ID: 385276
Sample Name:
RemitSwift119353 xlsx.htm
Cookbook: default.jbs
Time: 09:29:49
Date: 12/04/2021
Version: 31.0.0 Emerald

Table of Contents

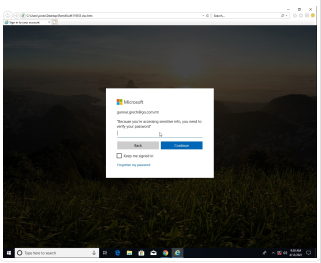
Analysis Report RemitSwift119353 xlsx.htm

Overview

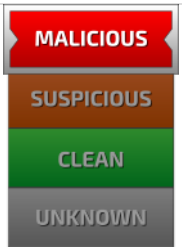
General Information

Sample Name:	RemitSwift119353 xlsx.htm
Analysis ID:	385276
MD5:	ca3a56c1d6eebe..
SHA1:	72d5d6ef29bd345.
SHA256:	3a6422545bcba4..
Infos:	

Most interesting Screenshot:



Detection



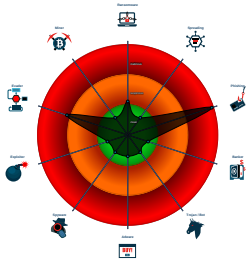
HTMLPhisher

Score:	88
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Phishing site detected (based on fav…
- Yara detected HtmlPhish10
- Yara detected HtmlPhish14
- Yara detected obfuscated html page
- Obfuscated HTML file found
- Phishing site detected (based on log…
- HTML title does not match URL
- IP address seen in connection with o…
- JA3 SSL client fingerprint seen in co…
- None HTTPS page querying sensitiv…
- Suspicious form URL found

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 6780 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6860 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6780 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

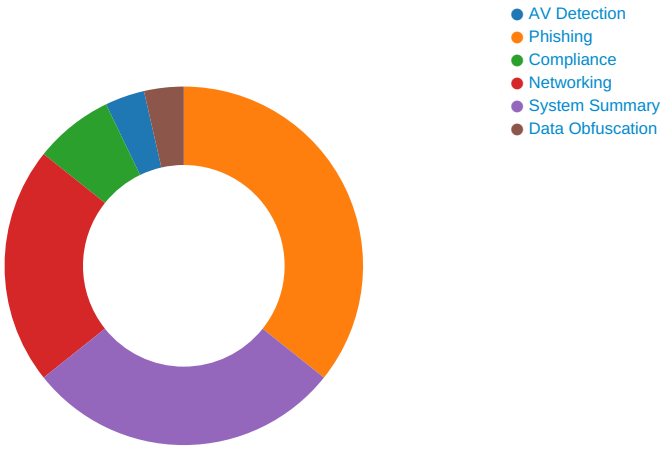
Initial Sample

Source	Rule	Description	Author	Strings
RemitSwift119353 xlsx.htm	JoeSecurity_Obshtml	Yara detected obfuscated html page	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Phishing:

Phishing site detected (based on favicon image match)

Yara detected HtmlPhish10

Yara detected HtmlPhish14

Yara detected obfuscated html page

Phishing site detected (based on logo template match)

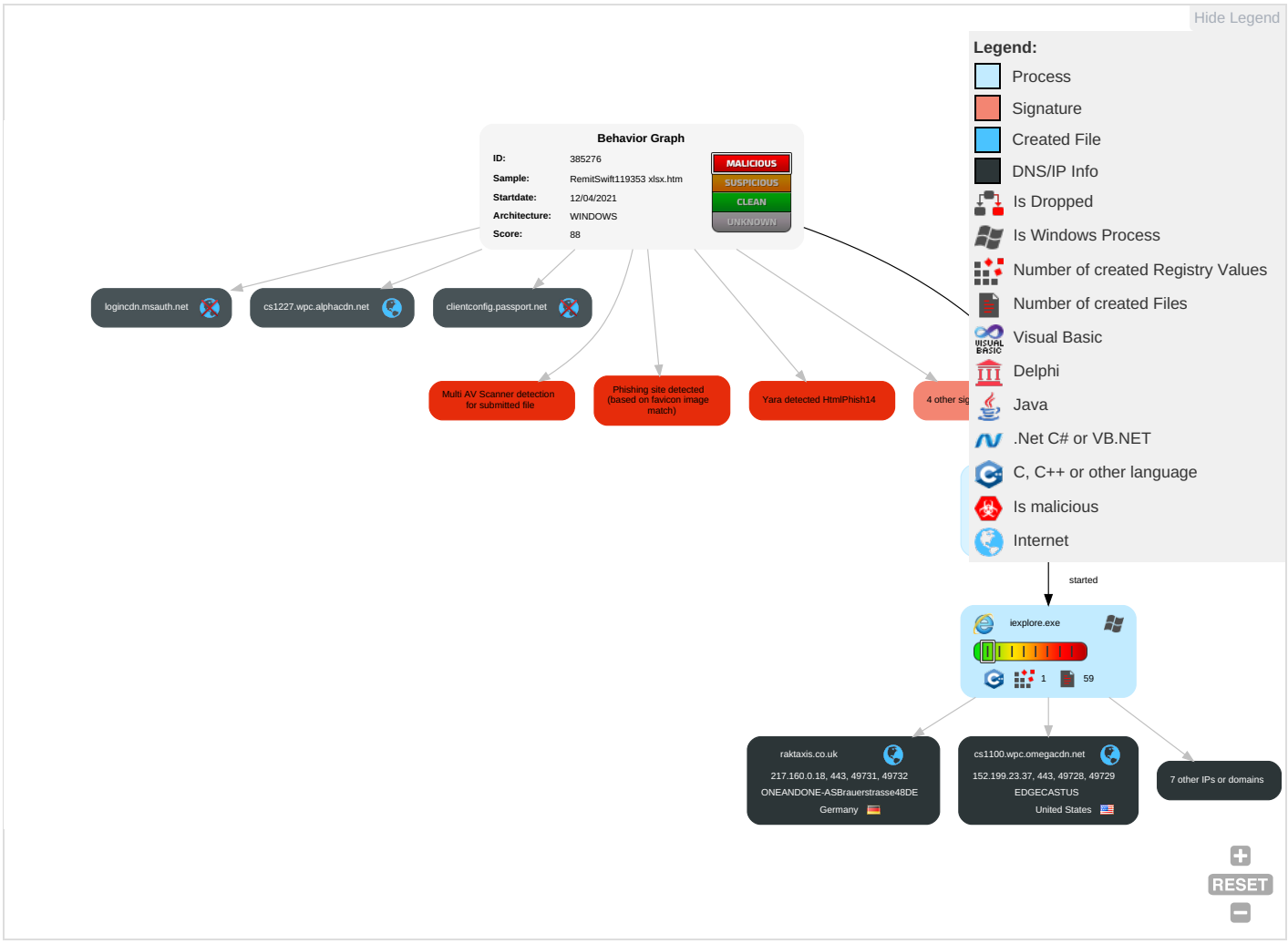
Data Obfuscation:

Obfuscated HTML file found

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impac
Valid Accounts	Scripting 1	Path Interception	Process Injection 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	Modify Syster Partiti
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	Device Lockou
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	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrie Billing Fraud

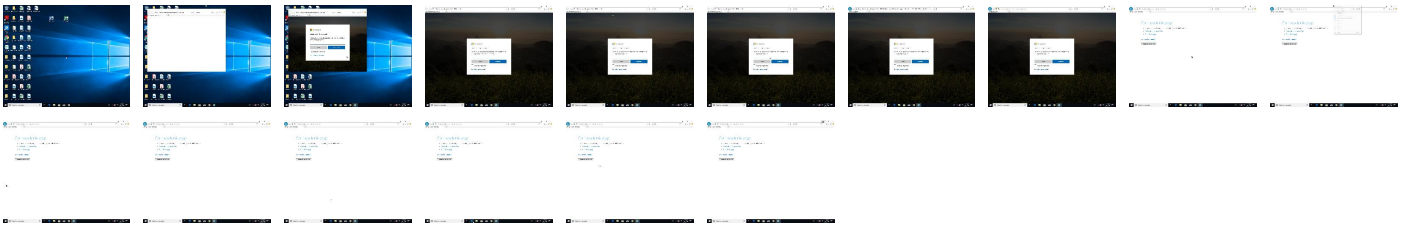
Behavior Graph

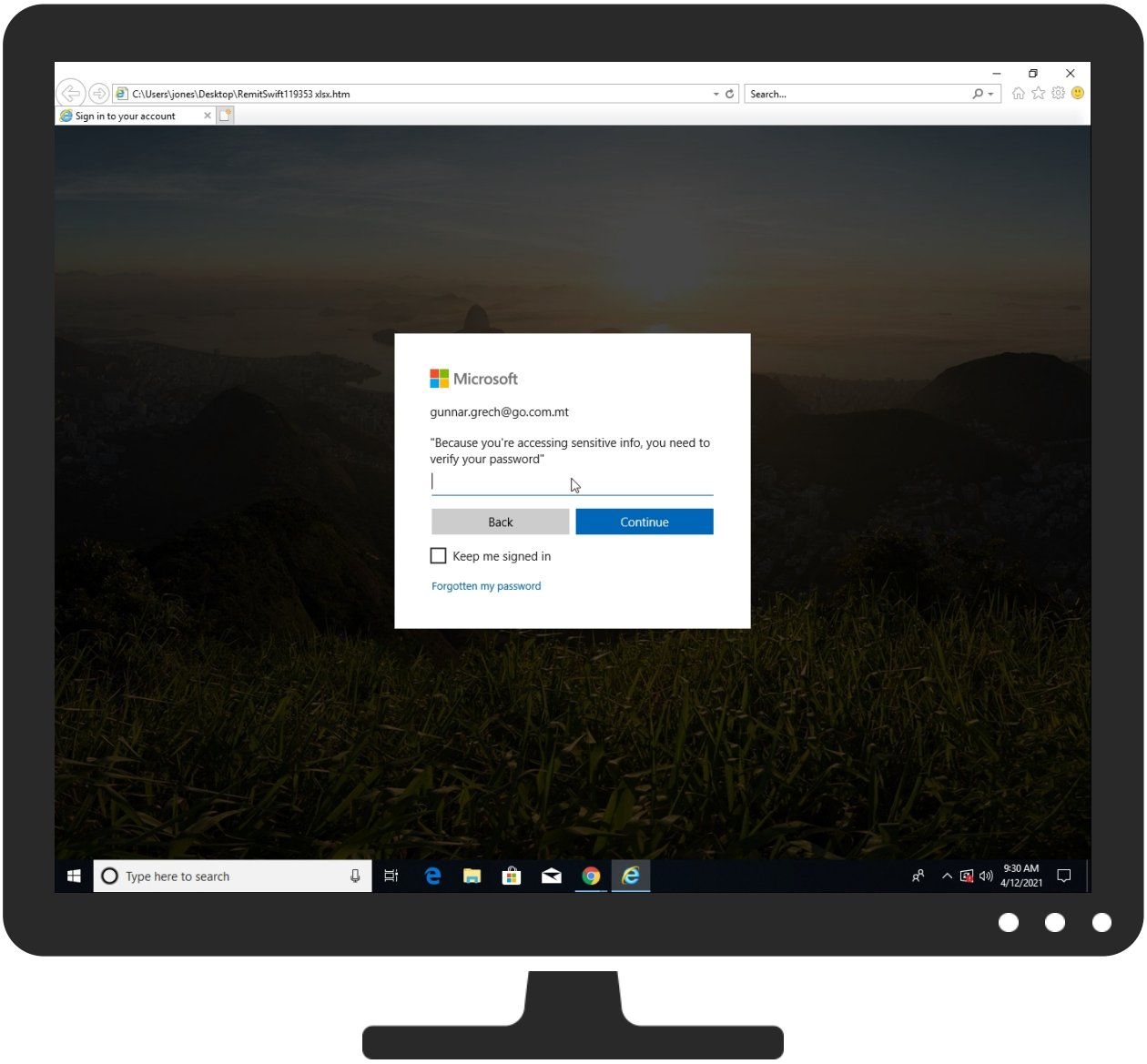


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
RemitSwift119353 xlsx.htm	20%	Virustotal		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
cs1227.wpc.alphacdn.net	0%	Virustotal		Browse
raktaxis.co.uk	2%	Virustotal		Browse
logincdn.msauth.net	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://privacy.micros	0%	URL Reputation	safe	
http://https://privacy.micros	0%	URL Reputation	safe	
http://https://privacy.micros	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://privacy.microsoft./en-GB/privacystatementsx.htm?rand=13InboxLightaspxn.1774256418&fid.4.1252	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
cs1227.wpc.alphacdn.net	192.229.221.185	true	false	• 0%, Virustotal, Browse	unknown
raktaxis.co.uk	217.160.0.18	true	false	• 2%, Virustotal, Browse	unknown
logincdn.msauth.net	unknown	unknown	false	• 1%, Virustotal, Browse	unknown
clientconfig.passport.net	unknown	unknown	false		unknown
aadcdn.msftauth.net	unknown	unknown	false		unknown
ajax.aspnetcdn.com	unknown	unknown	false		high
privacy.microsoft	unknown	unknown	false		unknown

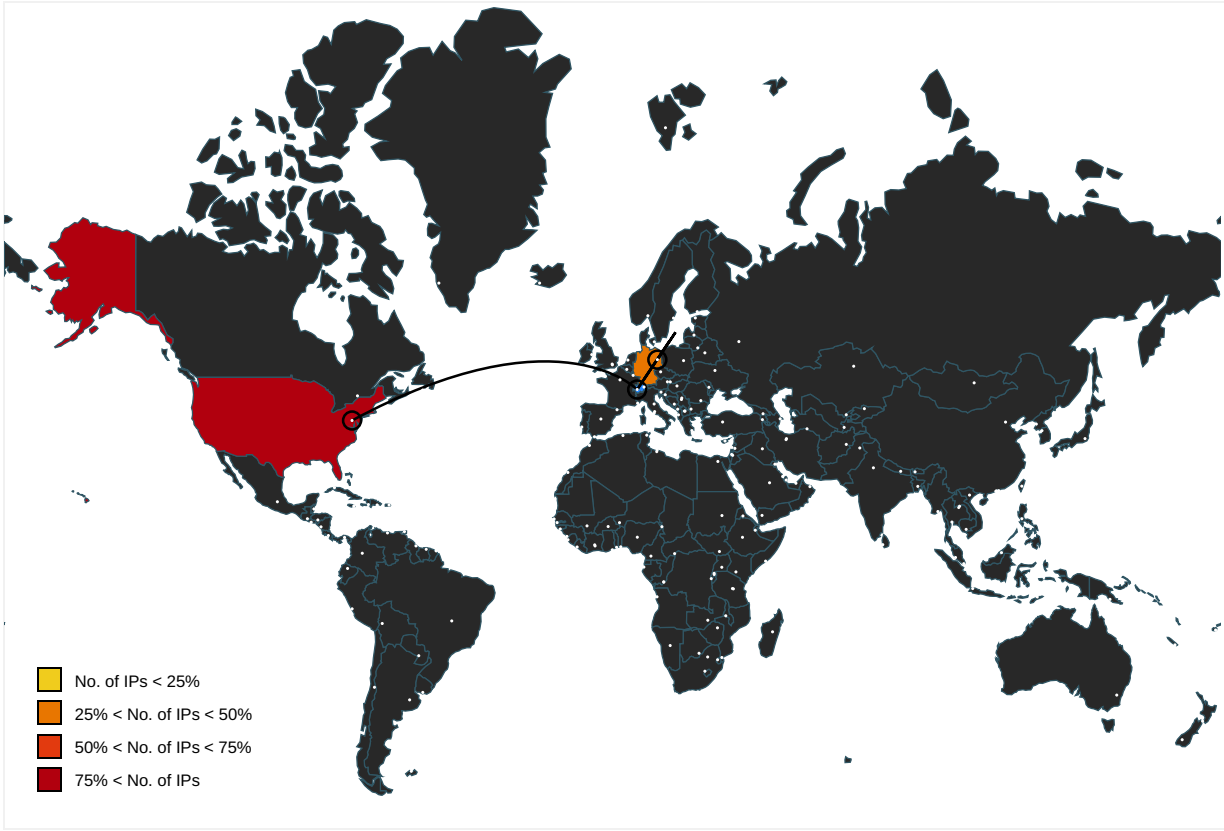
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
file:///C:/Users/user/Desktop/RemitSwift119353%20xlsx.htm?rand=13InboxLightaspxn.1774256418&fid.4.1252899642&fid=1&fav.1&rand.13InboxLight.aspxn.1774256418&fid.1252899642&fid.1&fav.1&email=gunnar.grech@go.com.mt&loginpage=&.rand=13InboxLight.aspx?n=1774256418&fid=4	true		low
file:///C:/Users/user/Desktop/RemitSwift119353%20xlsx.htm	true		low
http://https://privacy.microsoft./en-GB/privacystatement	true		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.skype.com/go/store.reactivate.credit	servicesagreement[1].htm.3.dr	false		high
http://https://www.skype.com/go/allrates	servicesagreement[1].htm.3.dr	false		high
http://https://aka.ms/redeemrewards	servicesagreement[1].htm.3.dr	false		high
http://https://ec.europa.eu/consumers/odr	servicesagreement[1].htm.3.dr	false		high
http://https://www.skype.com/go/legal.broadcast	servicesagreement[1].htm.3.dr	false		high
http://https://www.xbox.com/xbox-game-studios	servicesagreement[1].htm.3.dr	false		high
http://https://www.xbox.com/xbox-game-studios)	servicesagreement[1].htm.3.dr	false		high
http://https://privacy.micros	{FB42B5C1-9B60-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.skype.com/go/legal	servicesagreement[1].htm.3.dr	false		high
http://https://privacy.microsoft./en-GB/privacystatement	~DF21D4BF00FAEEC794.TMP.1.dr	false		unknown
http://https://www.microsoft.	{FB42B5C1-9B60-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.skype.com/go/emergency	servicesagreement[1].htm.3.dr	false		high
http://https://ec.europa.eu/consumers/odr);	servicesagreement[1].htm.3.dr	false		high
http://https://www.skype.com/go/emergency/	servicesagreement[1].htm.3.dr	false		high
http://github.com/requirejs/almond/LICENSE	17-f90ef1[1].js.3.dr	false		high
http://https://privacy.microsoft./en-GB/privacystatementsx.htm?rand=13InboxLightaspxn.1774256418&fid.4.1252	~DF21D4BF00FAEEC794.TMP.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://mixer.com/contact	servicesagreement[1].htm.3.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
217.160.0.18	raktaxis.co.uk	Germany		8560	ONEANDONE-ASBrauerstrasse48DE	false
192.229.221.185	cs1227.wpc.alphacdn.net	United States		15133	EDGECASTUS	false
152.199.23.37	cs1100.wpc.omegacdn.net	United States		15133	EDGECASTUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	385276
Start date:	12.04.2021
Start time:	09:29:49
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 33s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	RemitSwift119353 xlsx.htm
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	17
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0

Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal88.phis.evad.winHTM@3/31@9/4
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .htm • Browsing link: file:///C:/Users/user/Desktop/RemitSwift119353%20xlsx.htm?rand=13InboxLightaspxn.1774256418&fid.4.1252899642&fid=1&fav.1&rand.13InboxLight.aspxn.1774256418&fid.1252899642&fid.1&fav.1&email=gunnar.grech@go.com.mt&loginpage=&.rand=13InboxLight.aspx?n=1774256418&fid=4 • Browsing link: https://www.microsoft.com/en-GB/servicesagreement/ • Browsing link: https://privacy.microsoft./en-GB/privacystatement

Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 92.123.150.225, 52.255.188.83, 104.43.139.144, 104.42.151.234, 88.221.62.148, 13.64.90.137, 92.122.145.53, 92.122.213.194, 92.122.213.240, 152.199.19.160, 13.107.253.19, 184.30.25.170, 92.122.213.247, 20.82.210.154, 152.199.19.161, 40.88.32.150, 2.20.142.209, 2.20.142.210, 104.43.193.48, 20.82.209.183, 52.155.217.156, 20.54.26.129 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, e13678.dscb.akamaiedge.net, a1945.g2.akamai.net, e13551.dscg.akamaiedge.net, e11290.dspg.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, www.microsoft.com-c-3.edgekey.net, audownload.windowsupdate.nsatc.net, statics-marketingsites-eus-ms-com.akamaized.net, watson.telemetry.microsoft.com, au-bg-shim.trafficmanager.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, aadcdnoriginneu.azureedge.net, lgincdnvzeuno.ec.azureedge.net, skypedataprdcolcus16.cloudapp.net, c-s.cms.ms.akadns.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, lgincdn.trafficmanager.net, blobcollector.events.data.trafficmanager.net, t-0009.fb-t-msedge.net, c.s-microsoft.com-c.edgekey.net, cs9.wpc.v0cdn.net, au.download.windowsupdate.com.edgesuite.net, a1449.dscg2.akamai.net, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, www.microsoft.com-c-3.edgekey.net.globalredir.akadns.net, iecvlist.microsoft.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, msagfx.live.com-6.edgekey.net, authgfx.msa.akadns6.net, go.microsoft.com, mscomajax.vo.msecnd.net, dual.t-0009.t-msedge.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, consumerrp-displaycatalog-aks2eap.md.mp.microsoft.com.akadns.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, cs22.wpc.v0cdn.net, ie9comview.vo.msecnd.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, firstparty-azurefd-prod.trafficmanager.net, aadcdnoriginneu.ec.azureedge.net, lgincdnvzeuno.azureedge.net, skypedataprdcoleus17.cloudapp.net, c.s-microsoft.com, go.microsoft.com.edgekey.net, e13678.dscg.akamaiedge.net, skypedataprdcolwus16.cloudapp.net, www.microsoft.com, displaycatalog-rp.md.mp.microsoft.com.akadns.net, wcpstatic.microsoft.com • Report size getting too big, too many NtDeviceIoControlFile calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
217.160.0.18	brett.moss SWIFT Copy 2021.htm	Get hash	malicious	Browse	
	martin.connor SWIFT Copy 2021.htm	Get hash	malicious	Browse	
	Bacs scott.grossman@ensono.com.htm	Get hash	malicious	Browse	
	Bacs scott.grossman@ensono.com.htm	Get hash	malicious	Browse	
	donotreply-tripplanne.htm	Get hash	malicious	Browse	
	deborah_hernandez@qhr.com.htm	Get hash	malicious	Browse	
	check.htm	Get hash	malicious	Browse	
	fdhfdh.htm	Get hash	malicious	Browse	
	Thursday, August 20, 2020#32215...wav.htm	Get hash	malicious	Browse	
	Voice 004 .hTm	Get hash	malicious	Browse	
	Voice 004 .hTm	Get hash	malicious	Browse	
	Voice 004 .hTm	Get hash	malicious	Browse	
	Voice 004 .hTm	Get hash	malicious	Browse	
	Voice 004 .hTm	Get hash	malicious	Browse	
	Voice 004 .hTm	Get hash	malicious	Browse	
	ghjhkutgyyhy.Html	Get hash	malicious	Browse	
	Voice 004 .hTm	Get hash	malicious	Browse	
	Voice 004 .hTm	Get hash	malicious	Browse	
	Voice 004 .hTm	Get hash	malicious	Browse	
	kareemg@mashreq.com Payment .hTM	Get hash	malicious	Browse	
192.229.221.185	scan_715.htm	Get hash	malicious	Browse	
	securedmessage.htm	Get hash	malicious	Browse	
	Friday, April 2nd, 2021, 20210402062906.8CE1B73ADE2A192C@compassionarmy.com.htm	Get hash	malicious	Browse	
	#Ud83d#Udcde.htm.htm	Get hash	malicious	Browse	
	brett.moss SWIFT Copy 2021.htm	Get hash	malicious	Browse	
	martin.connor SWIFT Copy 2021.htm	Get hash	malicious	Browse	
	#Ufffd.HTML	Get hash	malicious	Browse	
	Keep password file foryyy .htm	Get hash	malicious	Browse	
	ATT31834.htm	Get hash	malicious	Browse	
	Bacs scott.grossman@ensono.com.htm	Get hash	malicious	Browse	
	Bacs scott.grossman@ensono.com.htm	Get hash	malicious	Browse	
	ATT00900.htm	Get hash	malicious	Browse	
	roccor-invoice-648133_xls.HtMl	Get hash	malicious	Browse	
	redwirespace-invoice-982323_xls.HtMl	Get hash	malicious	Browse	
	#Ud83d#Udccc Crtc Working Code .htm	Get hash	malicious	Browse	
	client confirmation.htm	Get hash	malicious	Browse	
	prismcosec-invoice-647718_xls.HtMl	Get hash	malicious	Browse	
	Purchase order.doc	Get hash	malicious	Browse	
	rightWWindow.dll	Get hash	malicious	Browse	
	borderLink.dll	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
cs1227.wpc.alphacdn.net	scan_715.htm	Get hash	malicious	Browse	• 192.229.221.185
	securedmessage.htm	Get hash	malicious	Browse	• 192.229.221.185
	Friday, April 2nd, 2021, 20210402062906.8CE1B73ADE2A192C@compassionarmy.com.htm	Get hash	malicious	Browse	• 192.229.221.185
	#Ud83d#Udcde.htm.htm	Get hash	malicious	Browse	• 192.229.221.185
	brett.moss SWIFT Copy 2021.htm	Get hash	malicious	Browse	• 192.229.221.185
	martin.connor SWIFT Copy 2021.htm	Get hash	malicious	Browse	• 192.229.221.185
	#Ufffd.HTML	Get hash	malicious	Browse	• 192.229.221.185

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Keep password file foryyy .htm	Get hash	malicious	Browse	• 192.229.221.185
	ATT31834.htm	Get hash	malicious	Browse	• 192.229.221.185
	Bacs scott.grossman@ensono.com.htm	Get hash	malicious	Browse	• 192.229.221.185
	Bacs scott.grossman@ensono.com.htm	Get hash	malicious	Browse	• 192.229.221.185
	ATT00900.htm	Get hash	malicious	Browse	• 192.229.221.185
	roccor-invoice-648133_xls.HtMl	Get hash	malicious	Browse	• 192.229.221.185
	redwirespace-invoice-982323_xls.HtMl	Get hash	malicious	Browse	• 192.229.221.185
	#Ud83d#Udccc Crtc Working Code .htm	Get hash	malicious	Browse	• 192.229.221.185
	client confirmation.htm	Get hash	malicious	Browse	• 192.229.221.185
	prismcosec-invoice-647718_xls.HtMl	Get hash	malicious	Browse	• 192.229.221.185
	Purchase order.doc	Get hash	malicious	Browse	• 192.229.221.185
	rightWWindow.dll	Get hash	malicious	Browse	• 192.229.221.185
	borderLink.dll	Get hash	malicious	Browse	• 192.229.221.185
cs1100.wpc.omegacdn.net	#Ud83d#Udcde973.htm	Get hash	malicious	Browse	• 152.199.23.37
	securedmessage.htm	Get hash	malicious	Browse	• 152.199.23.37
	Signed pages of agreement copy.html	Get hash	malicious	Browse	• 152.199.23.37
	Friday, April 2nd, 2021, 20210402062906.8CE1B73ADE2A192C@compassionarmy.com.htm	Get hash	malicious	Browse	• 152.199.23.37
	brett.moss SWIFT Copy 2021.htm	Get hash	malicious	Browse	• 152.199.23.37
	martin.connor SWIFT Copy 2021.htm	Get hash	malicious	Browse	• 152.199.23.37
	VM-(#Ud83d#Udcde)-- 19795.htm	Get hash	malicious	Browse	• 152.199.23.37
	Missed +443547900.wav - 45551 PM.htm.htm	Get hash	malicious	Browse	• 152.199.23.37
	#Ud83d#UdcdeMissed +60475998.wav - 82218 PM.htm	Get hash	malicious	Browse	• 152.199.23.37
	#Ud83d#UdcdeMissed +1957636658.wav - 63542 PM.htm.htm	Get hash	malicious	Browse	• 152.199.23.37
	OneNote.html	Get hash	malicious	Browse	• 152.199.23.37
	Bacs scott.grossman@ensono.com.htm	Get hash	malicious	Browse	• 152.199.23.37
	murexltd-Investment_265386-xlsx.html	Get hash	malicious	Browse	• 152.199.23.37
	Bacs scott.grossman@ensono.com.htm	Get hash	malicious	Browse	• 152.199.23.37
	sgs-Investment974041-xlsx.Html	Get hash	malicious	Browse	• 152.199.23.37
	roccor-invoice-648133_xls.HtMl	Get hash	malicious	Browse	• 152.199.23.37
	redwirespace-invoice-982323_xls.HtMl	Get hash	malicious	Browse	• 152.199.23.37
	prismcosec-invoice-647718_xls.HtMl	Get hash	malicious	Browse	• 152.199.23.37
	Purchase order.doc	Get hash	malicious	Browse	• 152.199.23.37
	Check4466.docx	Get hash	malicious	Browse	• 152.199.23.37

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ONEANDONE-ASBrauerstrasse48DE	Swift copy.pdf.exe	Get hash	malicious	Browse	• 74.208.236.87
	00000998880.exe	Get hash	malicious	Browse	• 74.208.5.2
	Payment advice IN18663Q0031139I.xlsx	Get hash	malicious	Browse	• 74.208.236.137
	cV1uaQeOGg.exe	Get hash	malicious	Browse	• 74.208.236.137
	JM0O99055.exe	Get hash	malicious	Browse	• 74.208.5.2
	829063701.tar	Get hash	malicious	Browse	• 212.227.15.142
	301085272.tar	Get hash	malicious	Browse	• 212.227.15.158
	HG546092227865431209.exe	Get hash	malicious	Browse	• 74.208.173.187
	Pe5KnG5wXy.dll	Get hash	malicious	Browse	• 82.223.21.211
	Pe5KnG5wXy.dll	Get hash	malicious	Browse	• 82.223.21.211
	bank transfer.exe	Get hash	malicious	Browse	• 217.160.0.160
	Szallitasi adatok.tar	Get hash	malicious	Browse	• 212.227.15.158
	mal5.exe	Get hash	malicious	Browse	• 74.208.5.15
	invoice.exe	Get hash	malicious	Browse	• 74.208.236.64
	PO7321.exe	Get hash	malicious	Browse	• 217.160.0.101
	BL01345678053567.exe	Get hash	malicious	Browse	• 74.208.236.134

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	A409043090.exe	Get hash	malicious	Browse	• 74.208.5.2
	Old9BZy7jO.dll	Get hash	malicious	Browse	• 82.223.21.211
	mULT14gGmy.dll	Get hash	malicious	Browse	• 82.223.21.211
	yWA1Ay0538.dll	Get hash	malicious	Browse	• 82.223.21.211
EDGECASTUS	scan_715.htm	Get hash	malicious	Browse	• 192.229.221.185
	#Ud83d#Udcde973.htm	Get hash	malicious	Browse	• 152.199.23.37
	Enclosed Updated Project Proposal From Robert Nilsson robert@lindstromundertak.se.html	Get hash	malicious	Browse	• 152.199.21.175
	securedmessage.htm	Get hash	malicious	Browse	• 152.199.23.37
	Signed pages of agreement copy.html	Get hash	malicious	Browse	• 152.199.23.37
	Receipt779G0D675432.html	Get hash	malicious	Browse	• 152.199.21.175
	PaymentAdvice-copy.htm	Get hash	malicious	Browse	• 152.199.21.35
	Friday, April 2nd, 2021, 20210402062906.8CE1B73ADE2A192C@compassionarmy.com.htm	Get hash	malicious	Browse	• 192.229.221.185
	#Ud83d#Udcde.htm.htm	Get hash	malicious	Browse	• 152.199.21.175
	ccavero@hycite.com.htm	Get hash	malicious	Browse	• 192.229.233.139
	brett.moss SWIFT Copy 2021.htm	Get hash	malicious	Browse	• 152.199.23.37
	martin.connor SWIFT Copy 2021.htm	Get hash	malicious	Browse	• 152.199.23.37
	#Ufffd.HTML	Get hash	malicious	Browse	• 192.229.221.185
	Keep password file foryyy .htm	Get hash	malicious	Browse	• 192.229.221.185
	VM-(#Ud83d#Udcde)-- 19795.htm	Get hash	malicious	Browse	• 152.199.23.37
	Missed +443547900.wav - 45551 PM.htm.htm	Get hash	malicious	Browse	• 152.199.23.37
	ATT31834.htm	Get hash	malicious	Browse	• 192.229.221.185
	Q lifesettlements INVOICE.htm	Get hash	malicious	Browse	• 152.199.21.175
	EU.exe	Get hash	malicious	Browse	• 152.199.21.175
	30250321.exe	Get hash	malicious	Browse	• 152.199.21.175

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
9e10692f1b7f78228b2d4e424db3a98c	Miral-Purushotham.verra.htm	Get hash	malicious	Browse	• 192.229.221.185 • 152.199.23.37
	IJht2pqbVh.exe	Get hash	malicious	Browse	• 192.229.221.185 • 152.199.23.37
	782kQ15aYm.dll	Get hash	malicious	Browse	• 192.229.221.185 • 152.199.23.37
	$108,459.00.html	Get hash	malicious	Browse	• 192.229.221.185 • 152.199.23.37
	Alexandra38.docx	Get hash	malicious	Browse	• 192.229.221.185 • 152.199.23.37
	Tmd7W7qwQw.dll	Get hash	malicious	Browse	• 192.229.221.185 • 152.199.23.37
	9R5WtLGEAy.dll	Get hash	malicious	Browse	• 192.229.221.185 • 152.199.23.37
	ghnrope2.dll	Get hash	malicious	Browse	• 192.229.221.185 • 152.199.23.37
	mail_6512365134_7863_202104108.html	Get hash	malicious	Browse	• 192.229.221.185 • 152.199.23.37
	mapdata.dll	Get hash	malicious	Browse	• 192.229.221.185 • 152.199.23.37
	#Ud83d#Udcde973.htm	Get hash	malicious	Browse	• 192.229.221.185 • 152.199.23.37
	#U266b SecuredMessage.htm	Get hash	malicious	Browse	• 192.229.221.185 • 152.199.23.37

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Offline_record_ON-035107.htm	Get hash	malicious	Browse	• 192.229.221.185 • 152.199.23.37
	Fax-Message-4564259.html	Get hash	malicious	Browse	• 192.229.221.185 • 152.199.23.37
	Enclosed Updated Project Proposal From Robert Nilsson robert@lindstromundertak.se.html	Get hash	malicious	Browse	• 192.229.221.185 • 152.199.23.37
	nicoleta.fagaras-DHL_TRACKING_1394942.html	Get hash	malicious	Browse	• 192.229.221.185 • 152.199.23.37
	Signed pages of agreement copy.html	Get hash	malicious	Browse	• 192.229.221.185 • 152.199.23.37
	ensono8639844766FAXMESSAGE.HTM	Get hash	malicious	Browse	• 192.229.221.185 • 152.199.23.37
	Payment Report.html	Get hash	malicious	Browse	• 192.229.221.185 • 152.199.23.37
	receipt-xxxx.htm	Get hash	malicious	Browse	• 192.229.221.185 • 152.199.23.37
37f463bf4616ecd445d4a1937da06e19	os9TZxfmTZ.exe	Get hash	malicious	Browse	• 192.229.221.185
	SWIFT Payment Advise 39 430-25.exe	Get hash	malicious	Browse	• 192.229.221.185
	malevolo.ps1	Get hash	malicious	Browse	• 192.229.221.185
	shipping document.exe	Get hash	malicious	Browse	• 192.229.221.185
	Statement-ID261179932209970.vbs	Get hash	malicious	Browse	• 192.229.221.185
	Alexandra38.docx	Get hash	malicious	Browse	• 192.229.221.185
	rRobw1VVRP.exe	Get hash	malicious	Browse	• 192.229.221.185
	Tmd7W7qwQw.dll	Get hash	malicious	Browse	• 192.229.221.185
	SecuriteInfo.com.Trojan.Agent.FFIJ.17175.exe	Get hash	malicious	Browse	• 192.229.221.185
	documents-351331057.xlsm	Get hash	malicious	Browse	• 192.229.221.185
	documents-1819557117.xlsm	Get hash	malicious	Browse	• 192.229.221.185
	mail_6512365134_7863_202104108.html	Get hash	malicious	Browse	• 192.229.221.185
	Copia bancaria de swift.exe	Get hash	malicious	Browse	• 192.229.221.185
	SecuriteInfo.com.Trojan.GenericKD.36659493.29456.exe	Get hash	malicious	Browse	• 192.229.221.185
	SecuriteInfo.com.Trojan.Siggen12.64197.30705.exe	Get hash	malicious	Browse	• 192.229.221.185
	#Ud83d#Udcde973.htm	Get hash	malicious	Browse	• 192.229.221.185
	3vQD6TIYA1.exe	Get hash	malicious	Browse	• 192.229.221.185
	SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.exe	Get hash	malicious	Browse	• 192.229.221.185
	XN123gfQJQ.exe	Get hash	malicious	Browse	• 192.229.221.185

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{FB42B5BF-9B60-11EB-90EB-ECF4BBEA1588}.dat

Process:	C:\Program Files\internet explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{FB42B5BF-9B60-11EB-90EB-ECF4BBEA1588}.dat	
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	33368
Entropy (8bit):	1.8739714500428286
Encrypted:	false
SSDEEP:	192:ruZWZa2zWCteif/8OzM32BqwDg2BmytI8Vj3:r6SZK6Piuhjdj
MD5:	C8C292B8B5BACD683D19368F82A787AD
SHA1:	8F0A62051DDC02FC24F034F0482C9AC78A371209
SHA-256:	C10510BF07209B830B7AF091739AC4DAF262515EBAE207AC66925917431CD22D
SHA-512:	F0EEF4917AC3B5E8BE707082AE84AE9BD373F5D3E1FEE15E5A02142667D74BF03456519061CFFBBFE231B622465469955D649C7C39C77F7D20D6360F5F5E1696
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\{FB42B5C1-9B60-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	93386
Entropy (8bit):	2.8400079188313447
Encrypted:	false
SSDEEP:	384:r8o3r2YsCtE1yYuXYpR/CVlWP7r/U+6HgsikN18HAFw/XR69sTJIYTd:y
MD5:	C68BCEB38918C073850B0D5276686055
SHA1:	CBED2EEB7A4BCF0823E8CD001D028B51EB5CA16A
SHA-256:	896D29B3A193C64B318A3C631823ECCA7306809E4B310537F230BCF2A90EAC1D
SHA-512:	2C6585B3B57EA16A935671C6A999DA2D661ACA265C6C07903CB0E2B95413D968741A61DF8355855A7E3AD1A88C4060B12D3199AB982CA632CF820BA3D301324
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\{FB42B5C2-9B60-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5667094986279155
Encrypted:	false
SSDEEP:	48:IwmGcpr6GwpabG4pQHGrapbSEGQpKKG7HpR5TGIpG:r6ZiQ96bBScAIT/A
MD5:	75B5A9AB3237E9F4EA3DD835B3215ECB
SHA1:	DEEB4698A9B3586AA6621F17D12EA60A2E4BB04C
SHA-256:	2654C17E3D013DDFCBF03E4C3B7309EF9F6208506F0AA3FCD897DCAC32327C99
SHA-512:	8680F574811916FE6019D710821D71F93C2CB1260C5DDCBFEF72965FDA8F37FFCCD1C2A3B2ADC36F2E06B89A816E03DE4A3223FA4EE7446F7225B2508CF501D
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\gee00pr\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	17876
Entropy (8bit):	3.032337724695834
Encrypted:	false
SSDEEP:	48:OAHAyAaAtgyyyyyyyyyyyy7ADWAGQQQQQV:CQQQQQV
MD5:	E558BD37414FAC6546092E271CB36450
SHA1:	D50CFF3D9E9CA962B89BA1F5A75F9F7EE83F4663

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\gee00pr\imagestore.dat	
SHA-256:	D8F2248353C1777FB8FC36B76173002F6495BF7F03D9710D00F71B10BF991D5A
SHA-512:	67B6C0B62BE5047901519868BBF5FCD0030E95994B14150EDA2850BBE928214D5E893660116CBEFF51C0345DEDA543B278825CABFC5ADED73C11D1C8754C53E
Malicious:	false
Reputation:	low
Preview:	%.h.t.t.p.s.:./.w.w.w...m.i.c.r.o.s.o.f.t...c.o.m./.f.a.v.i.c.o.n...i.c.o.~(.....h(.....(.....(.....P..... ...3333333333333333333333333333333"...3333333333333333333333333333333"...3333333333333333333333333333333"...3333333333333333333333333333333"...3333333333333333333333333333333"...3333333333333333333333333333333"...3333333333333333333333333333333"...3333333333333333333333333333333"...3333333333333333333333333333333"...3333333333333333333333333333333"...3333333333333333333333333333333"...3333333333333333333333333333333"...3333333333333333333333333333333"

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\Converged_v21033_AZXChPIB5jI3ijrmoNll5w2[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	100970
Entropy (8bit):	5.304591030098493
Encrypted:	false
SSDEEP:	1536:IpHDgWeWJw+k4zazA/PWrF7qvEAFiQcpmP4may352:ORsy3A
MD5:	0195C284F201E632378A3AE6A0D965E7
SHA1:	BF2B78CCE5E09830A0F057FB6935E206333B752A
SHA-256:	97EB235CAFA5525CEF7437B24548FB7936968778333DB62C0C661FFA8310090D
SHA-512:	98D6CE4074FA8A5DD1C67308A8282268D4DF1DAF18E95C11C1F5DF94C00559B0DF5150054D00F3EF58ABE0E72C35130753EEE2A624F910FACAC4A756EF92E55
Malicious:	false
Reputation:	moderate, very likely benign file
IE Cache URL:	http://https://logincdn.msauth.net/16.000/Converged_v21033_AZXChPIB5jI3ijrmoNll5w2.css
Preview:	/*! Copyright (C) Microsoft Corporation. All rights reserved. */./*!.---------- START OF THIRD PARTY NOTICE ----------..This fi 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 T itter, Inc..Permission is hereby granted, free of charge, to any perso

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\Print[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):	476
Entropy (8bit):	7.35124642782842
Encrypted:	false
SSDEEP:	12:6v/78/8QCeKXzjl5V6VQTdwbtsxET1SDQi7N:sNfF6VYd6tf1SdN
MD5:	B8E8859FCD4E43D51233559C17A3C7BD
SHA1:	F0CA023F26A84761995FA0BF6935DE6A3B8AE6F8
SHA-256:	DC15A37B4015D0DECF639006E4F9002E742DDBFD7C669EC0AE469057F238B78D
SHA-512:	3605E4C4FE22E6E05553F89D34CFE8B3E5CA72FBDADCCD8B279835A0ECEFCD10B1BF2AD1ACCEEB168EE369E23A8AD205720FBF33A184188A7F23AEA7B0F22 005
Malicious:	false
Reputation:	moderate, very likely benign file
IE Cache URL:	http://https://c.s-microsoft.com/en-gb/CMSImages/Print.png?version=03620f3a-5d1e-5a73-a117-a2f71eee437d
Preview:	.PNG.....IHDR.....a....sRGB.....gAMA.....a.....IDAT8O.S;..A.....M6.4....@.47....^I..<."&..W..Y...Y.....m...E.<..$..n...j..kL&.....}.j.....)@.....r..Q....]. .+.w...f3.R)...2^...ddO.^..Ud.BE..*D..h...!.....h..p..t...9.....1.."tD.....y.h.AQ.{."...J.D.U....c.b.i.h.t:..$&q..J..n.+9.r..B..F...e..`<...oS....Z-.H....NG...Jl..D.Z..@!...s<....m.'Ll..vc.?..~..v.n.9.; .m.5..K.A .....z=../>...M....r9..~...*..go.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\arrow_px_up[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 7 x 9
Category:	downloaded
Size (bytes):	829
Entropy (8bit):	0.6055646407132698
Encrypted:	false
SSDEEP:	3:CKY1q/rylAxrt/laIFBYEQvyIFle:sGFaIFBYfvDfe
MD5:	95B65C94F57061E15ECC8304D3E578D5
SHA1:	A7483D668A780949FDA842F39877A3C08D0FC51C
SHA-256:	BDA2D6EB8E72B3DBCA5EEF086178033F8A2BB3481180B2C63295FCF23843D960
SHA-512:	B17552D90D0038531A5F4E78DA553F9109346CB25851F38996BFAB54906A898DE848FEFFD31E8D0BF0A32D956513CA7ED72D2F4C3AE47922C6F9D370584288EF
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\arrow_px_up[1].gif	
Reputation:	moderate, very likely benign file
IE Cache URL:	http://https://c.s-microsoft.com/en-gb/CMSImages/arrow_px_up.gif?version=27f11222-771f-bb95-a744-f0b962f89b91
Preview:	GIF89a.....3..... ....I..... ..... .`.....\8....!>L(.b@.;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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
Encrypted:	false
SSDEEP:	96:wO4DZ+Stb/jY+eo4hAryAes9mBYYQgWLDm9:wToSBjlevudl9nO
MD5:	EE5C8D9FB6248C938FD0DC19370E90BD
SHA1:	D01A22720918B781338B5BBF9202B241A5F99EE4
SHA-256:	04D29248EE3A13A074518C93A18D6EFC491BF1F298F9B87FC989A6AE4B9FAD7A
SHA-512:	C77215B729D0E60C97F075998E88775CD0F813B4D094DC2FDD13E5711D16F4E5993D4521D0FBD5BF7150B0DBE253D88B1B1FF60901F053113C5D7C1919852D5
Malicious:	false
Reputation:	high, very likely benign file
IE Cache URL:	http://https://aadcdn.msftauth.net/ests/2.1/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\2WF3MMUU\script[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):	50466
Entropy (8bit):	5.403327253117392
Encrypted:	false
SSDEEP:	768:3Vs4A3c/bSKCzUm4D19h3j9UIAyjYXQgyjYXEoygRRsRnMtoafRnvdMIKebqH:h6c/bSKCzUm4DDh3j+9XQ4XE+BZdMIK9
MD5:	633B23CA8A850C508C146635DB4239F5
SHA1:	CF78DA53BD7561F3ACB33710016ECBF60E9F0204
SHA-256:	DAA1677D2640BE8A77F6C69EEE3911D2F8CF81DAA7BB604800A2D63A8F130C95
SHA-512:	82D4887AB9BB6A449FB0E5B6DEF80215B5F9E51058DCB1B8B7CD583A880F93428C3FB75B37C0E9481843203A4878FEF32424B5CD2EBCDD811D92604A1C1BCA B
Malicious:	false
Reputation:	moderate, very likely benign file
IE Cache URL:	http://https://c.s-microsoft.com/en-gb/CMSScripts/script.jsx?k=1a053411-4f63-d069-d3b8-11d5d720eeb4
Preview:	function ShowSelectedComponentKeyPress(n,t){if(window.event.keyCode==13)return ShowSelectedComponent(n,t),!1}function ShowHighLight(n){var t=$("#div"+ n).height();$.browser.msie&&parseInt($.browser.version,10)==7?$("#div"+n+" > .highlight").css({width:"0",height:"0","background-color":"white",float:"left","border-top":M ath.round(t/2+.3)+"px solid white","border-right":"0.75em solid "+$("#div"+n).css("background-color"),"border-bottom":Math.round(t/2+.3)+"px solid white"}):$("#div"+n+" > .highlight").css({width:"0",height:"0","background-color":"white",float:"left","border-top":t/2+.3+"px solid white","border-right":"0.75em solid "+$("#div"+n).css("background- color"),"border-bottom":t/2+.3+"px solid white"})}function SetRightSideNavigationMenuHeight(){$("[id^=dvModuleGroup_]").hide();window.location.search.toLowerCase(). indexOf("bookmarkid")!=-1&&SelectBookMark();window.location.search.toLowerCase().indexOf("componentid")!=-1&&LoadSelectedInternalLink();$(".div_side_comp").leng th>0&&$(".

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\style[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):	136271
Entropy (8bit):	5.355801424758139
Encrypted:	false
SSDEEP:	1536:2Fk5W0azHVaAgrBmeZCstBwB/BxBf9e969j9S9h919g9Z9C9f9g9Z9e979Q9t9Vn:2Fk5W0agiCK
MD5:	9A3769F2253DF9AE29B12DC21062E2BC
SHA1:	23E899CB0B626CD27ED59033E60E9FDF0B1E6CBF
SHA-256:	9E2732FD685A5101AB8B3EA0EBDA9764A004F21538F40BD42FAC359490C4CF80
SHA-512:	F1D26F368B55CEACD87243F9783D51927ED5520636B80D3AC98C649675602467F3988EF4C402048F77610525698EECB6E7C8C95A170BE81B127A29B639134ECD
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\style[1].css	
IE Cache URL:	http://https://c.s-microsoft.com/en-gb/CMSStyles/style.csx?k=3c9ade18-bc6a-b6bd-84c3-fc69aaaa7520_f05cbaf8-1aa4-2e42-0beb-040a76f09433_e688a192-b2e5-4598-dec4-9340a1bb6723_6e5b2ac7-688a-4a18-9695-a31e8139fa0f_b3dad3e4-0853-1041-fa46-2e9d6598a584_fc29d27f-7342-9cf3-c2b5-a04f30605f03_28863b11-6a1b-a28c-4aab-c36e3deb3375_907fa087-b443-3de8-613e-b445338dad1f_a66bb9d1-7095-dfc6-5a12-849441da475c_1b0ca1a3-6da9-0dbf-9932-198c9f68caeb_ef11258b-15d1-8dab-81d5-8d18bc3234bc_11339d5d-cf04-22ad-4987-06a506090313_50edf96d-7437-c38c-ad33-ebe81b170501_8031d0e3-4981-8dbc-2504-bbd5121027b7_3f0c3b77-e132-00a5-3afc-9a2f141e9eae_aebeacd9-6349-54aa-9608-cb67eadc2d17_0cdb912f-7479-061d-e4f3-bea46f10a753_343d1ae8-c6c4-87d3-af9d-4720b6ea8f34_a905814f-2c84-2cd4-839e-5634cc0cc383_190a3885-bf35-9fab-6806-86ce81df76f6_05c744db-5e3d-bcfb-75b0-441b9afb179b_8beffb66-d700-2891-2c8d-02e40c7ac557_b1fe3f15-7512-0a8f-a55b-b316245621b5_f9c8eff0-3e34-2c33-6c0d-1fa7c5077eec
Preview:	@font-face{font-family:'wf_segoe-ui_light';src:url('//c.s-microsoft.com/static/fonts/segoe-ui/west-european/light/latest.eot');src:url('//c.s-microsoft.com/static/fonts/segoe-ui/west-european/light/latest.eot?#iefix') format('embedded-opentype'),url('//c.s-microsoft.com/static/fonts/segoe-ui/west-european/light/latest.woff') format('woff'),url('//c.s-microsoft.com/static/fonts/segoe-ui/west-european/light/latest.ttf') format('truetype'),url('//c.s-microsoft.com/static/fonts/segoe-ui/west-european/light/latest.svg#web') format('svg');font-weight:normal;font-style:normal}@font-face{font-family:'wf_segoe-ui_normal';src:url('//c.s-microsoft.com/static/fonts/segoe-ui/west-european/normal/latest.eot');src:url('//c.s-microsoft.com/static/fonts/segoe-ui/west-european/normal/latest.eot?#iefix') format('embedded-opentype'),url('//c.s-microsoft.com/static/fonts/segoe-ui/west-european/normal/latest.woff') format('woff'),url('//c.s-microsoft.com/static/fonts/segoe-ui/west-european/normal/latest.ttf

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\d7-808fb1[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):	169145
Entropy (8bit):	5.043578345658209
Encrypted:	false
SSDEEP:	3072:jzCPZkTP3bDLH0tfRqQ0xtLfj4ZDSIpTt813viY8R1j35Ap7LQZLPPJH7PAbOCxq:jlZAjLkeeTC
MD5:	B5C29B4AC43102BF428D32BF9C12C76D
SHA1:	ED7C97F502484C62E5D2D8D098EE2A4D240FF991
SHA-256:	3673431352D7EAF65DEC60074374B6DF40EFA17997230B086A62D0688077E508
SHA-512:	B43E7C24BAD43D8D1BEDCBECFA9CC59511A5F9CDD4876530D1A61576B6645AF70A4DBBD96086DDC61E611FF4FE2F59DE15FDAD8FFAB05FA3463AD56A6EB7A41A
Malicious:	false
IE Cache URL:	http://https://www.microsoft.com/onerfstatics/marketingsites-eus-prod/west-european/shell/_scrf/css/themes=default.device=uplevel_web_pc/9f-350029/f7-19b3db/e7-5e6a15/18-5a610e/e9-86f957/42-f4e005/50-7d6580/d7-808fb1?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\9026IKNJ\dnserror[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	2997
Entropy (8bit):	4.4885437940628465
Encrypted:	false
SSDEEP:	48:u7u5V4VyhhV2lFUW29vj0RkpNc7KpAP8Rra:vllJ6G7Ao8Ra
MD5:	2DC61EB461DA1436F5D22BCE51425660
SHA1:	E1B79BCAB0F073868079D807FAEC669596DC46C1
SHA-256:	ACDEB4966289B6CE46ECC879531F85E9C6F94B718AAB521D38E2E00F7F7F7993
SHA-512:	A88BECB4FBDDC5AFC55E4DC0135AF714A3EEC4A63810AE5A989F2CECB824A686165D3CEDB8CBD8F35C7E5B9F4136C29DEA32736AABB451FE8088B978B493AC6D
Malicious:	false
IE Cache URL:	res://ieframe.dll/dnserror.htm?ErrorStatus=0x800C0005&DNSError=9003
Preview:	.<!DOCTYPE HTML>..<html>.. <head>.. <link rel="stylesheet" type="text/css" href="NewErrorPageTemplate.css" >.. <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.. <title>Can’t reach this page</title>.. <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="getInfo(); initMoreInfo('infoBlockID');">.. .. Can’t reach this page .. .. <ul id="cantDisplayTasks" class="tasks">.. <li id="task1-1">Make sure the web address is correct .. <li id="task1-2">Search for this site on Bing ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\httpErrorPagesScripts[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	12105
Entropy (8bit):	5.451485481468043
Encrypted:	false
SSDEEP:	192:x20iniOciwd1BtvjrG8tAGGGVWnvyJVUrUiki3ayimi5ezLCvJG1gwm3z:xPini/i+1Btvjy815ZVUwiki3ayimi5f
MD5:	9234071287E637F85D721463C488704C
SHA1:	CCA09B1E0FBA38BA29D3972ED8DCECEFDEF8C152

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\httpErrorPagesScripts[1]	
SHA-256:	65CC039890C7CEB927CE40F6F199D74E49B8058C3F8A6E22E8F916AD90EA8649
SHA-512:	87D691987E7A2F69AD8605F35F94241AB7E68AD4F55AD384F1F0D40DC59FFD1432C758123661EE39443D624C881B01DCD228A67AFB8700FE5E66FC794A6C0384
Malicious:	false
IE Cache URL:	res://ieframe.dll/httpErrorPagesScripts.js
Preview:	...function isExternalUrlSafeForNavigation(urlStr)..{..var regEx = new RegExp("^(http(s?)|ftp|file)://", "i");..return regEx.exec(urlStr);..}..function clickRefresh()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..window.location.replace(location.substring(poundIndex+1));..}..}..function navCancelInit()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..var bElement = document.createElement("A");..bElement.innerText = L_REFRESH_TEXT;..bElement.href = 'javascript:clickRefresh()';..navCancelContainer.appendChild(bElement);..}..else..{..var textNode = document.createTextNode(L_RELOAD_TEXT);..navCancelContainer.appendChild(textNode);..}..}..function getDisplayValue(elem

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\latest[1].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), Segoe UI family
Category:	downloaded
Size (bytes):	35047
Entropy (8bit):	7.975792390307888
Encrypted:	false
SSDEEP:	768:I6ibzTDpOGuAJ63YB9eSzDtQEspfAzyNyuBmOfAJYCM:/iPMYJ4GEAZoTyglcM
MD5:	CAD76E4816AF6890C9BFD02A6D1EA899
SHA1:	9EDC91541C31034FCE0D83AABBAAD4C314CD3D33
SHA-256:	D5794223D1A062E5DBE6C34C1994C8CE3792B24AFD5218D0644CB1F53DA4BE58
SHA-512:	24983A5856C2B4D8CBE2A4BD233A93B266A03D4218942E1D1733B33B65AB7A504AF0AC31DE2F1E69F6FF8CCD7A169CD4555539D34FFF8DE4CB8C98DB2DB2C863
Malicious:	false
IE Cache URL:	http://https://c.s-microsoft.com/static/fonts/segoe-ui/west-european/normal/latest.eot?
Preview:	...=.....LP#...B..... .....S.e.g.o.e. .U.l.....R.e.g.u.l.a.r.....V.e.r.s.i.o.n. .5...3.2.....S.e.g.o.e. .U.l.....RV.z..;~.....U.D.-..iu...N4P\..GLFM .Y.?.;..-...~~....Ox.M..".$.._.....g..sC*2..4W.....9AGc.[a..*.rCl,..@..U_..L...e..Ru.J.-.f..3.....S`.A.....K<;...n.Y...rli.....([...W...5k.....^K.G...U.@....2H..B.)N0w.....C..9.....#.l2,4..6y.3$b....K.wx...l.$E..?3.8.c...,x..t.wa.O....4.c...!..+.<EM...2T.>\..]4.A.H.;..G.....W.:.?...Z".....e....8....84.L,.)0..y.Xdd.Pa.@.&.o(.I.q.yF...[.y.m(D...(....T.....,A.;q.... .w.$..C..a.. .Y.O?{..0...'1.;C.,.....W..Q-..'.5tD@9..U...E4e.&_...S.Y...\)b.s.rIR.....%..R..KU O..{.0(.....^Q\^!.et...Kf%..K...}.1...S.{.....3p..]...|Y...w..|JeS$..k.....>(8 .ZlV..N.). c...Z.K.\..q...'S.j.....9...._.E.#s*'#.....[.....DJ^.L7../1...+U.qG.....-..MM..q....L..c...^...:e....<h...:.`.jz..fb.Ha.....k.....e\)g..\."..M

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\latest[2].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), Segoe UI Light family
Category:	downloaded
Size (bytes):	28315
Entropy (8bit):	7.9724193003797
Encrypted:	false
SSDEEP:	384:+R0Z7+bHAtrQ1yBFbgqLct7rJhhPLLkHsrvSzaJu4mI3n5o+MmKCxDg6iT7jdVye:+uNUAtE3phPLLFTiMu+pxCjHyGEQ9zL
MD5:	17DFE73CB9C64527F7248B0A24DB317D
SHA1:	345198B9239FCDAF038FB2D3A919E4724037DBAA
SHA-256:	AD75FB92B2EBCE6C37640F03E1AB96A752F388BCE60C877ADE4780B13839E8C4
SHA-512:	421B56D93E9BD5E4B4449DD0FCDEE8D531087FD484C91530AAF0A67EDEA33D5AC2F14A7F4966C528C0F130F17F26629FCAB9F8AB47E950CEB5B9F1A827EA0728
Malicious:	false
IE Cache URL:	http://https://c.s-microsoft.com/static/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\9026IKNJ\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):	201859
Entropy (8bit):	5.151612322590051
Encrypted:	false
SSDEEP:	6144:LUpUqbKWk+8gSoH26vd+SiOfsyUCXFfgmCVWT2Ph9mUMbT+vZht5+VKsZf:LMUqbKQ8gSoH26vd+SiOfsyUCXFfgmCw
MD5:	44A416A6D2C7B863B2B52AA92A0FBDDA
SHA1:	228D7BA0AA5D72A114CA3896601E7C22463C121F
SHA-256:	23B458A23ADA39A1B1FA71AA025DE4E321360F3C4AE6099BD8EB2640C161CAF5
SHA-512:	6ABCD4F7636DDF88EF87B950FFC87BBABC1CFE4396C515E81A63B438E1A4E250E36B2FB787C11052EAE0D17CC1451BE1F008DC42324F97F2594226761F6D4E58
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\servicesagreement[1].htm	
Preview:	.<!DOCTYPE html ><html xmlns:mscom="http://schemas.microsoft.com/CMSvNext" xmlns:md="http://schemas.microsoft.com/mscom-data" lang="en-gb" 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>default page</title><meta name="Title" content="default page" /><meta name="CorrelationVector" content="kZ+7WrRVrkG82Fuz.1" /><meta name="Description" content="default page." /><meta name="MscomContentLocale" content="en-gb" /><link href="https://www.microsoft.com/onerfstatics/marketingsites-eus-prod/west-european/shell/_scrf/css/themes=default.device=uplevel_web_pc/9f-350029/f7-19b3db/e7-5e6a15/18-5a610e/e9-86f957/42-f4e005/50-7d6580/d7-808fb1?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="stylesheet" type="t

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\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):	135290
Entropy (8bit):	5.2254562447372
Encrypted:	false
SSDEEP:	3072:1f/HuFzpxJIS20i9d1EwgXA95KSqDCE4t:1f/HuXIZRjt
MD5:	07CB1B6723F61F949C862B399E06B3BF
SHA1:	83ABC38AB7E787F719E859E3EA97D4A634FE61FC
SHA-256:	82A7ACB7D942575069E4067375BEC0C33F1949EA2864BE8BD12E9D6DB74A345D
SHA-512:	D520D31E12A3D2D316347D96E4E3D20D7E5C988A4824228097D1DF0A5AB3F12334096C2ADD5D0A7345EF8A2E674712F84D9F8CFC2E973A2A4DEDA546337C940D
Malicious:	false
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-c07ea1/9d-b58f60/f6-aa5278/cd-23d3b0/6d-1e7ed0/b7-cadaa7/c4-898cf2/ca-40b7b0/4e-ee3a55/3e-f5c39b/c3-6454d7/f9-7592d3/92-10345d/79-499886/7e-cda2d3/69-13871c/b7-0ad59f/e0-3c9860/91-97a04f/1f-100dea/33-abe4df/17-f90ef1?ver=2.0&iife=1
Preview:	(function(){/**. * @license almond 0.3.3 Copyright jQuery Foundation and other contributors.. * Released under MIT license, http://github.com/requirejs/almond/LICENSE. */ .var requirejs,require,define,__extends;(function(n){function r(n,t){return w.call(n,t)}function s(n,t){var o,s,f,e,h,p,c,b,r,l,w,k,u=t&&t.split("/"),a=i.map,y=a&&a["*"]||{};if(n){ for(n=n.split("/"),h=n.length-1,i.nodeIdCompat&&v.test(n[h])&&(n[h]=n[h].replace(v,"")),n[0].charAt(0)==="."&&u&&(k=u.slice(0,u.length-1),n=k.concat(n)),r=0;r<n.length;r++)if(w=n[r],w==="."")n.splice(r,1),r-=1;else if(w===".."){if(r===0||r===1&&n[2]===".."||n[r-1]===..")continue;else r>0&&(n.splice(r-1,2),r-=2);n=n.join("/")}if((u||y)&&a){ for(o=n.split("/"),r=o.length;r>0;r-=1){if(s=o.slice(0,r).join("/"),u)for(l=u.length;l>0;l-=1)if(f=a[u.slice(0,l).join("/")],f&&(f=f[s],f)){e=f;p=r;break}if(e)break;!c&&y&&y[s]&&(c=y[s],b=r)}!e&&c&&(e=c,p=b);e&&(o.splice(0,p,e),n=o.join("/"))}return n}function y(t,i){return function(){var r=b.call(arguments,0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\NewErrorPageTemplate[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	1612
Entropy (8bit):	4.869554560514657
Encrypted:	false
SSDEEP:	24:5Y0bQ573pHpACtUZtJD0lFBopZleqw87xTe4D8FaFJ/Doz9AtjJgbCzg:5m73jcJqQep89TEw7Uxkk
MD5:	DFEABDE84792228093A5A270352395B6
SHA1:	E41258C9576721025926326F76063C2305586F76
SHA-256:	77B138AB5D0A90FF04648C26ADDD5E414CC178165E3B54A4CB3739DA0F58E075
SHA-512:	E256F603E67335151BB709294749794E2E3085F4063C623461A0B3DECBCCA8E620807B707EC9BCBE36DCD7D639C55753DA0495BE85B4AE5FB6BFC52AB4B284FD
Malicious:	false
IE Cache URL:	res://ieframe.dll/NewErrorPageTemplate.css
Preview:	.body..{.. background-repeat: repeat-x;.. background-color: white;.. font-family: "Segoe UI", "verdana", "arial";.. margin: 0em;.. color: #1f1f1f;..}.....mainContent..{.. margin-top:80px;.. width: 700px;.. margin-left: 120px;.. margin-right: 120px;..}.....title..{.. color: #54b0f7;.. font-size: 36px;.. font-weight: 300;.. line-height: 40px;.. margin-bottom: 24px;.. font-family: "Segoe UI", "verdana";.. position: relative;..}.....errorExplanation..{.. color: #000000;.. font-size: 12pt;.. font-family: "Segoe UI", "verdana", "arial";.. text-decoration: none;..}.....taskSection..{.. margin-top: 20px;.. margin-bottom: 28px;.. position: relative; ..}.....tasks..{.. color: #000000;.. font-family: "Segoe UI", "verdana";.. font-weight:200;.. font-size: 12pt;..}....li..{.. margin-top: 8px;..}.....diagnoseButton..{.. outline: none;.. font-size: 9pt; ..}.....launchInternetOptionsButton..{.. outline: none;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\down[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	748
Entropy (8bit):	7.249606135668305
Encrypted:	false
SSDEEP:	12:6v/7/2QeZ7HVJ6o6yiq1p4tSQfAVFcm6R2HkZuU4fB4CsY4NJlrvMezoW2uONroc:GeZ6oLiqkbDuU4fqzTrvMeBBlE
MD5:	C4F558C4C8B56858F15C09037CD6625A
SHA1:	EE497CC061D6A7A59BB66DEFEA65F9A8145BA240
SHA-256:	39E7DE847C9F731EAA72338AD9053217B957859DE27B50B6474EC42971530781
SHA-512:	D60353D3FBEA2992D96795BA30B20727B022B9164B2094B922921D33CA7CE1634713693AC191F8F5708954544F7648F4840BCD5B62CB6A032EF292A8B0E52A44
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\down[1]	
IE Cache URL:	res://ieframe.dll/down.png
Preview:	.PNG.....IHDR.....ex....PLTE....W..W..W..W..W..W..W..W..W..W..W..W..W.U.....W..W.!Y.#Z.$\.'].<r.=s.P..Q..Q..U..o..p..r..x..z..~..... ....b.....$..s...7tRNS.a.o(,.s....e.....q*..... .....F.Z....IDATx^%.S..@.C..jm.mTk...m.?|;.y..S....F.t...,.....D.>..LpX=f.M...H4.....=...=..xy.[h..7....7.....<.q.kH....#+....I..z.....'.ksC...X<.+..J>....%3BmqaV ...h..Z._.:<.Y_jG...vN^.<>.Nu.u@.....M....?...1D.m~)s8..&....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\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
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\CS6IXJW6\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):	128026
Entropy (8bit):	5.263686738901574
Encrypted:	false
SSDEEP:	1536:+JXd+YOlaYOyguihQ3ZYrH6GdXJKjZtQ3EBJ0PYmwYmEZeQ8Wt2Db7ACu8J8lvCs:ed+YOlaYOyguihQ3ZOHbdX2nX5PaCfey
MD5:	793D36029B8AD32CB261F226B7012686
SHA1:	168780848C49158030673BD4DBA93CD3071D1DC8
SHA-256:	E3BEAC351290C97CEFAF06552F5BF1CB1EE48611C896D46E9B397291869DA137
SHA-512:	CE1A120334350B2D40E8BC84502500A6C0BEE82FD1630481DE4EF54138A0458E99A0323785F8A7FF98F39FB54D64AD2F0F5F738F5225C6F9A168C932390187BC
Malicious:	false
IE Cache URL:	http://https://c.s-microsoft.com/en-gb/CMSScripts/script.jsx?k=0502864a-b6ef-2f14-9f8e-267004d3a4e0_c5ea3348-55af-729a-2641-14f0312bacf3_742bd11f-3d7c-9955-3df5-f02b66689699_cb9d43d2-fbae-5b5c-827f-72166d6b87fc_49488e0d-6ae2-5101-c995-f4d56443b1d8_7dea7b90-4334-c043-b252-9f132d19ee19_38aa9ffb-ddb5-75be-6536-a58628f435f5_e3e65a0a-c133-43e7-571d-2293e03f85e6_c7a4393f-7c9b-39d3-762d-af461a6d6564_4ca0e9dc-a4de-17ba-f0de-d1d346cb99e2_06310cd8-41c6-3b11-4645-b4884789ed70_5c27e8aa-9347-969e-39ac-37a4de428a8d_d6872b5a-5310-a73c-7cb3-227a3213a1c5_be92d794-4118-193f-9871-58b72092a5ac_64c742e2-b29c-b6c1-fdd9-accf33ec40bd_cf2ceca9-3467-a5b3-d095-68958eee6d4c_cec39dd8-f1d3-56f1-abfc-a7db34ff7b46_ec5fa2c9-3950-ff57-a5c3-1fa77e0db190_d19f9592-65df-bcc9-e30e-439b875c3381_76a3d06f-f11f-77ef-9bfd-6227ba750200_5e1caa45-461c-3b04-f88b-8cd50af16db5_c2dceda8-20b4-7d3f-13b6-9cac67d7df17_914fa41b-cc86-d3b0-4e15-2fdfa357bcc7_40c6c884-da6e-7c2c-081f-4a7dfe7c7245_ae79ba96-1a9d-debd-a5b1-f3067213b9b8
Preview:	function getQueryValue(n,t){var r=new RegExp("[\\?&]"+t+"=([^&#]*)","gi"),i=r.exec(n);return i==null?"":decodeURIComponent(i[1].replace(/\+/g," "))}function getStore(n){var t="ClosestStore.asmx",r,i;$(".store-geo[data-GeoStoreLocalServiceURL]").length&&(t=$(".store-geo").first().attr("data-GeoStoreLocalServiceURL"));i="POST";typeof n!="undefined"&&(r={latitude:JSON.stringify(n.coords.latitude),longitude:JSON.stringify(n.coords.longitude)},t=t+"ClientGeo",i="GET");$.ajax({url:t,type:i,timeout:5e3,data:r,contentType:"application/json; charset=UTF-8",dataType:"json",error:function(){$(".store-geo").remove();$(".store-editorial").fadeIn(1e3)},success:function(n){if(typeof n!="undefined"&&typeof n.d!="undefined"&&typeof n.d.City!="undefined"&&n.d.City!=""&&n.d.StoreUrl!="undefined"&&n.d.StoreUrl!=""){var t=$(".store-geo:first").text();$(".store-geo a").html(t+" "+n.d.City);$(".store-geo a").attr("href",n.d.StoreUrl);$(".store-editorial").remove();$(".store-geo").fadeIn(1e3)}else $(".store-g

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\wcp-consent[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):	255440
Entropy (8bit):	6.051861579501256
Encrypted:	false
SSDEEP:	6144:PIgagvUI0iDsW9Whsredo7NjIZjIZP0aNWgF9Dyjzh:PIgaHI0iIUedo7NjIZjIZP0o74t
MD5:	38B769522DD0E4C2998C9034A54E174E
SHA1:	D95EF070878D50342B045DCF9ABD3FF4CCA0AAF3
SHA-256:	208EDBED32B2ADAC9446DF83CAA4A093A261492BA6B8B3BCFE6A75EFB8B70294
SHA-512:	F0A10A4C1CA4BAC8A2DBD41F80BBE1F83D767A4D289B149E1A7B6E7F4DBA41236C5FF244350B04E2EF485FDF6EB774B9565A858331389CA3CB474172465EB3E F

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\wcp-consent[1].js	
Malicious:	false
IE Cache URL:	http://https://wcpstatic.microsoft.com/mscc/lib/v2/wcp-consent.js
Preview:	var WcpConsent=function(e){var a={};function i(n){if(a[n])return a[n].exports;var o=a[n]={i:n,l:!1,exports:{}};return e[n].call(o.exports,o,o.exports,i),o.l=!0,o.exports}return i.m=e,i.c=a,i.d=function(e,a,n){i.o(e,a)||Object.defineProperty(e,a,{enumerable:!0,get:n})},i.r=function(e){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(e,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(e,"__esModule",{value:!0})},i.t=function(e,a){if(1&a&&(e=i(e)),8&a)return e;if(4&a&&"object"==typeof e&&e&&e.__esModule)return e;var n=Object.create(null);if(i.r(n),Object.defineProperty(n,"default",{enumerable:!0,value:e}),2&a&&"string"!=typeof e)for(var o in e)i.d(n,o,function(a){return e[a]}.bind(null,o));return n},i.n=function(e){var a=e&&e.__esModule?function(){return e.default}:function(){return e};return i.d(a,"a",a),a},i.o=function(e,a){return Object.prototype.hasOwnProperty.call(e,a)},i.p="",i(i.s=1)}([function(e,a,i){window,e.exports=function(e){var a={};function i(n)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\0_pdvuot_2pyxh5ith335y8a2[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, baseline, precision 8, 1920x1080, frames 3
Category:	downloaded
Size (bytes):	283351
Entropy (8bit):	7.975896455873056
Encrypted:	false
SSDEEP:	6144:hPgRhluS12CyK8XGsLzsr5XONnQ4/bEmhZSlj6xU2zyOX/:2vz1pyWsLoXqN/YWPUU2OOX/
MD5:	A5DBD4393FF6A725C7E62B61DF7E72F0
SHA1:	55B292F885FFC92ABCE18750B07AA4ACFA4E903E
SHA-256:	211A907DE2DA0FF4A0E90917AC8054E2F35C351180977550C26E51B4909F2BEB
SHA-512:	850586A05B67EF25492BD50A090F1EC0A0CC21DC4E4EFEB35E19CDC78A98F9415A3807318FA02664EADE87F0E2D8FA2A2958CD0D712329800FC05689E01DC61
Malicious:	false
IE Cache URL:	http://https://aadcdn.msftauth.net/ests/2.1/content/images/backgrounds/0_pdvuot_2pyxh5ith335y8a2.jpg?x=12f4b8b543125cc986c79cd85320812f
Preview:	.....Phttp://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c142 79.160924, 2017/07/13-01:06:39 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about=""/> </rdf:RDF> </x:xmpmeta>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\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:	D4F6E49C854E15FE48D6A1F1A03FDA93218AB8FCDB2C443668E7DF478830831ACC2B41DAEFC25ED38FCC8D96C4401377374FED35C36A5017A11E63C8DAE5C 87
Malicious:	false
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\OR0WKIO1\errorPageStrings[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	4720
Entropy (8bit):	5.164796203267696
Encrypted:	false
SSDEEP:	96:z9UUiqRxqH211CUIRgRLnRynjZbRXkRPRk6C87Apsat/5/+mhPcF+5g+mOQb7A9o:JsUOG1yNlX6ZzWpHOWLia16Cb7bk
MD5:	D65EC06F21C379C87040B83CC1ABAC6B
SHA1:	208D0A0BB775661758394BE7E4AFB18357E46C8B
SHA-256:	A1270E90CEA31B46432EC44731BF4400D22B38EB2855326BF934FE8F1B169A4F
SHA-512:	8A166D26B49A5D95AEA49BC649E5EA58786A2191F4D2ADAC6F5FBB7523940CE4482D6A2502AA870A931224F215CB2010A8C9B99A2C1820150E4D365CAB28299
Malicious:	false
IE Cache URL:	res://ieframe.dll/errorPageStrings.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\errorPageStrings[1]	
Preview:	.//Split out for localization...var L_GOBACK_TEXT = "Go back to the previous page.";..var L_REFRESH_TEXT = "Refresh the page.";..var L_MOREINFO_TEXT = "More information";..var L_OFFLINE_USERS_TEXT = "For offline users";..var L_RELOAD_TEXT = "Retype the address.";..var L_HIDE_HOTKEYS_TEXT = "Hide tab shortcuts";..var L_SHOW_HOTKEYS_TEXT = "Show more tab shortcuts";..var L_CONNECTION_OFF_TEXT = "You are not connected to the Internet. Check your Internet connection.";..var L_CONNECTION_ON_TEXT = "It appears you are connected to the Internet, but you might want to try to reconnect to the Internet.";....//used by invalidcert.js and hstscerterror.js..var L_CertUnknownCA_TEXT = "Your PC doesn\u2019t trust this website\u2019s security certificate.";..var L_CertExpired_TEXT = "The website\u2019s security certificate is not yet valid or has expired.";..var L_CertCNMismatch_TEXT = "The hostname in the website\u2019s security certificate differs from the web site you are trying to visit.";..var L

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\favicon[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 6 icons, 128x128, 16 colors, 72x72, 16 colors
Category:	downloaded
Size (bytes):	17174
Entropy (8bit):	2.9129715116732746
Encrypted:	false
SSDEEP:	24:QSNTmTFxg4lyyyyyyyyyyyyyio7eeeeeeeeekzgsLsLsLsLsLsQZp:nfgyyyyyyyyyyyyynzQQQQQO
MD5:	12E3DAC858061D088023B2BD48E2FA96
SHA1:	E08CE1A144ECEAE0C3C2EA7A9D6FBC5658F24CE5
SHA-256:	90CDAF487716184E4034000935C605D1633926D348116D198F355A98B8C6CD21
SHA-512:	C5030C55A855E7A9E20E22F4C70BF1E0F3C558A9B7D501CFAB6992AC2656AE5E41B050CCAC541EFA55F9603E0D349B247EB4912EE169D44044271789C719CD0
Malicious:	false
IE Cache URL:	http://https://www.microsoft.com/favicon.ico
Preview:	..............h(..f...HH...........(..00......h....6.. ....=..............@..........(....A..(...................(.....................................''P...'' ...3333333333333333333333333333333'' ...3333333333333333333333333333333'' ...3333333333333333333333333333333'' ...3333333333333333333333333333333'' ...3333333333333333333333333333333'' ...3333333333333333333333333333333'' ...3333333333333333333333333333333'' ...3333333333333333333333333333333'' ...3333333333333333333333333333333'' ...3333333333333333333333333333333''

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\jquery-1.7.2.min[1].js</th></tr>
<tr><td>Process:</td><td>C:\Program Files (x86)\Internet Explorer\iexplore.exe</td></tr>
<tr><td>File Type:</td><td>HTML document, UTF-8 Unicode text, with very long lines</td></tr>
<tr><td>Category:</td><td>downloaded</td></tr>
<tr><td>Size (bytes):</td><td>94840</td></tr>
<tr><td>Entropy (8bit):</td><td>5.372946098601679</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>1536:8YRKUfAjtledhTmtaFyQHGvCXsedOgRc9izzr4yff8teLvHHEjam7W5X3yzSiLnM:VUb6GvCu09s2o2skAieW</td></tr>
<tr><td>MD5:</td><td>B8D64D0BC142B3F670CC0611B0AEBCAE</td></tr>
<tr><td>SHA1:</td><td>ABCD2BA13348F178B17141B445BC99F1917D47AF</td></tr>
<tr><td>SHA-256:</td><td>47B68DCE8CB6805AD5B3EA4D27AF92A241F4E29A5C12A274C852E4346A0500B4</td></tr>
<tr><td>SHA-512:</td><td>A684ABBE37E8047C55C394366B012CC9AE5D682D29D340BC48A37BE1A549AECED72DE6408BEDFED776A14611E6F3374015B236FBF49422B2982EF18125FF47D
C</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>IE Cache URL:</td><td>http://https://ajax.aspnetcdn.com/ajax/jQuery/jquery-1.7.2.min.js</td></tr>
<tr><td>Preview:</td><td>/*! 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</td></tr>
</table>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\mwfmdl2-v3.54[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 26288, version 0.0
Category:	downloaded
Size (bytes):	26288
Entropy (8bit):	7.984195877171481
Encrypted:	false
SSDEEP:	768:56JqQaQphRbTHiKNF5z/02h5KpJW3pPOA8Y9g/:gdTTH5XKpJWdH1W/
MD5:	D0263DC03BE4C393A90BDA733C57D6DB
SHA1:	8A032B6DEAB53A33234C735133B48518F8643B92
SHA-256:	22B4DF5C33045B645CAFA45B04685F4752E471A2E933BFF5BF14324D87DEEE12
SHA-512:	9511BEF269AE0797ADDF4CD6F2FEC4AD0C4A4E06B3E5BF6138C7678A203022AC4818C7D446D154594504C947DA3061030E82472D2708149C0709B1A070FDD0E
Malicious:	false
IE Cache URL:	http://https://www.microsoft.com/mwf/_h/v3.54/mwf.app/fonts/mwfmdl2-v3.54.woff

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\mwfmdl2-v3.54[1].woff	
Preview:	wOFF.....f.....D.....OS/2...X...H...`JM.FVDMX.....^.qcmap.....*.9cvt ...4... ...*....fpgm...T.....Y...gasp...D.....glyf...P..U5.....head..]....2...6.. .Chhea..]....$$...hmtx..]....ye'loca..^.....Gmaxp..`.... ... ./..name..`....8....]..Rpost..f..... .Q.wprep..f$.....x...x.c`.Pf.....:....Q.B3_dHc..`e.bdb... .`@..`...../9.\|... V...)00...-.Wx...S....._..m.m.m.m.m;e..y.~.....<p..a.0t.&...a.pa.0B.1..F...Q.ha.0F.3....q.xa.0A.0L.&...l.da.0E.2L....i.ta.0C.1..f...Y.la.0G.3.....y.\|a..@X0,....E.ba.DX2,....e .ra..BX1..V...U.ja..FX3.....u.za..A.0l.6...M.fa.E.2l....m.va..C.1..v...].na..G.3.....}.~a.p@80.....C.a..pD82.....c.q..pB81..N...S.i..pF83.....s.y..pA.0\.....K.e..pE.2\....k.u..pC.1..n...[. m..pG.3.....{.}...@x0<.....G.c...Dx2<....g.s...Bx1..^...W.k...Fx3.....w.{...A.0\|.>...O.g...E.2\|....o.w...C.1..~..._.o..08.....?..0$.....x...mL.U.....9.x.`[...&BF@X...V.h.Z..h. .....`n....[..U

C:\Users\user\AppData\Local\Temp\~DF21D4BF00FAEEC794.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	85016
Entropy (8bit):	1.6634961474678256
Encrypted:	false
SSDEEP:	384:kBqoxKAuqR+0SYpyl3yYQY/eOhtVv4GtZb8:
MD5:	8A4052E0D2490922EAF463EFA99889BC
SHA1:	67CA1A8A69144530F422863709177C5C54824542
SHA-256:	B4D9DCE43EAC21EAD0970247C56B57F2DF20EC6BF5B8EEE8CE8A1747F3ADBAA7
SHA-512:	5C6EE8E6CDA69A462920553A9994010DC4C9FE2D5AE20530768026C789F38BB702684224CD98F793210E7F4A11DB0F4B7013B12A978D59AD1AA3C47C9079E29D
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFA4B72BDCB6871BC2.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.39663867163216643
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laAggplvuS7Sm:kBqoxxJhHWSVSEabTvklo
MD5:	BE76B75F3D6D4F247C5AD6D07DC61E3F
SHA1:	D8867E33EFDD9A19671365D3BFC1450AB48EDF7B
SHA-256:	A21C2755232544B08A58D4089C0993A4629124BD6C50D8743AB15313DA5DAB98
SHA-512:	30B76BF0E676704D2B9EBC127D985576AC065DD3900520FE08F9E1D81314F392A2412789920809E2B55305295AE9D20D3B63B66F36E44BEABE46420304A695DC
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFFED1E8E288005E12.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13077
Entropy (8bit):	0.5097110636418096
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loQ9log9lWrFan3HB:kBqoIrNE
MD5:	54FB92858E99E8216154FAAB46BCFFDF
SHA1:	14B8A59360ADF797D61F1802A9D2B3AE6B6A8851
SHA-256:	6E28D3030AD8C4CE7E3BB0573CB01AD608837A7B6118EBBC32B4D986175F7487
SHA-512:	3171A054D81055CFA739F60D5B2896F8B57C995AB9944B99719D3B1A20383AEBC00584EA1F21D32FBD6848A0228CC7B592DBC308FEA929055E01E81721CDA6E
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

Static File Info

General

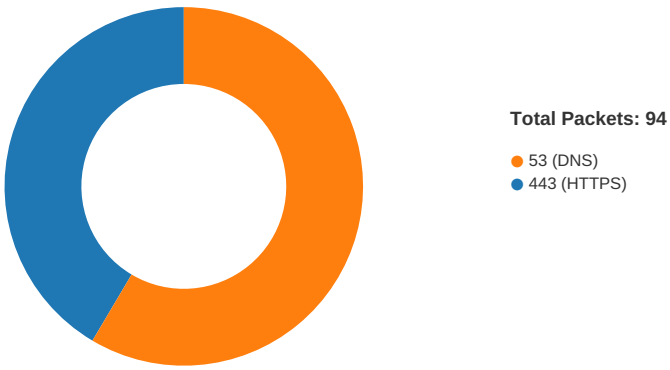
File type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Entropy (8bit):	3.29796850155148
TrID:	
File name:	RemitSwift119353 xlsx.htm
File size:	49724
MD5:	ca3a56c1d6eebe70576bb7196f53b1d0
SHA1:	72d5d6ef29bd345f17dcff7c299f47558e745d3e
SHA256:	3a6422545bcba48ce42dcbce1838b7042d8e5546f2ae527af18e7cd8b53ee879
SHA512:	e819a98723dbd5310fd630029343008c639b921d46a0660bfd142847a27219330ff1a852bc9cc3ad6ce333651add92fbc02b99106e71e1046d125bdd5f4eefc5
SSDEEP:	384:ZaWyc2bPTBPBE92bWBNQN4SaQdaAwGKrzLLuY/d1c4+GvArbOUaG4Mtd9z4NiDu0:Zp2l+AA+b4MNS6juPP
File Content Preview:	<script language="javascript">document.write(unescape('%0A%0A%0A%3C%21%44%4F%43%54%59%50%45%20%68%74%6D%6C%3E%0A%0A%3C%68%74%6D%6C%20%6C%61%6E%67%3D%22%65%6E%22%3E%3C%68%65%61%64%3E%3C%6D%65%74%61%20%68%74%74%70%2D%65%71%75%69%76%3D%22%43%6F%6E%74%65%6E%7

File Icon

Icon Hash:	f8c89c9a9a998cb8

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 09:30:43.264152050 CEST	49727	443	192.168.2.4	192.229.221.185
Apr 12, 2021 09:30:43.264826059 CEST	49728	443	192.168.2.4	152.199.23.37
Apr 12, 2021 09:30:43.265036106 CEST	49729	443	192.168.2.4	152.199.23.37
Apr 12, 2021 09:30:43.265223026 CEST	49730	443	192.168.2.4	192.229.221.185
Apr 12, 2021 09:30:43.287009001 CEST	49731	443	192.168.2.4	217.160.0.18
Apr 12, 2021 09:30:43.287126064 CEST	49732	443	192.168.2.4	217.160.0.18
Apr 12, 2021 09:30:43.305028915 CEST	443	49727	192.229.221.185	192.168.2.4
Apr 12, 2021 09:30:43.305192947 CEST	49727	443	192.168.2.4	192.229.221.185
Apr 12, 2021 09:30:43.305484056 CEST	443	49728	152.199.23.37	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 09:30:43.305546045 CEST	443	49729	152.199.23.37	192.168.2.4
Apr 12, 2021 09:30:43.305583000 CEST	49728	443	192.168.2.4	152.199.23.37
Apr 12, 2021 09:30:43.305630922 CEST	49729	443	192.168.2.4	152.199.23.37
Apr 12, 2021 09:30:43.305771112 CEST	443	49730	192.229.221.185	192.168.2.4
Apr 12, 2021 09:30:43.305883884 CEST	49730	443	192.168.2.4	192.229.221.185
Apr 12, 2021 09:30:43.313823938 CEST	49727	443	192.168.2.4	192.229.221.185
Apr 12, 2021 09:30:43.313968897 CEST	49729	443	192.168.2.4	152.199.23.37
Apr 12, 2021 09:30:43.314121008 CEST	49728	443	192.168.2.4	152.199.23.37
Apr 12, 2021 09:30:43.314198017 CEST	49730	443	192.168.2.4	192.229.221.185
Apr 12, 2021 09:30:43.334233999 CEST	443	49731	217.160.0.18	192.168.2.4
Apr 12, 2021 09:30:43.334295988 CEST	443	49732	217.160.0.18	192.168.2.4
Apr 12, 2021 09:30:43.334386110 CEST	49731	443	192.168.2.4	217.160.0.18
Apr 12, 2021 09:30:43.334465027 CEST	49732	443	192.168.2.4	217.160.0.18
Apr 12, 2021 09:30:43.335398912 CEST	49731	443	192.168.2.4	217.160.0.18
Apr 12, 2021 09:30:43.335699081 CEST	49732	443	192.168.2.4	217.160.0.18
Apr 12, 2021 09:30:43.354566097 CEST	443	49727	192.229.221.185	192.168.2.4
Apr 12, 2021 09:30:43.354623079 CEST	443	49729	152.199.23.37	192.168.2.4
Apr 12, 2021 09:30:43.354661942 CEST	443	49728	152.199.23.37	192.168.2.4
Apr 12, 2021 09:30:43.354700089 CEST	443	49730	192.229.221.185	192.168.2.4
Apr 12, 2021 09:30:43.355482101 CEST	443	49727	192.229.221.185	192.168.2.4
Apr 12, 2021 09:30:43.355542898 CEST	443	49727	192.229.221.185	192.168.2.4
Apr 12, 2021 09:30:43.355597973 CEST	443	49727	192.229.221.185	192.168.2.4
Apr 12, 2021 09:30:43.355643034 CEST	443	49727	192.229.221.185	192.168.2.4
Apr 12, 2021 09:30:43.355664015 CEST	49727	443	192.168.2.4	192.229.221.185
Apr 12, 2021 09:30:43.355688095 CEST	443	49727	192.229.221.185	192.168.2.4
Apr 12, 2021 09:30:43.355705976 CEST	49727	443	192.168.2.4	192.229.221.185
Apr 12, 2021 09:30:43.355711937 CEST	49727	443	192.168.2.4	192.229.221.185
Apr 12, 2021 09:30:43.355715990 CEST	49727	443	192.168.2.4	192.229.221.185
Apr 12, 2021 09:30:43.355742931 CEST	443	49729	152.199.23.37	192.168.2.4
Apr 12, 2021 09:30:43.355760098 CEST	49727	443	192.168.2.4	192.229.221.185
Apr 12, 2021 09:30:43.355798960 CEST	443	49729	152.199.23.37	192.168.2.4
Apr 12, 2021 09:30:43.355819941 CEST	49729	443	192.168.2.4	152.199.23.37
Apr 12, 2021 09:30:43.355854034 CEST	443	49729	152.199.23.37	192.168.2.4
Apr 12, 2021 09:30:43.355868101 CEST	49729	443	192.168.2.4	152.199.23.37
Apr 12, 2021 09:30:43.355894089 CEST	443	49729	152.199.23.37	192.168.2.4
Apr 12, 2021 09:30:43.355918884 CEST	49729	443	192.168.2.4	152.199.23.37
Apr 12, 2021 09:30:43.355947018 CEST	443	49730	192.229.221.185	192.168.2.4
Apr 12, 2021 09:30:43.355953932 CEST	49729	443	192.168.2.4	152.199.23.37
Apr 12, 2021 09:30:43.355999947 CEST	443	49730	192.229.221.185	192.168.2.4
Apr 12, 2021 09:30:43.356024027 CEST	49730	443	192.168.2.4	192.229.221.185
Apr 12, 2021 09:30:43.356059074 CEST	443	49730	192.229.221.185	192.168.2.4
Apr 12, 2021 09:30:43.356060028 CEST	49730	443	192.168.2.4	192.229.221.185
Apr 12, 2021 09:30:43.356098890 CEST	443	49730	192.229.221.185	192.168.2.4
Apr 12, 2021 09:30:43.356122017 CEST	49730	443	192.168.2.4	192.229.221.185
Apr 12, 2021 09:30:43.356138945 CEST	443	49730	192.229.221.185	192.168.2.4
Apr 12, 2021 09:30:43.356154919 CEST	49730	443	192.168.2.4	192.229.221.185
Apr 12, 2021 09:30:43.356192112 CEST	49730	443	192.168.2.4	192.229.221.185
Apr 12, 2021 09:30:43.356192112 CEST	443	49728	152.199.23.37	192.168.2.4
Apr 12, 2021 09:30:43.356247902 CEST	443	49728	152.199.23.37	192.168.2.4
Apr 12, 2021 09:30:43.356264114 CEST	49728	443	192.168.2.4	152.199.23.37
Apr 12, 2021 09:30:43.356302023 CEST	443	49728	152.199.23.37	192.168.2.4
Apr 12, 2021 09:30:43.356306076 CEST	49728	443	192.168.2.4	152.199.23.37
Apr 12, 2021 09:30:43.356340885 CEST	443	49728	152.199.23.37	192.168.2.4
Apr 12, 2021 09:30:43.356355906 CEST	49728	443	192.168.2.4	152.199.23.37
Apr 12, 2021 09:30:43.356378078 CEST	443	49728	152.199.23.37	192.168.2.4
Apr 12, 2021 09:30:43.356398106 CEST	49728	443	192.168.2.4	152.199.23.37
Apr 12, 2021 09:30:43.356451988 CEST	49728	443	192.168.2.4	152.199.23.37
Apr 12, 2021 09:30:43.382467031 CEST	443	49731	217.160.0.18	192.168.2.4
Apr 12, 2021 09:30:43.382654905 CEST	443	49732	217.160.0.18	192.168.2.4
Apr 12, 2021 09:30:43.383692026 CEST	443	49731	217.160.0.18	192.168.2.4
Apr 12, 2021 09:30:43.383833885 CEST	49731	443	192.168.2.4	217.160.0.18
Apr 12, 2021 09:30:43.383841991 CEST	443	49732	217.160.0.18	192.168.2.4
Apr 12, 2021 09:30:43.383932114 CEST	49732	443	192.168.2.4	217.160.0.18
Apr 12, 2021 09:30:43.391112089 CEST	49731	443	192.168.2.4	217.160.0.18

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 09:30:43.401228905 CEST	49732	443	192.168.2.4	217.160.0.18
Apr 12, 2021 09:30:43.402962923 CEST	49733	443	192.168.2.4	217.160.0.18
Apr 12, 2021 09:30:43.406573057 CEST	49734	443	192.168.2.4	217.160.0.18
Apr 12, 2021 09:30:43.413547993 CEST	49728	443	192.168.2.4	152.199.23.37
Apr 12, 2021 09:30:43.413830996 CEST	49729	443	192.168.2.4	152.199.23.37
Apr 12, 2021 09:30:43.427077055 CEST	49727	443	192.168.2.4	192.229.221.185
Apr 12, 2021 09:30:43.427125931 CEST	49730	443	192.168.2.4	192.229.221.185
Apr 12, 2021 09:30:43.428458929 CEST	49728	443	192.168.2.4	152.199.23.37
Apr 12, 2021 09:30:43.429126024 CEST	49728	443	192.168.2.4	152.199.23.37
Apr 12, 2021 09:30:43.429395914 CEST	49729	443	192.168.2.4	152.199.23.37
Apr 12, 2021 09:30:43.429461002 CEST	49728	443	192.168.2.4	152.199.23.37
Apr 12, 2021 09:30:43.429738998 CEST	49727	443	192.168.2.4	192.229.221.185
Apr 12, 2021 09:30:43.429833889 CEST	49730	443	192.168.2.4	192.229.221.185
Apr 12, 2021 09:30:43.430102110 CEST	49727	443	192.168.2.4	192.229.221.185
Apr 12, 2021 09:30:43.438375950 CEST	443	49731	217.160.0.18	192.168.2.4
Apr 12, 2021 09:30:43.448530912 CEST	443	49732	217.160.0.18	192.168.2.4
Apr 12, 2021 09:30:43.450067043 CEST	443	49733	217.160.0.18	192.168.2.4
Apr 12, 2021 09:30:43.450212002 CEST	49733	443	192.168.2.4	217.160.0.18
Apr 12, 2021 09:30:43.451065063 CEST	49733	443	192.168.2.4	217.160.0.18
Apr 12, 2021 09:30:43.453685999 CEST	443	49734	217.160.0.18	192.168.2.4
Apr 12, 2021 09:30:43.453780890 CEST	49734	443	192.168.2.4	217.160.0.18
Apr 12, 2021 09:30:43.454421043 CEST	443	49728	152.199.23.37	192.168.2.4
Apr 12, 2021 09:30:43.454440117 CEST	49734	443	192.168.2.4	217.160.0.18
Apr 12, 2021 09:30:43.454468012 CEST	443	49728	152.199.23.37	192.168.2.4
Apr 12, 2021 09:30:43.454505920 CEST	443	49729	152.199.23.37	192.168.2.4
Apr 12, 2021 09:30:43.454516888 CEST	49728	443	192.168.2.4	152.199.23.37
Apr 12, 2021 09:30:43.454540014 CEST	49728	443	192.168.2.4	152.199.23.37

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 09:30:34.578136921 CEST	54531	53	192.168.2.4	8.8.8.8
Apr 12, 2021 09:30:34.640104055 CEST	53	54531	8.8.8.8	192.168.2.4
Apr 12, 2021 09:30:35.185735941 CEST	49714	53	192.168.2.4	8.8.8.8
Apr 12, 2021 09:30:35.234519005 CEST	53	49714	8.8.8.8	192.168.2.4
Apr 12, 2021 09:30:36.042802095 CEST	58028	53	192.168.2.4	8.8.8.8
Apr 12, 2021 09:30:36.091407061 CEST	53	58028	8.8.8.8	192.168.2.4
Apr 12, 2021 09:30:39.566015005 CEST	53097	53	192.168.2.4	8.8.8.8
Apr 12, 2021 09:30:39.614768028 CEST	53	53097	8.8.8.8	192.168.2.4
Apr 12, 2021 09:30:40.846093893 CEST	49257	53	192.168.2.4	8.8.8.8
Apr 12, 2021 09:30:40.896308899 CEST	53	49257	8.8.8.8	192.168.2.4
Apr 12, 2021 09:30:41.723522902 CEST	62389	53	192.168.2.4	8.8.8.8
Apr 12, 2021 09:30:41.784208059 CEST	53	62389	8.8.8.8	192.168.2.4
Apr 12, 2021 09:30:43.170629025 CEST	49910	53	192.168.2.4	8.8.8.8
Apr 12, 2021 09:30:43.172379017 CEST	55854	53	192.168.2.4	8.8.8.8
Apr 12, 2021 09:30:43.221049070 CEST	64549	53	192.168.2.4	8.8.8.8
Apr 12, 2021 09:30:43.237215042 CEST	53	55854	8.8.8.8	192.168.2.4
Apr 12, 2021 09:30:43.240854979 CEST	53	49910	8.8.8.8	192.168.2.4
Apr 12, 2021 09:30:43.283854961 CEST	53	64549	8.8.8.8	192.168.2.4
Apr 12, 2021 09:30:47.163029909 CEST	63153	53	192.168.2.4	8.8.8.8
Apr 12, 2021 09:30:47.211579084 CEST	53	63153	8.8.8.8	192.168.2.4
Apr 12, 2021 09:30:48.903703928 CEST	52991	53	192.168.2.4	8.8.8.8
Apr 12, 2021 09:30:48.955811024 CEST	53	52991	8.8.8.8	192.168.2.4
Apr 12, 2021 09:30:50.601283073 CEST	53700	53	192.168.2.4	8.8.8.8
Apr 12, 2021 09:30:50.650140047 CEST	53	53700	8.8.8.8	192.168.2.4
Apr 12, 2021 09:30:59.836519957 CEST	51726	53	192.168.2.4	8.8.8.8
Apr 12, 2021 09:30:59.912904978 CEST	53	51726	8.8.8.8	192.168.2.4
Apr 12, 2021 09:31:02.718218088 CEST	56794	53	192.168.2.4	8.8.8.8
Apr 12, 2021 09:31:02.776968002 CEST	53	56794	8.8.8.8	192.168.2.4
Apr 12, 2021 09:31:03.875019073 CEST	56534	53	192.168.2.4	8.8.8.8
Apr 12, 2021 09:31:03.882917881 CEST	56627	53	192.168.2.4	8.8.8.8
Apr 12, 2021 09:31:03.891386032 CEST	56621	53	192.168.2.4	8.8.8.8
Apr 12, 2021 09:31:03.904808998 CEST	63116	53	192.168.2.4	8.8.8.8
Apr 12, 2021 09:31:03.934113026 CEST	53	56534	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 09:31:03.950686932 CEST	53	56621	8.8.8.8	192.168.2.4
Apr 12, 2021 09:31:03.962254047 CEST	53	63116	8.8.8.8	192.168.2.4
Apr 12, 2021 09:31:03.963937998 CEST	53	56627	8.8.8.8	192.168.2.4
Apr 12, 2021 09:31:04.246608973 CEST	64078	53	192.168.2.4	8.8.8.8
Apr 12, 2021 09:31:04.305052996 CEST	53	64078	8.8.8.8	192.168.2.4
Apr 12, 2021 09:31:06.391772985 CEST	64801	53	192.168.2.4	8.8.8.8
Apr 12, 2021 09:31:06.440553904 CEST	53	64801	8.8.8.8	192.168.2.4
Apr 12, 2021 09:31:07.294369936 CEST	61721	53	192.168.2.4	8.8.8.8
Apr 12, 2021 09:31:07.367722988 CEST	53	61721	8.8.8.8	192.168.2.4
Apr 12, 2021 09:31:07.375009060 CEST	51255	53	192.168.2.4	8.8.8.8
Apr 12, 2021 09:31:07.452588081 CEST	53	51255	8.8.8.8	192.168.2.4
Apr 12, 2021 09:31:07.464745998 CEST	61522	53	192.168.2.4	8.8.8.8
Apr 12, 2021 09:31:07.524912119 CEST	53	61522	8.8.8.8	192.168.2.4
Apr 12, 2021 09:31:08.455502987 CEST	52337	53	192.168.2.4	8.8.8.8
Apr 12, 2021 09:31:08.504163027 CEST	53	52337	8.8.8.8	192.168.2.4
Apr 12, 2021 09:31:11.709834099 CEST	55046	53	192.168.2.4	8.8.8.8
Apr 12, 2021 09:31:11.766972065 CEST	53	55046	8.8.8.8	192.168.2.4
Apr 12, 2021 09:31:11.922339916 CEST	49612	53	192.168.2.4	8.8.8.8
Apr 12, 2021 09:31:11.971256971 CEST	53	49612	8.8.8.8	192.168.2.4
Apr 12, 2021 09:31:12.403685093 CEST	49285	53	192.168.2.4	8.8.8.8
Apr 12, 2021 09:31:12.455398083 CEST	53	49285	8.8.8.8	192.168.2.4
Apr 12, 2021 09:31:12.724056005 CEST	55046	53	192.168.2.4	8.8.8.8
Apr 12, 2021 09:31:12.772881031 CEST	53	55046	8.8.8.8	192.168.2.4
Apr 12, 2021 09:31:13.166614056 CEST	50601	53	192.168.2.4	8.8.8.8
Apr 12, 2021 09:31:13.226478100 CEST	53	50601	8.8.8.8	192.168.2.4
Apr 12, 2021 09:31:13.410136938 CEST	49285	53	192.168.2.4	8.8.8.8
Apr 12, 2021 09:31:13.470027924 CEST	53	49285	8.8.8.8	192.168.2.4
Apr 12, 2021 09:31:13.722676992 CEST	55046	53	192.168.2.4	8.8.8.8
Apr 12, 2021 09:31:13.771724939 CEST	53	55046	8.8.8.8	192.168.2.4
Apr 12, 2021 09:31:14.425597906 CEST	49285	53	192.168.2.4	8.8.8.8
Apr 12, 2021 09:31:14.477128029 CEST	53	49285	8.8.8.8	192.168.2.4
Apr 12, 2021 09:31:15.758095026 CEST	55046	53	192.168.2.4	8.8.8.8
Apr 12, 2021 09:31:15.806595087 CEST	53	55046	8.8.8.8	192.168.2.4
Apr 12, 2021 09:31:16.987096071 CEST	49285	53	192.168.2.4	8.8.8.8
Apr 12, 2021 09:31:17.046869040 CEST	53	49285	8.8.8.8	192.168.2.4
Apr 12, 2021 09:31:18.515506029 CEST	60875	53	192.168.2.4	8.8.8.8
Apr 12, 2021 09:31:18.576658964 CEST	53	60875	8.8.8.8	192.168.2.4
Apr 12, 2021 09:31:19.776366949 CEST	55046	53	192.168.2.4	8.8.8.8
Apr 12, 2021 09:31:19.824953079 CEST	53	55046	8.8.8.8	192.168.2.4
Apr 12, 2021 09:31:20.988698006 CEST	49285	53	192.168.2.4	8.8.8.8
Apr 12, 2021 09:31:21.040359974 CEST	53	49285	8.8.8.8	192.168.2.4
Apr 12, 2021 09:31:21.215708971 CEST	56448	53	192.168.2.4	8.8.8.8
Apr 12, 2021 09:31:21.264410973 CEST	53	56448	8.8.8.8	192.168.2.4
Apr 12, 2021 09:31:22.258886099 CEST	59172	53	192.168.2.4	8.8.8.8
Apr 12, 2021 09:31:22.307576895 CEST	53	59172	8.8.8.8	192.168.2.4
Apr 12, 2021 09:31:27.827488899 CEST	62420	53	192.168.2.4	8.8.8.8
Apr 12, 2021 09:31:27.876153946 CEST	53	62420	8.8.8.8	192.168.2.4
Apr 12, 2021 09:31:28.749253035 CEST	60579	53	192.168.2.4	8.8.8.8
Apr 12, 2021 09:31:28.797941923 CEST	53	60579	8.8.8.8	192.168.2.4
Apr 12, 2021 09:31:29.827549934 CEST	50183	53	192.168.2.4	8.8.8.8
Apr 12, 2021 09:31:29.889019966 CEST	53	50183	8.8.8.8	192.168.2.4
Apr 12, 2021 09:31:40.043010950 CEST	61531	53	192.168.2.4	8.8.8.8
Apr 12, 2021 09:31:40.091716051 CEST	53	61531	8.8.8.8	192.168.2.4
Apr 12, 2021 09:31:43.949306011 CEST	49228	53	192.168.2.4	8.8.8.8
Apr 12, 2021 09:31:43.998027086 CEST	53	49228	8.8.8.8	192.168.2.4
Apr 12, 2021 09:31:55.636276007 CEST	59794	53	192.168.2.4	8.8.8.8
Apr 12, 2021 09:31:55.684946060 CEST	53	59794	8.8.8.8	192.168.2.4
Apr 12, 2021 09:31:59.848927021 CEST	55916	53	192.168.2.4	8.8.8.8
Apr 12, 2021 09:31:59.897872925 CEST	53	55916	8.8.8.8	192.168.2.4
Apr 12, 2021 09:32:08.234915972 CEST	52752	53	192.168.2.4	8.8.8.8
Apr 12, 2021 09:32:08.283832073 CEST	53	52752	8.8.8.8	192.168.2.4
Apr 12, 2021 09:32:28.321472883 CEST	60542	53	192.168.2.4	8.8.8.8
Apr 12, 2021 09:32:28.451842070 CEST	53	60542	8.8.8.8	192.168.2.4
Apr 12, 2021 09:32:28.968429089 CEST	60689	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 09:32:29.070774078 CEST	53	60689	8.8.8.8	192.168.2.4
Apr 12, 2021 09:32:29.477828979 CEST	64206	53	192.168.2.4	8.8.8.8
Apr 12, 2021 09:32:29.537633896 CEST	53	64206	8.8.8.8	192.168.2.4
Apr 12, 2021 09:32:29.963913918 CEST	50904	53	192.168.2.4	8.8.8.8
Apr 12, 2021 09:32:30.020930052 CEST	53	50904	8.8.8.8	192.168.2.4
Apr 12, 2021 09:32:30.180957079 CEST	57525	53	192.168.2.4	8.8.8.8
Apr 12, 2021 09:32:30.252482891 CEST	53	57525	8.8.8.8	192.168.2.4
Apr 12, 2021 09:32:30.705209017 CEST	53814	53	192.168.2.4	8.8.8.8
Apr 12, 2021 09:32:30.806536913 CEST	53	53814	8.8.8.8	192.168.2.4
Apr 12, 2021 09:32:31.966768980 CEST	53418	53	192.168.2.4	8.8.8.8
Apr 12, 2021 09:32:32.024225950 CEST	53	53418	8.8.8.8	192.168.2.4
Apr 12, 2021 09:33:08.363903046 CEST	62833	53	192.168.2.4	8.8.8.8
Apr 12, 2021 09:33:08.422676086 CEST	53	62833	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 12, 2021 09:30:34.578136921 CEST	192.168.2.4	8.8.8.8	0x981b	Standard query (0)	clientconfig.passport.net	A (IP address)	IN (0x0001)
Apr 12, 2021 09:30:43.170629025 CEST	192.168.2.4	8.8.8.8	0x77ff	Standard query (0)	logincdn.msauth.net	A (IP address)	IN (0x0001)
Apr 12, 2021 09:30:43.172379017 CEST	192.168.2.4	8.8.8.8	0x6d2d	Standard query (0)	aadcdn.msftauth.net	A (IP address)	IN (0x0001)
Apr 12, 2021 09:30:43.221049070 CEST	192.168.2.4	8.8.8.8	0xac10	Standard query (0)	raktaxis.co.uk	A (IP address)	IN (0x0001)
Apr 12, 2021 09:30:59.836519957 CEST	192.168.2.4	8.8.8.8	0xca7	Standard query (0)	logincdn.msauth.net	A (IP address)	IN (0x0001)
Apr 12, 2021 09:31:03.891386032 CEST	192.168.2.4	8.8.8.8	0x77a7	Standard query (0)	ajax.aspnetcdn.com	A (IP address)	IN (0x0001)
Apr 12, 2021 09:31:07.294369936 CEST	192.168.2.4	8.8.8.8	0x419d	Standard query (0)	privacy.microsoft	A (IP address)	IN (0x0001)
Apr 12, 2021 09:31:07.375009060 CEST	192.168.2.4	8.8.8.8	0x5fec	Standard query (0)	privacy.microsoft	A (IP address)	IN (0x0001)
Apr 12, 2021 09:31:07.464745998 CEST	192.168.2.4	8.8.8.8	0x8cf5	Standard query (0)	privacy.microsoft	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 12, 2021 09:30:34.640104055 CEST	8.8.8.8	192.168.2.4	0x981b	No error (0)	clientconfig.passport.net	authgfx.msa.akadns6.net		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 09:30:43.237215042 CEST	8.8.8.8	192.168.2.4	0x6d2d	No error (0)	aadcdn.msftauth.net	aadcdnoriginneu.azureedge.net		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 09:30:43.237215042 CEST	8.8.8.8	192.168.2.4	0x6d2d	No error (0)	cs1100.wpc.omegacdn.net		152.199.23.37	A (IP address)	IN (0x0001)
Apr 12, 2021 09:30:43.240854979 CEST	8.8.8.8	192.168.2.4	0x77ff	No error (0)	logincdn.msauth.net	lgincdn.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 09:30:43.240854979 CEST	8.8.8.8	192.168.2.4	0x77ff	No error (0)	cs1227.wpc.alphacdn.net		192.229.221.185	A (IP address)	IN (0x0001)
Apr 12, 2021 09:30:43.283854961 CEST	8.8.8.8	192.168.2.4	0xac10	No error (0)	raktaxis.co.uk		217.160.0.18	A (IP address)	IN (0x0001)
Apr 12, 2021 09:30:59.912904978 CEST	8.8.8.8	192.168.2.4	0xca7	No error (0)	logincdn.msauth.net	lgincdn.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 09:30:59.912904978 CEST	8.8.8.8	192.168.2.4	0xca7	No error (0)	cs1227.wpc.alphacdn.net		192.229.221.185	A (IP address)	IN (0x0001)
Apr 12, 2021 09:31:03.950686932 CEST	8.8.8.8	192.168.2.4	0x77a7	No error (0)	ajax.aspnetcdn.com	mscomajax.vo.msecnd.net		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 09:31:03.962254047 CEST	8.8.8.8	192.168.2.4	0xab2f	No error (0)	consentdeliveryfd.azurefd.net	firstparty-azurefd-prod.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 09:31:07.367722988 CEST	8.8.8.8	192.168.2.4	0x419d	Name error (3)	privacy.microsoft	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 12, 2021 09:31:07.452588081 CEST	8.8.8.8	192.168.2.4	0x5fec	Name error (3)	privacy.microsoft	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 09:31:07.524912119 CEST	8.8.8.8	192.168.2.4	0x8cf5	Name error (3)	privacy.microsoft	none	none	A (IP address)	IN (0x0001)

HTTPS Packets

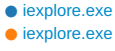
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 12, 2021 09:30:43.355643034 CEST	192.229.221.185	443	192.168.2.4	49727	CN=identitycdn.msauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Jul 20 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013 Fri Nov 10 01:00:00 CET 2006	Tue Jul 20 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023 Mon Nov 10 01:00:00 CET 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
Apr 12, 2021 09:30:43.355854034 CEST	152.199.23.37	443	192.168.2.4	49729	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		
Apr 12, 2021 09:30:43.356098890 CEST	192.229.221.185	443	192.168.2.4	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 Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Jul 20 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013 Fri Nov 10 01:00:00 CET 2006	Tue Jul 20 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023 Mon Nov 10 01:00:00 CET 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		

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 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		
Apr 12, 2021 09:30:43.356302023 CEST	152.199.23.37	443	192.168.2.4	49728	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		
Apr 12, 2021 09:31:00.002074957 CEST	192.229.221.185	443	192.168.2.4	49740	CN=identitycdn.msauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Jul 20 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013 Fri Nov 10 01:00:00 CET 2006	Tue Jul 20 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023 Mon Nov 10 01:00:00 CET 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					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		

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 6780 Parent PID: 800

General

Start time:	09:30:40
Start date:	12/04/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff721b10000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	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: 6860 Parent PID: 6780

General

Start time:	09:30:41

Start date:	12/04/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6780 CREDAT:17410 /prefetch:2
Imagebase:	0x300000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly