window.attachEvent&&window.attachEvent("onload",function(){i()}),t=window.ss,t||(window.ss=t={init:f,ready:f});for(r in u)t[r]=u[r]})(),Object.__typeName="Object",Object.__baseType=null,Object.clearKeys=function(n){for(var t in n)delete n[t]},Object.keyExists=function(n,t){return n[t]!==undefined},Object.keys?Object.getKeyCount=function(n){return Object.keys(n).length}:(Object.keys=function(n){var t=[],i;for(i in n)t.push(i);return t},Object.getKeyCount=function(n){var t=0,i;for(i in n)t++;return t}),Boolean.__typeName

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\o365_gallatin_logo[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 162 x 46, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	6081
Entropy (8bit):	7.931174059511865
Encrypted:	false
SSDEEP:	96:CllcHitlIxv9vk7C1+I4wWHLihk/xlBepCYaLqKeI5CD65XzqztfRMnZv8opIkyL:pIIHUCD4wa1ekYaLqKeE5Xmzn4uopIkE
MD5:	79920DBF8491B1C6BDC101ACEBF8DDA0
SHA1:	935A7EE1A7265FC27C674F225E023A0DA9D93FDC
SHA-256:	5A8D21C9A6A6850C6DC4F328A98167E48258597A8D2B4ED7257CE3794F974E12
SHA-512:	61BF48137252ADF01C490B18E4C625AEC7B79801250FCC8F54044B57601CE8B13C0FFF06EB3FF0EFEA44B58CB6D3579F68734BA7EEE18F26B808B608D4A554EB
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://prod.msocdn.com/shell/images/o365_gallatin_logo.png
Preview:	.PNG.....IHDR.....pHYs.....o.d...MiCCPPhotoshop ICC profile..x.SwX...>..e.VB..l.."#....Y....a...@...V....HU...H...(.gA..Z.U\8....}z.....y.....&..j.9R.<:...OH.....H.....g.....yx~t.?...o...p..$.....P&W. ..."....R...T.....S.d.....ly\|B"....I>.....(G$.@..`U.R,.....@"....Y.2G.....v.X..@`...B,.. 8..C.... L..0.._p..H.....K.3.....w....!..l.Ba.).f.."...#.H..L.....8?.....f.l....k.o">!.....N...._....p...u.k.[..V.h..]3...Z..z..y8.@...P.<.....%b..0.>.3.o..~..@...z..q.@.....qanv.R....B1n..#.....)..4.\,...X..P"M.y.R.D!.....2.....w....O.N....l.~...X.v.@~.-.....g42y.....@+.....\...L....D..*.A.....a.D@.$.<.B.....A.T.:.....18....\..p..`.....A...a!:..b.."....."aH4... ..Q"..r...Bj.]H#.-r.9.\@.... 2....G1...Q...u@.....s.t4.]..k....=.....K.ut.}..c..1.f..a\..E`.X.&..c.X5V.5c.X7v....a..$.....^...I...GXLXC.%.#....W...1.'"..O.%z...xb:..XF.&.!.!.%^'.._.H$...N.!%.2I.IkH.H-.S.>..i.L&.m.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\pagelayout_mos_background_left[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.02, aspect ratio, density 100x100, segment length 16, baseline, precision 8, 14x493, frames 3
Category:	downloaded
Size (bytes):	1445
Entropy (8bit):	7.3505082081877235
Encrypted:	false
SSDEEP:	24:EShItJf5i9oFWWCPKyuQrpphoTumOvSeqYBXDdKHe4qe:EBtmoFjCPKyzrfhoTuAeJBzQH0e
MD5:	D1C2F3A69333665062F624843EE095AC
SHA1:	792FD6AE744C4CAEE41330CFAFCE2DA7D8566370
SHA-256:	DEF703FF9A3024077FCADF10A40BEDB185AF87D201DB648D0733CA6F21BCDC64
SHA-512:	86F9910D89141ECC91DDA369D89983414CE426F338ED70E024D955C6841E8B6359BD28C2F290B8A39B86F126D499812AB1120360314615719FC4CD79C706F915
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://prod.msocdn.com/Shell/Images/pagelayout_mos_background_left.jpg
Preview:	......JFIF.....d.d.....Ducky.....d.....Adobe.d.....Qa..!..1A....q..."S2b..R#3c.....!1.Qa2.Aq.".#....R..C.....?... ...?_h>.k.z.C.....?_h>.i.5....G...]...+v.O..s..g.MJ..ek:Y.'...On.....=W..t.j\.@=...~..%{p..z.....d...-..".q.....u.....Z...T..tU...:..T...Q.S...../.....+7..]....:....u..:...8q.....m}..9~[....K....s.>.....?l...Y...-.y.....TjQM]h.q...I.r.tu*....`.....]z..{sc#.._.....\6u.`.]]9u.J.4uA..r.w..J...L._g^9...4....YWj.u<.R...}!..U..g.a...Ib..d..[D.LE.._..W.h.%.....<.j$..$3I..3..&.....I.....G5Y5.*1..D2...UMa..~(!..]..%.kh.]..$.i....y&".29*.Z..H-DdqU.k.H."28..M!..S.!...EYF...J$.....HBE%.D.Ud...I..+...}K....#..5.R..5r.....BqZx.o1..`....~.E.6..x.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\pagelayout_mos_background_right[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.02, aspect ratio, density 100x100, segment length 16, baseline, precision 8, 14x493, frames 3
Category:	downloaded
Size (bytes):	1444
Entropy (8bit):	7.383016953278326
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\pagelayout_mos_background_right[1].jpg	
SSDEEP:	24:ES2DrYR3VKJmJ7XZN4kP8lT4OU/yh0g5zDGbX8mxAN7rPOa0SoBG8:EzYRgJQpN90l/D2eDVeAN7LdoI8
MD5:	548272F0B8A2D3C0E5075AEF077C055D
SHA1:	03577CD960CDA29F1293CC6DD2717DCD4FA7476A
SHA-256:	543F554F8A38070D4BC60D0C180EACD0561451C8DD03876630261B7F1ABF7FD8
SHA-512:	2B261EC4C5DF25923B6EB025CE6099962BFD342F4D87C4FCA30A69DC1C8343FA8DA65FF805127F56BD7FC3A9D090208E64B292CBB59E3BF37B3D8FC50B11EF C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://prod.msocdn.com/Shell/Images/pagelayout_mos_background_right.jpg
Preview:	......JFIF.....d.d......Ducky.......d......Adobe.d.. ....!Qa1...A..."2..q..b..BS....Rr3.$.......................!1Qa..A."...R...q#.............?.........?.....a.\|O...C.....>.P{...\|.......T.........o.........&..?{(x.7.?4..1..c(...\....... Lg..\|.o....+.\:......\.4Z...[[...............N.....6~x_.....U.Z....y-.w....A..G.[..N..,.w.....:../.D........c.m.['..x/.F.......\|.o.F..m..x.....^.u7[..7..?.p+:.Q..5s....8{bq_o...k6.Yjg.&.....w....GO........\...~ .3~..d.w.....ZK.M_9......z..B.:cN......E.N....e..d.Q.r...g....RX.Bm.6..M.m.<y.n.;......M.9.<.U.5...REY....S&.....*Bc.R.!1.."....d....oI..L3.Rk.L3.A...t..I.D.t.$...E;M*'.6.....LtATFc..F...4.! ....i.LsOH.Fc..e.B..PIB....F...%.D.*d.....Gb..........n.....Tp............}\.M~...............c.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\pagelayout_nav_highlight[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.02, aspect ratio, density 100x100, segment length 16, baseline, precision 8, 2x22, frames 3
Category:	downloaded
Size (bytes):	358
Entropy (8bit):	3.97325990896992
Encrypted:	false
SSDEEP:	6:3ll7QzDkmIWmM1//RklRlzsXemlVS8AqOzL3:VqDk/MSWjAqcz
MD5:	97C03A5E680C961CD18DD0C048784C26
SHA1:	0AA771C6CE74FA593565DFACB3AF406FDC378CB7
SHA-256:	6FC479441003A973BE28DBAB8A89BE8D9A82FF932077850E34601F5C8FAD5CF3
SHA-512:	6B92B3859CF082981A55B86766AA126D22B9867E33803545E5B205ED59C695FA48B89D511286289BC543BF753B0C30F94359C58549070CA108DC681AEF924FDA
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://prod.msocdn.com/Shell/Images/pagelayout_nav_highlight.jpg
Preview:	......JFIF.....d.d......Ducky.......d......Adobe.d..d...................................... ..........................R...S.......................Q................?......3.o.!p.$........ {VP......

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\pagelayout_white_panel[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 14x1200, frames 3
Category:	downloaded
Size (bytes):	962
Entropy (8bit):	6.125053602347189
Encrypted:	false
SSDEEP:	24:M9YMWb9o0XxDuLHeOWXG4OZ7DAJuLHenX3u3:M9YMBuERAc
MD5:	04B62B22952990D6D698FB030F4A3BA5
SHA1:	EDD318DE1E1356DA6EDB43A1127453BD8CDE037A
SHA-256:	941AFBD0047A84F7205EFABC6884F3C6762DA3033263111E4761695CB91E7423
SHA-512:	F26232102C14E881E368EAF51F88860D39B9839251C5E583F4E6AF649AFA1DDADA8E12D7FCD26226F8B0E1D92A9AE19A8B453952789F09E75C673FC162C06A76
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://prod.msocdn.com/Shell/Images/pagelayout_white_panel.jpg
Preview:	......JFIF.....`.`......Ducky.......d......Adobe.d........C.................................. $.' ",#..(7),01444.'9=82<.342...C...........2!.!222222222222222222222222222222222222222 2222222222222..........."...}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz......................... ....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz................. ....?...(... (...(..?..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\reporting[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):	14200
Entropy (8bit):	5.216559889928471
Encrypted:	false
SSDEEP:	384:HH8plriujltva099S9QFLcTTERzl6ThXIh+zfgeh3iz5Wa:HHnuPv1Dl69eEYehSz5Wa
MD5:	C83815695A9DDF5A158F8A0999D9B789
SHA1:	1C9BE85A1322756BAD087C960BB7F71518CEDBEE
SHA-256:	E1FFB8A7DE8F113F1CFDE124558410B62E1941BCBAF255BD4629CC54DFB144A5

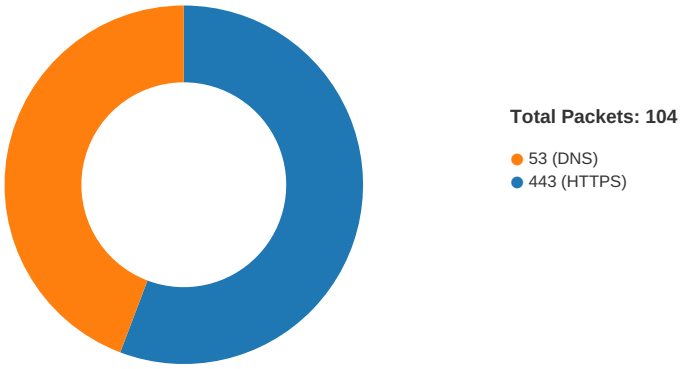
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\reporting[1].js	
SHA-512:	6DB8D753A6584342007CA98516B44B47220843EB96B6042EC6F11A9DE5796F4E7A037ECAF330DABCC8AE368A3DA1C037D9B7B0B23AB7C47D8D2A12326E19B16
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://prod.msocdn.com/2021.1.28.2/en-US/js/reporting.js
Preview:	var Reporting={};Reporting.MainChartImgId=null,Reporting.AlertErrorMessageDivId=null,Reporting.DivMoreReportsLinkId=null,Reporting.GeneralChartErrorMessage=null,Reporting.ServiceId=null,Reporting.CategoryId=null,Reporting.ReportIds=[],Reporting.Titles=[],Reporting.Descriptions=[],Reporting.CurrentSelectedThumbnailId=null,Reporting.ThumbnailImgIDs=null,Reporting.TableViewContainerDivId=null,Reporting.DataItemNotAvailableTexts=null,Reporting.Loading=function(){Reporting.MainChartAreaLoading(),Reporting.LoadedAdvanceFilter(Reporting.ServiceId,Reporting.CategoryId,Reporting.MainChartImgId),Reporting.LoadedTable(Reporting.ServiceId,Reporting.CategoryId,Reporting.MainChartImgId),Reporting.SideChartsAreaLoading(null)},Reporting.HandleLoaded=function(n,t,i,r){$('#'+t).show(),r=="1"?($('#'+n).attr('status','complete').attr('error','false'),Reporting.MainChartAreaLoaded(i)):($('#'+n).attr('status','complete').hide(),$('#divSpinner_'+i).show(),Reporting.SideChartsAreaLoaded()),PageLayout.ResizePa

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 5, 2021 08:10:07.403109074 CET	49702	443	192.168.2.3	152.199.23.37
Feb 5, 2021 08:10:07.404068947 CET	49703	443	192.168.2.3	152.199.23.37
Feb 5, 2021 08:10:07.440967083 CET	443	49702	152.199.23.37	192.168.2.3
Feb 5, 2021 08:10:07.441072941 CET	49702	443	192.168.2.3	152.199.23.37
Feb 5, 2021 08:10:07.441606998 CET	49702	443	192.168.2.3	152.199.23.37
Feb 5, 2021 08:10:07.441709995 CET	443	49703	152.199.23.37	192.168.2.3
Feb 5, 2021 08:10:07.441809893 CET	49703	443	192.168.2.3	152.199.23.37
Feb 5, 2021 08:10:07.442244053 CET	49703	443	192.168.2.3	152.199.23.37
Feb 5, 2021 08:10:07.479298115 CET	443	49702	152.199.23.37	192.168.2.3
Feb 5, 2021 08:10:07.479967117 CET	443	49703	152.199.23.37	192.168.2.3
Feb 5, 2021 08:10:07.480176926 CET	443	49702	152.199.23.37	192.168.2.3
Feb 5, 2021 08:10:07.480220079 CET	443	49702	152.199.23.37	192.168.2.3
Feb 5, 2021 08:10:07.480257034 CET	443	49702	152.199.23.37	192.168.2.3
Feb 5, 2021 08:10:07.480278015 CET	49702	443	192.168.2.3	152.199.23.37
Feb 5, 2021 08:10:07.480285883 CET	443	49702	152.199.23.37	192.168.2.3
Feb 5, 2021 08:10:07.480325937 CET	49702	443	192.168.2.3	152.199.23.37
Feb 5, 2021 08:10:07.480333090 CET	49702	443	192.168.2.3	152.199.23.37
Feb 5, 2021 08:10:07.480338097 CET	49702	443	192.168.2.3	152.199.23.37

Copyright null 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 5, 2021 08:10:07.480923891 CET	443	49703	152.199.23.37	192.168.2.3
Feb 5, 2021 08:10:07.480973959 CET	443	49703	152.199.23.37	192.168.2.3
Feb 5, 2021 08:10:07.480989933 CET	49703	443	192.168.2.3	152.199.23.37
Feb 5, 2021 08:10:07.481019020 CET	443	49703	152.199.23.37	192.168.2.3
Feb 5, 2021 08:10:07.481033087 CET	49703	443	192.168.2.3	152.199.23.37
Feb 5, 2021 08:10:07.481046915 CET	443	49703	152.199.23.37	192.168.2.3
Feb 5, 2021 08:10:07.481069088 CET	49703	443	192.168.2.3	152.199.23.37
Feb 5, 2021 08:10:07.481075048 CET	443	49703	152.199.23.37	192.168.2.3
Feb 5, 2021 08:10:07.481093884 CET	49703	443	192.168.2.3	152.199.23.37
Feb 5, 2021 08:10:07.481123924 CET	49703	443	192.168.2.3	152.199.23.37
Feb 5, 2021 08:10:07.487701893 CET	49703	443	192.168.2.3	152.199.23.37
Feb 5, 2021 08:10:07.487884998 CET	49702	443	192.168.2.3	152.199.23.37
Feb 5, 2021 08:10:07.488159895 CET	49703	443	192.168.2.3	152.199.23.37
Feb 5, 2021 08:10:07.488318920 CET	49703	443	192.168.2.3	152.199.23.37
Feb 5, 2021 08:10:07.488437891 CET	49703	443	192.168.2.3	152.199.23.37
Feb 5, 2021 08:10:07.488500118 CET	49702	443	192.168.2.3	152.199.23.37
Feb 5, 2021 08:10:07.525496006 CET	443	49703	152.199.23.37	192.168.2.3
Feb 5, 2021 08:10:07.525528908 CET	443	49703	152.199.23.37	192.168.2.3
Feb 5, 2021 08:10:07.525579929 CET	49703	443	192.168.2.3	152.199.23.37
Feb 5, 2021 08:10:07.525615931 CET	49703	443	192.168.2.3	152.199.23.37
Feb 5, 2021 08:10:07.525660992 CET	443	49702	152.199.23.37	192.168.2.3
Feb 5, 2021 08:10:07.525691986 CET	443	49702	152.199.23.37	192.168.2.3
Feb 5, 2021 08:10:07.525717974 CET	443	49703	152.199.23.37	192.168.2.3
Feb 5, 2021 08:10:07.525737047 CET	49702	443	192.168.2.3	152.199.23.37
Feb 5, 2021 08:10:07.525753021 CET	49702	443	192.168.2.3	152.199.23.37
Feb 5, 2021 08:10:07.525782108 CET	49703	443	192.168.2.3	152.199.23.37
Feb 5, 2021 08:10:07.526041985 CET	443	49702	152.199.23.37	192.168.2.3
Feb 5, 2021 08:10:07.526099920 CET	49702	443	192.168.2.3	152.199.23.37
Feb 5, 2021 08:10:07.526406050 CET	443	49703	152.199.23.37	192.168.2.3
Feb 5, 2021 08:10:07.529850006 CET	443	49703	152.199.23.37	192.168.2.3
Feb 5, 2021 08:10:07.529894114 CET	49703	443	192.168.2.3	152.199.23.37
Feb 5, 2021 08:10:07.530028105 CET	443	49703	152.199.23.37	192.168.2.3
Feb 5, 2021 08:10:07.530092001 CET	49703	443	192.168.2.3	152.199.23.37
Feb 5, 2021 08:10:07.532035112 CET	49703	443	192.168.2.3	152.199.23.37
Feb 5, 2021 08:10:07.533454895 CET	49702	443	192.168.2.3	152.199.23.37
Feb 5, 2021 08:10:07.611062050 CET	443	49703	152.199.23.37	192.168.2.3
Feb 5, 2021 08:10:07.611283064 CET	443	49702	152.199.23.37	192.168.2.3
Feb 5, 2021 08:10:08.781018972 CET	49703	443	192.168.2.3	152.199.23.37
Feb 5, 2021 08:10:08.818958998 CET	443	49703	152.199.23.37	192.168.2.3
Feb 5, 2021 08:10:08.820183992 CET	443	49703	152.199.23.37	192.168.2.3
Feb 5, 2021 08:10:08.820291996 CET	49703	443	192.168.2.3	152.199.23.37
Feb 5, 2021 08:10:11.780276060 CET	49719	443	192.168.2.3	52.97.250.242
Feb 5, 2021 08:10:11.780493975 CET	49720	443	192.168.2.3	52.97.250.242
Feb 5, 2021 08:10:11.824387074 CET	443	49719	52.97.250.242	192.168.2.3
Feb 5, 2021 08:10:11.824438095 CET	443	49720	52.97.250.242	192.168.2.3
Feb 5, 2021 08:10:11.824596882 CET	49719	443	192.168.2.3	52.97.250.242
Feb 5, 2021 08:10:11.824645042 CET	49720	443	192.168.2.3	52.97.250.242
Feb 5, 2021 08:10:11.825838089 CET	49720	443	192.168.2.3	52.97.250.242
Feb 5, 2021 08:10:11.826301098 CET	49719	443	192.168.2.3	52.97.250.242
Feb 5, 2021 08:10:11.870543003 CET	443	49720	52.97.250.242	192.168.2.3
Feb 5, 2021 08:10:11.870588064 CET	443	49720	52.97.250.242	192.168.2.3
Feb 5, 2021 08:10:11.870629072 CET	443	49720	52.97.250.242	192.168.2.3
Feb 5, 2021 08:10:11.870717049 CET	49720	443	192.168.2.3	52.97.250.242
Feb 5, 2021 08:10:11.870831013 CET	443	49719	52.97.250.242	192.168.2.3
Feb 5, 2021 08:10:11.870867968 CET	443	49719	52.97.250.242	192.168.2.3
Feb 5, 2021 08:10:11.870872974 CET	49720	443	192.168.2.3	52.97.250.242
Feb 5, 2021 08:10:11.870915890 CET	443	49719	52.97.250.242	192.168.2.3
Feb 5, 2021 08:10:11.870986938 CET	49719	443	192.168.2.3	52.97.250.242
Feb 5, 2021 08:10:11.871038914 CET	49719	443	192.168.2.3	52.97.250.242
Feb 5, 2021 08:10:11.889779091 CET	49719	443	192.168.2.3	52.97.250.242
Feb 5, 2021 08:10:11.889977932 CET	49720	443	192.168.2.3	52.97.250.242
Feb 5, 2021 08:10:11.890582085 CET	49719	443	192.168.2.3	52.97.250.242
Feb 5, 2021 08:10:11.934374094 CET	443	49719	52.97.250.242	192.168.2.3
Feb 5, 2021 08:10:11.934545040 CET	443	49719	52.97.250.242	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 5, 2021 08:10:11.934710979 CET	443	49720	52.97.250.242	192.168.2.3
Feb 5, 2021 08:10:11.934827089 CET	49719	443	192.168.2.3	52.97.250.242
Feb 5, 2021 08:10:11.934947014 CET	49720	443	192.168.2.3	52.97.250.242
Feb 5, 2021 08:10:11.940269947 CET	443	49719	52.97.250.242	192.168.2.3
Feb 5, 2021 08:10:11.940310001 CET	443	49719	52.97.250.242	192.168.2.3
Feb 5, 2021 08:10:11.940340042 CET	443	49719	52.97.250.242	192.168.2.3
Feb 5, 2021 08:10:11.940407038 CET	49719	443	192.168.2.3	52.97.250.242
Feb 5, 2021 08:10:11.940489054 CET	49719	443	192.168.2.3	52.97.250.242
Feb 5, 2021 08:10:27.897830009 CET	49728	443	192.168.2.3	152.199.21.175
Feb 5, 2021 08:10:27.898612022 CET	49729	443	192.168.2.3	152.199.21.175
Feb 5, 2021 08:10:27.899308920 CET	49730	443	192.168.2.3	152.199.21.175
Feb 5, 2021 08:10:27.900033951 CET	49731	443	192.168.2.3	152.199.21.175
Feb 5, 2021 08:10:27.901024103 CET	49732	443	192.168.2.3	152.199.21.175
Feb 5, 2021 08:10:27.901853085 CET	49733	443	192.168.2.3	152.199.21.175
Feb 5, 2021 08:10:27.935764074 CET	443	49728	152.199.21.175	192.168.2.3
Feb 5, 2021 08:10:27.936005116 CET	49728	443	192.168.2.3	152.199.21.175
Feb 5, 2021 08:10:27.936214924 CET	443	49729	152.199.21.175	192.168.2.3
Feb 5, 2021 08:10:27.936315060 CET	49729	443	192.168.2.3	152.199.21.175

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 5, 2021 08:10:00.428750038 CET	60985	53	192.168.2.3	8.8.8.8
Feb 5, 2021 08:10:00.474503040 CET	53	60985	8.8.8.8	192.168.2.3
Feb 5, 2021 08:10:01.239511967 CET	50200	53	192.168.2.3	8.8.8.8
Feb 5, 2021 08:10:01.285624981 CET	53	50200	8.8.8.8	192.168.2.3
Feb 5, 2021 08:10:02.169176102 CET	51281	53	192.168.2.3	8.8.8.8
Feb 5, 2021 08:10:02.217761040 CET	53	51281	8.8.8.8	192.168.2.3
Feb 5, 2021 08:10:03.261465073 CET	49199	53	192.168.2.3	8.8.8.8
Feb 5, 2021 08:10:03.307430983 CET	53	49199	8.8.8.8	192.168.2.3
Feb 5, 2021 08:10:05.805584908 CET	50620	53	192.168.2.3	8.8.8.8
Feb 5, 2021 08:10:05.865209103 CET	53	50620	8.8.8.8	192.168.2.3
Feb 5, 2021 08:10:06.194051027 CET	64938	53	192.168.2.3	8.8.8.8
Feb 5, 2021 08:10:06.248266935 CET	53	64938	8.8.8.8	192.168.2.3
Feb 5, 2021 08:10:06.899844885 CET	60152	53	192.168.2.3	8.8.8.8
Feb 5, 2021 08:10:06.957181931 CET	53	60152	8.8.8.8	192.168.2.3
Feb 5, 2021 08:10:07.168133974 CET	57544	53	192.168.2.3	8.8.8.8
Feb 5, 2021 08:10:07.214205027 CET	53	57544	8.8.8.8	192.168.2.3
Feb 5, 2021 08:10:07.330593109 CET	55984	53	192.168.2.3	8.8.8.8
Feb 5, 2021 08:10:07.345014095 CET	64185	53	192.168.2.3	8.8.8.8
Feb 5, 2021 08:10:07.355663061 CET	65110	53	192.168.2.3	8.8.8.8
Feb 5, 2021 08:10:07.391937971 CET	53	55984	8.8.8.8	192.168.2.3
Feb 5, 2021 08:10:07.401617050 CET	53	64185	8.8.8.8	192.168.2.3
Feb 5, 2021 08:10:07.414972067 CET	53	65110	8.8.8.8	192.168.2.3
Feb 5, 2021 08:10:08.185141087 CET	58361	53	192.168.2.3	8.8.8.8
Feb 5, 2021 08:10:08.253019094 CET	53	58361	8.8.8.8	192.168.2.3
Feb 5, 2021 08:10:08.565447092 CET	63492	53	192.168.2.3	8.8.8.8
Feb 5, 2021 08:10:08.611310959 CET	53	63492	8.8.8.8	192.168.2.3
Feb 5, 2021 08:10:08.774686098 CET	60831	53	192.168.2.3	8.8.8.8
Feb 5, 2021 08:10:08.830410957 CET	53	60831	8.8.8.8	192.168.2.3
Feb 5, 2021 08:10:10.592588902 CET	60100	53	192.168.2.3	8.8.8.8
Feb 5, 2021 08:10:10.639857054 CET	53	60100	8.8.8.8	192.168.2.3
Feb 5, 2021 08:10:11.423183918 CET	53195	53	192.168.2.3	8.8.8.8
Feb 5, 2021 08:10:11.468247890 CET	50141	53	192.168.2.3	8.8.8.8
Feb 5, 2021 08:10:11.468966961 CET	53	53195	8.8.8.8	192.168.2.3
Feb 5, 2021 08:10:11.514054060 CET	53	50141	8.8.8.8	192.168.2.3
Feb 5, 2021 08:10:11.728693008 CET	53023	53	192.168.2.3	8.8.8.8
Feb 5, 2021 08:10:11.777076006 CET	53	53023	8.8.8.8	192.168.2.3
Feb 5, 2021 08:10:11.965456963 CET	49563	53	192.168.2.3	8.8.8.8
Feb 5, 2021 08:10:12.022640944 CET	53	49563	8.8.8.8	192.168.2.3
Feb 5, 2021 08:10:23.339262962 CET	51352	53	192.168.2.3	8.8.8.8
Feb 5, 2021 08:10:23.397706032 CET	53	51352	8.8.8.8	192.168.2.3
Feb 5, 2021 08:10:25.596612930 CET	59349	53	192.168.2.3	8.8.8.8
Feb 5, 2021 08:10:25.608531952 CET	57084	53	192.168.2.3	8.8.8.8

Copyright null 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 5, 2021 08:10:25.655293941 CET	53	59349	8.8.8.8	192.168.2.3
Feb 5, 2021 08:10:25.655759096 CET	53	57084	8.8.8.8	192.168.2.3
Feb 5, 2021 08:10:25.661562920 CET	58823	53	192.168.2.3	8.8.8.8
Feb 5, 2021 08:10:25.715740919 CET	53	58823	8.8.8.8	192.168.2.3
Feb 5, 2021 08:10:25.975199938 CET	57568	53	192.168.2.3	8.8.8.8
Feb 5, 2021 08:10:26.050416946 CET	53	57568	8.8.8.8	192.168.2.3
Feb 5, 2021 08:10:27.836867094 CET	50540	53	192.168.2.3	8.8.8.8
Feb 5, 2021 08:10:27.896348000 CET	53	50540	8.8.8.8	192.168.2.3
Feb 5, 2021 08:10:30.361295938 CET	54366	53	192.168.2.3	8.8.8.8
Feb 5, 2021 08:10:30.418406963 CET	53	54366	8.8.8.8	192.168.2.3
Feb 5, 2021 08:10:31.554537058 CET	53034	53	192.168.2.3	8.8.8.8
Feb 5, 2021 08:10:31.611934900 CET	53	53034	8.8.8.8	192.168.2.3
Feb 5, 2021 08:10:33.491322994 CET	57762	53	192.168.2.3	8.8.8.8
Feb 5, 2021 08:10:33.546890020 CET	53	57762	8.8.8.8	192.168.2.3
Feb 5, 2021 08:10:33.722245932 CET	55435	53	192.168.2.3	8.8.8.8
Feb 5, 2021 08:10:33.779962063 CET	53	55435	8.8.8.8	192.168.2.3
Feb 5, 2021 08:10:34.817063093 CET	50713	53	192.168.2.3	8.8.8.8
Feb 5, 2021 08:10:34.825160980 CET	56132	53	192.168.2.3	8.8.8.8
Feb 5, 2021 08:10:34.862633944 CET	58987	53	192.168.2.3	8.8.8.8
Feb 5, 2021 08:10:34.872684956 CET	53	50713	8.8.8.8	192.168.2.3
Feb 5, 2021 08:10:34.884542942 CET	53	56132	8.8.8.8	192.168.2.3
Feb 5, 2021 08:10:34.920648098 CET	53	58987	8.8.8.8	192.168.2.3
Feb 5, 2021 08:10:35.002290010 CET	56579	53	192.168.2.3	8.8.8.8
Feb 5, 2021 08:10:35.057780027 CET	53	56579	8.8.8.8	192.168.2.3
Feb 5, 2021 08:10:35.800249100 CET	60633	53	192.168.2.3	8.8.8.8
Feb 5, 2021 08:10:35.854572058 CET	53	60633	8.8.8.8	192.168.2.3
Feb 5, 2021 08:10:36.528753042 CET	61292	53	192.168.2.3	8.8.8.8
Feb 5, 2021 08:10:36.586060047 CET	53	61292	8.8.8.8	192.168.2.3
Feb 5, 2021 08:10:36.812241077 CET	60633	53	192.168.2.3	8.8.8.8
Feb 5, 2021 08:10:36.859666109 CET	53	60633	8.8.8.8	192.168.2.3
Feb 5, 2021 08:10:37.298377037 CET	63619	53	192.168.2.3	8.8.8.8
Feb 5, 2021 08:10:37.356467009 CET	53	63619	8.8.8.8	192.168.2.3
Feb 5, 2021 08:10:37.527842045 CET	61292	53	192.168.2.3	8.8.8.8
Feb 5, 2021 08:10:37.584755898 CET	53	61292	8.8.8.8	192.168.2.3
Feb 5, 2021 08:10:37.824199915 CET	60633	53	192.168.2.3	8.8.8.8
Feb 5, 2021 08:10:37.869960070 CET	53	60633	8.8.8.8	192.168.2.3
Feb 5, 2021 08:10:38.010914087 CET	64938	53	192.168.2.3	8.8.8.8
Feb 5, 2021 08:10:38.066756964 CET	53	64938	8.8.8.8	192.168.2.3
Feb 5, 2021 08:10:38.523471117 CET	61946	53	192.168.2.3	8.8.8.8
Feb 5, 2021 08:10:38.527551889 CET	61292	53	192.168.2.3	8.8.8.8
Feb 5, 2021 08:10:38.585860014 CET	53	61946	8.8.8.8	192.168.2.3
Feb 5, 2021 08:10:38.587800980 CET	53	61292	8.8.8.8	192.168.2.3
Feb 5, 2021 08:10:39.830982924 CET	60633	53	192.168.2.3	8.8.8.8
Feb 5, 2021 08:10:39.885535955 CET	53	60633	8.8.8.8	192.168.2.3
Feb 5, 2021 08:10:40.532761097 CET	61292	53	192.168.2.3	8.8.8.8
Feb 5, 2021 08:10:40.590045929 CET	53	61292	8.8.8.8	192.168.2.3
Feb 5, 2021 08:10:43.845472097 CET	60633	53	192.168.2.3	8.8.8.8
Feb 5, 2021 08:10:43.900089025 CET	53	60633	8.8.8.8	192.168.2.3
Feb 5, 2021 08:10:44.548612118 CET	61292	53	192.168.2.3	8.8.8.8
Feb 5, 2021 08:10:44.606973886 CET	53	61292	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 5, 2021 08:10:06.899844885 CET	192.168.2.3	8.8.8.8	0x543d	Standard query (0)	zauthxcovidtestinnt0kajxktkatak0jtt0a0jnkowauath.fra1.cdn.digitaloceanspaces.com	A (IP address)	IN (0x0001)
Feb 5, 2021 08:10:07.330593109 CET	192.168.2.3	8.8.8.8	0xecef	Standard query (0)	secure.aadcdn.microsoftonline-p.com	A (IP address)	IN (0x0001)
Feb 5, 2021 08:10:07.345014095 CET	192.168.2.3	8.8.8.8	0x697e	Standard query (0)	aadcdn.msftauth.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 5, 2021 08:10:07.355663061 CET	192.168.2.3	8.8.8.8	0x449f	Standard query (0)	ajax.aspnetcdn.com	A (IP address)	IN (0x0001)
Feb 5, 2021 08:10:08.185141087 CET	192.168.2.3	8.8.8.8	0x9dba	Standard query (0)	portal.microsoftonline.com	A (IP address)	IN (0x0001)
Feb 5, 2021 08:10:08.774686098 CET	192.168.2.3	8.8.8.8	0xcc51	Standard query (0)	prod.msocdn.com	A (IP address)	IN (0x0001)
Feb 5, 2021 08:10:11.468247890 CET	192.168.2.3	8.8.8.8	0xcf0a	Standard query (0)	www.office.com	A (IP address)	IN (0x0001)
Feb 5, 2021 08:10:11.728693008 CET	192.168.2.3	8.8.8.8	0x17b2	Standard query (0)	outlook.office365.com	A (IP address)	IN (0x0001)
Feb 5, 2021 08:10:11.965456963 CET	192.168.2.3	8.8.8.8	0xa12b	Standard query (0)	r4.res.office365.com	A (IP address)	IN (0x0001)
Feb 5, 2021 08:10:23.339262962 CET	192.168.2.3	8.8.8.8	0x372b	Standard query (0)	secure.aadcdn.microsoftonline-p.com	A (IP address)	IN (0x0001)
Feb 5, 2021 08:10:25.596612930 CET	192.168.2.3	8.8.8.8	0x11e3	Standard query (0)	clientlog.portal.office.com	A (IP address)	IN (0x0001)
Feb 5, 2021 08:10:25.661562920 CET	192.168.2.3	8.8.8.8	0xb0f1	Standard query (0)	clientlog.portal.office.com	A (IP address)	IN (0x0001)
Feb 5, 2021 08:10:25.975199938 CET	192.168.2.3	8.8.8.8	0xd9f0	Standard query (0)	signup.live.com	A (IP address)	IN (0x0001)
Feb 5, 2021 08:10:27.836867094 CET	192.168.2.3	8.8.8.8	0x79e6	Standard query (0)	acctcdn.msauth.net	A (IP address)	IN (0x0001)
Feb 5, 2021 08:10:31.554537058 CET	192.168.2.3	8.8.8.8	0x7b1b	Standard query (0)	account.live.com	A (IP address)	IN (0x0001)
Feb 5, 2021 08:10:38.010914087 CET	192.168.2.3	8.8.8.8	0x5206	Standard query (0)	assets.onestore.ms	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 5, 2021 08:10:06.957181931 CET	8.8.8.8	192.168.2.3	0x543d	No error (0)	zauthxcovidtestinnt0kajxktkatak0jtt0a0jnkowauath.fra1.cdn.digitaloceanspaces.com	cds.b5g9b8e4.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Feb 5, 2021 08:10:07.391937971 CET	8.8.8.8	192.168.2.3	0xecef	No error (0)	secure.aadcdn.microsoftonline-p.com	secure.aadcdn.microsoftonline-p.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Feb 5, 2021 08:10:07.401617050 CET	8.8.8.8	192.168.2.3	0x697e	No error (0)	aadcdn.msftauth.net	aadcdnoriginneu.azureedge.net		CNAME (Canonical name)	IN (0x0001)
Feb 5, 2021 08:10:07.401617050 CET	8.8.8.8	192.168.2.3	0x697e	No error (0)	cs1100.wpc.omegacdn.net		152.199.23.37	A (IP address)	IN (0x0001)
Feb 5, 2021 08:10:07.414972067 CET	8.8.8.8	192.168.2.3	0x449f	No error (0)	ajax.aspnetcdn.com	mscomajax.vo.msecnd.net		CNAME (Canonical name)	IN (0x0001)
Feb 5, 2021 08:10:08.253019094 CET	8.8.8.8	192.168.2.3	0x9dba	No error (0)	portal.microsoftonline.com	geo.portal.microsoftonline.akadns.net		CNAME (Canonical name)	IN (0x0001)
Feb 5, 2021 08:10:08.830410957 CET	8.8.8.8	192.168.2.3	0xcc51	No error (0)	prod.msocdn.com	wildcard.msocdn.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Feb 5, 2021 08:10:11.514054060 CET	8.8.8.8	192.168.2.3	0xcf0a	No error (0)	www.office.com	home-portal.office.com		CNAME (Canonical name)	IN (0x0001)
Feb 5, 2021 08:10:11.514054060 CET	8.8.8.8	192.168.2.3	0xcf0a	No error (0)	home-portal.office.com	home-office365-com.b-0004.b-msedge.net		CNAME (Canonical name)	IN (0x0001)
Feb 5, 2021 08:10:11.777076006 CET	8.8.8.8	192.168.2.3	0x17b2	No error (0)	outlook.office365.com	outlook.ha.office365.com		CNAME (Canonical name)	IN (0x0001)
Feb 5, 2021 08:10:11.777076006 CET	8.8.8.8	192.168.2.3	0x17b2	No error (0)	outlook.ha.office365.com	outlook.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Feb 5, 2021 08:10:11.777076006 CET	8.8.8.8	192.168.2.3	0x17b2	No error (0)	outlook.ms-acdc.office.com	FRA-efz.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Feb 5, 2021 08:10:11.777076006 CET	8.8.8.8	192.168.2.3	0x17b2	No error (0)	FRA-efz.ms-acdc.office.com		52.97.250.242	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 5, 2021 08:10:11.777076006 CET	8.8.8.8	192.168.2.3	0x17b2	No error (0)	FRA-efz.ms-acdc.office.com		52.97.135.114	A (IP address)	IN (0x0001)
Feb 5, 2021 08:10:11.777076006 CET	8.8.8.8	192.168.2.3	0x17b2	No error (0)	FRA-efz.ms-acdc.office.com		40.101.80.194	A (IP address)	IN (0x0001)
Feb 5, 2021 08:10:12.022640944 CET	8.8.8.8	192.168.2.3	0xa12b	No error (0)	r4.res.office365.com	r4.res.office365.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Feb 5, 2021 08:10:23.397706032 CET	8.8.8.8	192.168.2.3	0x372b	No error (0)	secure.aadcdn.microsoftonline-p.com	secure.aadcdn.microsoftonline-p.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Feb 5, 2021 08:10:25.655293941 CET	8.8.8.8	192.168.2.3	0x11e3	Name error (3)	clientlog.portal.office.com	none	none	A (IP address)	IN (0x0001)
Feb 5, 2021 08:10:25.655759096 CET	8.8.8.8	192.168.2.3	0xed	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Feb 5, 2021 08:10:25.715740919 CET	8.8.8.8	192.168.2.3	0xb0f1	Name error (3)	clientlog.portal.office.com	none	none	A (IP address)	IN (0x0001)
Feb 5, 2021 08:10:26.050416946 CET	8.8.8.8	192.168.2.3	0xd9f0	No error (0)	signup.live.com	account.msa.msidentity.com		CNAME (Canonical name)	IN (0x0001)
Feb 5, 2021 08:10:26.050416946 CET	8.8.8.8	192.168.2.3	0xd9f0	No error (0)	account.msa.msidentity.com	account.msa.akadns6.net		CNAME (Canonical name)	IN (0x0001)
Feb 5, 2021 08:10:27.896348000 CET	8.8.8.8	192.168.2.3	0x79e6	No error (0)	acctcdn.msauth.net	acctcdn.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Feb 5, 2021 08:10:27.896348000 CET	8.8.8.8	192.168.2.3	0x79e6	No error (0)	scdn1efff.wpc.9da5e.alphacdn.net	sni1gl.wpc.alphacdn.net		CNAME (Canonical name)	IN (0x0001)
Feb 5, 2021 08:10:27.896348000 CET	8.8.8.8	192.168.2.3	0x79e6	No error (0)	sni1gl.wpc.alphacdn.net		152.199.21.175	A (IP address)	IN (0x0001)
Feb 5, 2021 08:10:31.611934900 CET	8.8.8.8	192.168.2.3	0x7b1b	No error (0)	account.live.com	account.msa.msidentity.com		CNAME (Canonical name)	IN (0x0001)
Feb 5, 2021 08:10:31.611934900 CET	8.8.8.8	192.168.2.3	0x7b1b	No error (0)	account.msa.msidentity.com	account.msa.akadns6.net		CNAME (Canonical name)	IN (0x0001)
Feb 5, 2021 08:10:34.920648098 CET	8.8.8.8	192.168.2.3	0x3362	No error (0)	consentdeliveryfd.azurefd.net	star-azurefd-prod.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Feb 5, 2021 08:10:38.066756964 CET	8.8.8.8	192.168.2.3	0x5206	No error (0)	assets.onestore.ms	assets.onestore.ms.akadns.net		CNAME (Canonical name)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 5, 2021 08:10:07.480257034 CET	152.199.23.37	443	192.168.2.3	49702	CN=aadcdn.msftauth.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	Thu Jul 09 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013 Fri Nov 10 01:00:00 CET 2006	Fri Jul 09 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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 5, 2021 08:10:07.481019020 CET	152.199.23.37	443	192.168.2.3	49703	CN=aadcdn.msftauth.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	Thu Jul 09 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013 Fri Nov 10 01:00:00 CET 2006	Fri Jul 09 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 5, 2021 08:10:28.028099060 CET	152.199.21.175	443	192.168.2.3	49733	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 SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Sun Jan 03 01:00:00 CET 2021 Fri Mar 08 13:00:00 CET 2013	Mon Jan 03 00:59:59 CET 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 5, 2021 08:10:28.028323889 CET	152.199.21.175	443	192.168.2.3	49732	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 SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Sun Jan 03 01:00:00 CET 2021 Fri Mar 08 13:00:00 CET 2013	Mon Jan 03 00:59:59 CET 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 5, 2021 08:10:28.029805899 CET	152.199.21.175	443	192.168.2.3	49731	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 SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Sun Jan 03 01:00:00 CET 2021 Fri Mar 08 13:00:00 CET 2013	Mon Jan 03 00:59:59 CET 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 5, 2021 08:10:28.031860113 CET	152.199.21.175	443	192.168.2.3	49729	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 SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Sun Jan 03 01:00:00 CET 2021 Fri Mar 08 13:00:00 CET 2013	Mon Jan 03 00:59:59 CET 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

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		
Feb 5, 2021 08:10:28.037930012 CET	152.199.21.175	443	192.168.2.3	49730	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 SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Sun Jan 03 01:00:00 CET 2021 Fri Mar 08 13:00:00 CET 2013	Mon Jan 03 00:59:59 CET 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 5, 2021 08:10:28.037972927 CET	152.199.21.175	443	192.168.2.3	49728	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 SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Sun Jan 03 01:00:00 CET 2021 Fri Mar 08 13:00:00 CET 2013	Mon Jan 03 00:59:59 CET 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: iexplore.exe PID: 5204 Parent PID: 792

General

Start time:	08:10:05
Start date:	05/02/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff6703b0000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: iexplore.exe PID: 1740 Parent PID: 5204

General

Start time:	08:10:05
Start date:	05/02/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5204 CREDAT:17410 /prefetch:2
Imagebase:	0xf70000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly