ID: 412851
Sample Name: receipt319.html
Cookbook: default.jbs
Time: 01:21:48
Date: 13/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

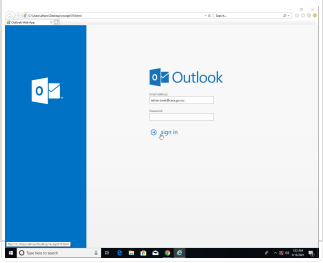
Analysis Report receipt319.html

Overview

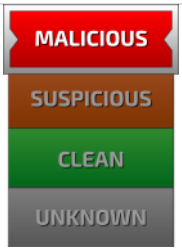
General Information

Sample Name:	receipt319.html
Analysis ID:	412851
MD5:	2c2e3af2ecfca31…
SHA1:	3ebe21a94454b1..
SHA256:	b80c548232c20a..
Infos:	

Most interesting Screenshot:



Detection



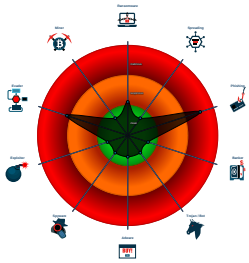
HTMLPhisher

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

Signatures

- Yara detected HtmlPhish44
- Yara detected obfuscated html page
- Obfuscated HTML file found
- Phishing site detected (based on log…
- HTML body contains low number of …
- HTML title does not match URL
- IP address seen in connection with o…
- Invalid T&C link found
- JA3 SSL client fingerprint seen in co…
- None HTTPS page querying sensitiv…

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 4192 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 4636 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4192 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

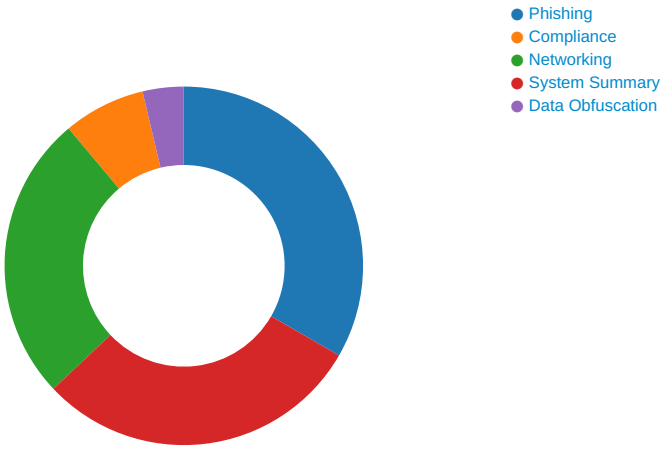
Initial Sample

Source	Rule	Description	Author	Strings
receipt319.html	JoeSecurity_Obshtml	Yara detected obfuscated html page	Joe Security	
receipt319.html	JoeSecurity_HtmlPhish_44	Yara detected HtmlPhish_44	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

Phishing:

Yara detected HtmlPhish44

Yara detected obfuscated html page

Phishing site detected (based on logo template match)

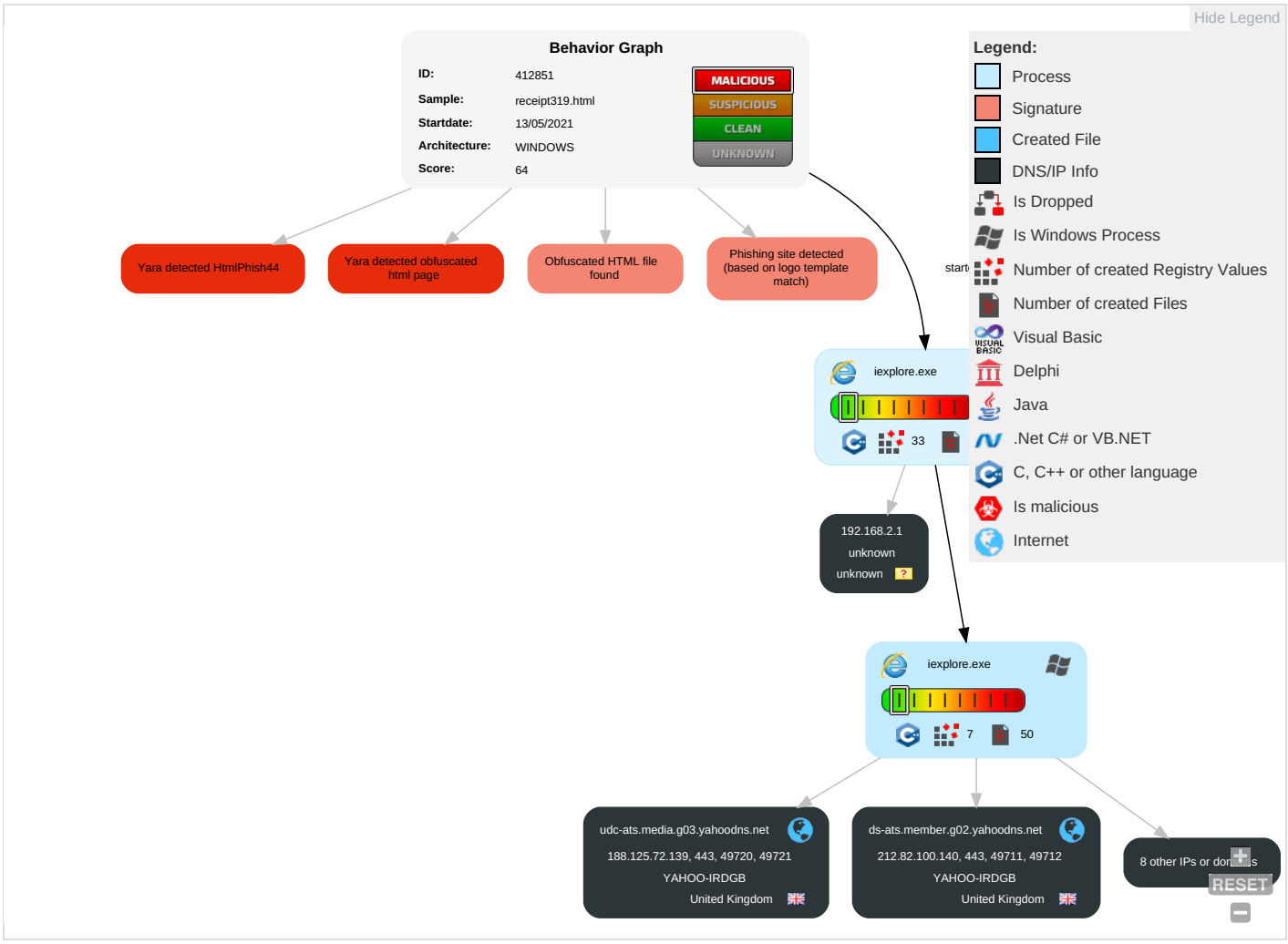
Data Obfuscation:

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	Impact
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 System Partition
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 Lockout
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

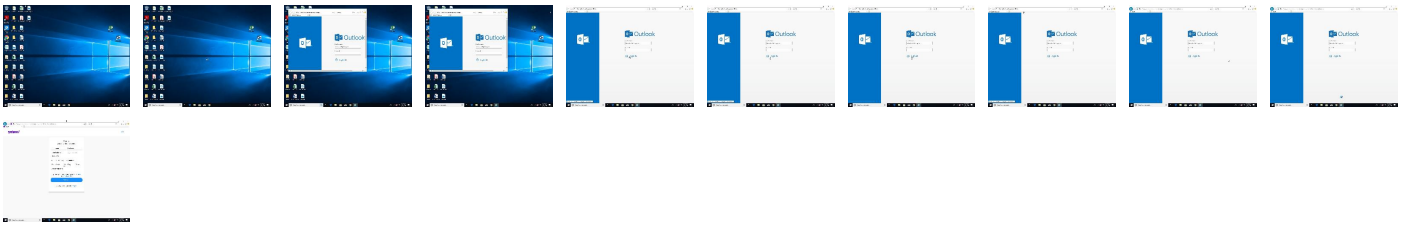
Behavior Graph

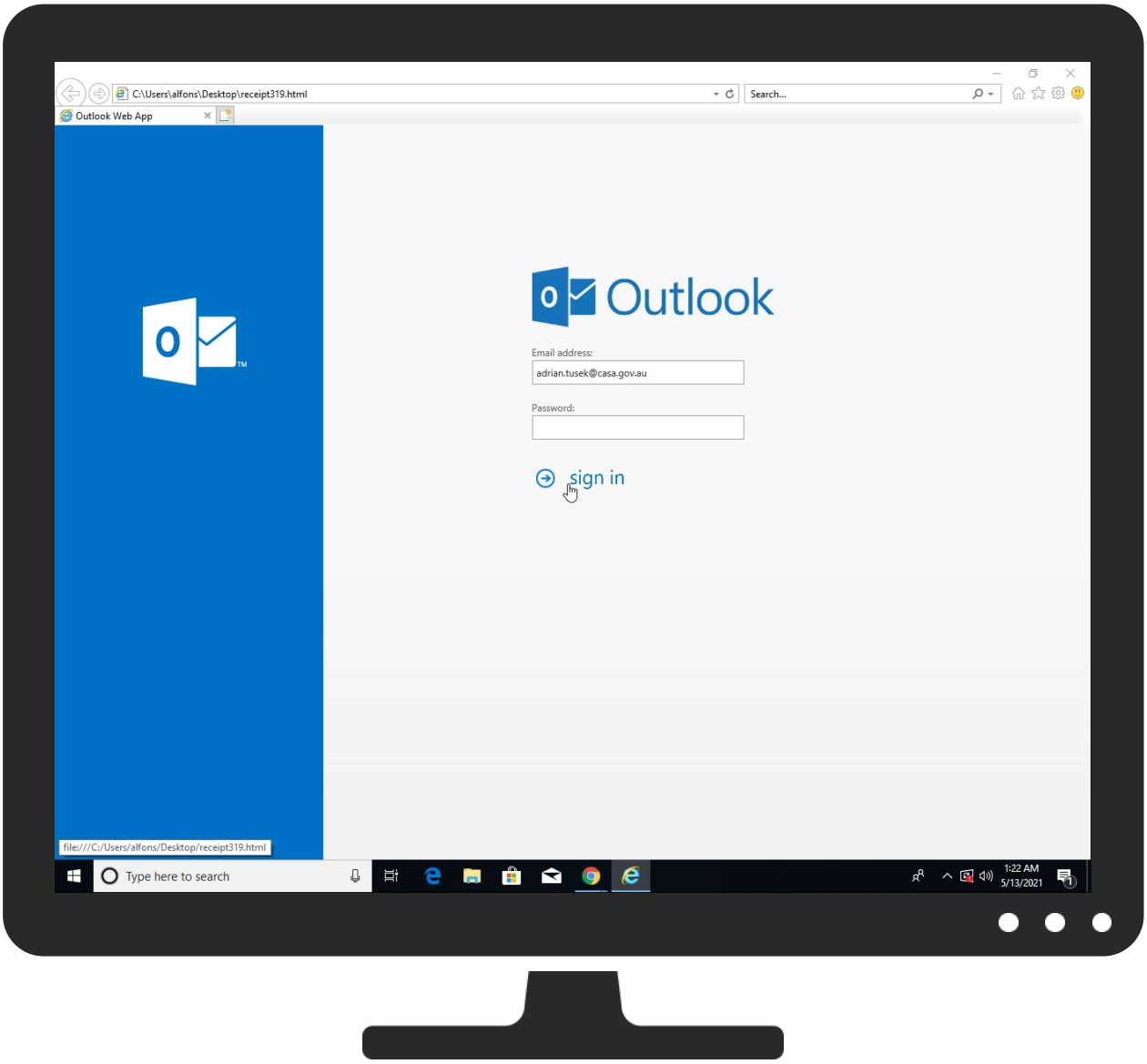


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
geo-atsv2.media.g03.yahoodns.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://login.yahoo.co	0%	Avira URL Cloud	safe	
http://https://www.verizonmedia.com/policies/us/en/verizonmedia/terms/otos/index.html	0%	URL Reputation	safe	
http://https://www.verizonmedia.com/policies/us/en/verizonmedia/terms/otos/index.html	0%	URL Reputation	safe	
http://https://www.verizonmedia.com/policies/us/en/verizonmedia/terms/otos/index.html	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://www.verizonmedia.com/policies/us/en/verizonmedia/privacy/index.html	0%	URL Reputation	safe	
http://https://www.verizonmedia.com/policies/us/en/verizonmedia/privacy/index.html	0%	URL Reputation	safe	
http://https://www.verizonmedia.com/policies/us/en/verizonmedia/privacy/index.html	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
geo-atsv2.media.g03.yahoodns.net	188.125.72.139	true	false	• 0%, Virustotal, Browse	unknown
udc-ats.media.g03.yahoodns.net	188.125.72.139	true	false		unknown
ds-ats.member.g02.yahoodns.net	212.82.100.140	true	false		unknown
edge.gycpi.b.yahoodns.net	87.248.118.23	true	false		unknown
s.yimg.com	unknown	unknown	false		high
udc.yahoo.com	unknown	unknown	false		high
eu.edit.yahoo.com	unknown	unknown	false		high
login.yahoo.com	unknown	unknown	false		high
geo.yahoo.com	unknown	unknown	false		high

Contacted URLs

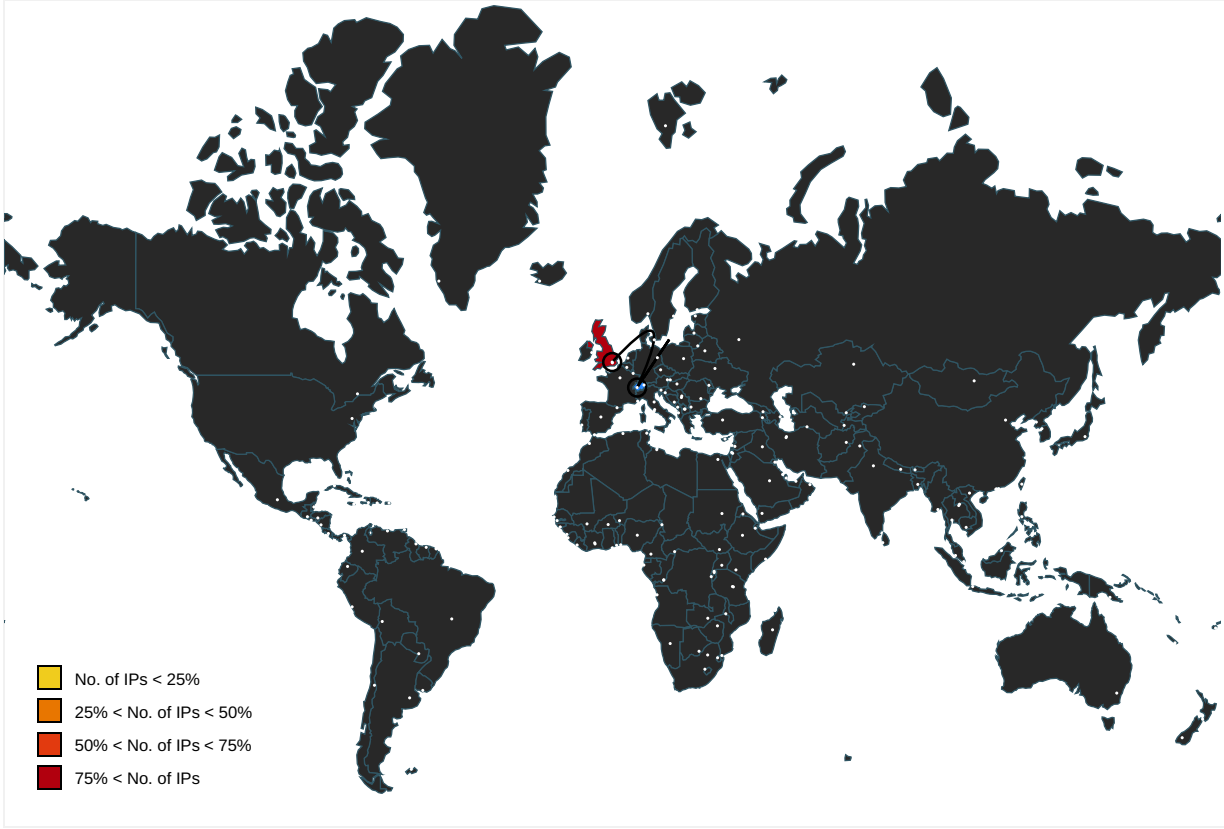
Name	Malicious	Antivirus Detection	Reputation
file:///C:/Users/user/Desktop/receipt319.html	true		low
http://https://login.yahoo.com/account/create?specId=yidReg&altreg=0#yuhead-search	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://s.yimg.com/cv/ae/sports/fonts/2017/Yahoo_Sans-ExtraBold.woff)	yahoo-main[1].css.3.dr	false		high
http://https://s.yimg.com/cv/ae/sports/fonts/2017/Yahoo_Sans-Italic.woff)	yahoo-main[1].css.3.dr	false		high
http://https://s.yimg.com/cv/ae/sports/fonts/2017/Yahoo_Sans-Light.woff)	yahoo-main[1].css.3.dr	false		high
http://https://s.yimg.com/cv/ae/sports/fonts/2017/Yahoo_Sans-Regular.woff)	yahoo-main[1].css.3.dr	false		high
http://https://s.yimg.com/cv/ae/sports/fonts/2017/Yahoo_Sans-ExtraLight.eot);src:url(https://s.yimg.com/cv/	yahoo-main[1].css.3.dr	false		high
http://https://s.yimg.com/cv/ae/sports/fonts/2017/Yahoo_Sans-Italic.eot);src:url(https://s.yimg.com/cv/ae/s	yahoo-main[1].css.3.dr	false		high
http://https://login.yahoo.com/account/create?specId=yidReg&altreg=0#yuhead-search	~DFDC14B9469AEC2819.TMP.1.dr	false		high
http://https://s.yimg.com/wm/mbr/52e318e4b7eb24ab3105befa60106819f8864e34/yahoo-main.css	create[1].htm.3.dr	false		high
http://https://s.yimg.com/cv/ae/sports/fonts/2017/Yahoo_Sans-Bold.woff)	yahoo-main[1].css.3.dr	false		high
http://https://s.yimg.com/cv/ae/sports/fonts/2017/Yahoo_Sans-Black.woff2)	yahoo-main[1].css.3.dr	false		high
http://https://s.yimg.com/cv/ae/sports/fonts/2017/Yahoo_Sans-Medium.eot);src:url(https://s.yimg.com/cv/ae/s	yahoo-main[1].css.3.dr	false		high
http://https://login.yahoo.com/account/create?specId=yidreg&intl=us&altreg=0&con	create[1].htm.3.dr	false		high
http://https://s.yimg.com/rz/p/yahoo_frontpage_en-US_s_f_p_bestfit_frontpage_2x.png	create[1].htm.3.dr	false		high
http://https://github.com/yui/pure/blob/master/LICENSE.md	yahoo-main[1].css.3.dr	false		high
http://https://login.yahoo.com/account/create?specId=yidReg&altreg=0	~DFDC14B9469AEC2819.TMP.1.dr	false		high
http://https://s.yimg.com/cv/ae/sports/fonts/2017/Yahoo_Sans-Semibold.eot);src:url(https://s.yimg.com/cv/ae	yahoo-main[1].css.3.dr	false		high
http://https://login.yahoo.com/	~DFDC14B9469AEC2819.TMP.1.dr	false		high
http://https://s.yimg.com/cv/ae/sports/fonts/2017/Yahoo_Sans-Semibold.woff)	yahoo-main[1].css.3.dr	false		high
http://https://s.yimg.com/cv/ae/sports/fonts/2017/Yahoo_Sans-Bold.eot);src:url(https://s.yimg.com/cv/ae/spo	yahoo-main[1].css.3.dr	false		high
http://https://login.yahoo.co	{5FF79C09-B3C4-11EB-90E5-ECF4BB570DC9}.dat.1.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.verizonmedia.com/policies/us/en/verizonmedia/terms/otos/index.html	create[1].htm.3.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://s.yimg.com/cv/ae/sports/fonts/2017/Yahoo_Sans-Black.eot);src:url(https://s.yimg.com/cv/ae/sp	yahoo-main[1].css.3.dr	false		high
http://https://s.yimg.com/cv/ae/sports/fonts/2017/Yahoo_Sans-ExtraBold.woff2)	yahoo-main[1].css.3.dr	false		high
http://https://mobileexchange.yahoo.com/dismiss	bundle[1].js.3.dr	false		high
http://https://s.yimg.com/wm/mbr/images/yahoo-favicon-img-v0.0.2.ico	create[1].htm.3.dr	false		high
http://https://s.yimg.com/cv/ae/sports/fonts/2017/Yahoo_Sans-Regular.woff2)	yahoo-main[1].css.3.dr	false		high
http://https://s.yimg.com/cv/ae/sports/fonts/2017/Yahoo_Sans-Black.woff)	yahoo-main[1].css.3.dr	false		high
http://https://s.yimg.com/wm/mbr/images/yahoo-favicon-img-v0.0.2.ico~	imagestore.dat.3.dr	false		high
http://https://s.yimg.com/cv/ae/sports/fonts/2017/Yahoo_Sans-Light.woff2)	yahoo-main[1].css.3.dr	false		high
http://https://s.yimg.com/cv/ae/sports/fonts/2017/Yahoo_Sans-Italic.woff2)	yahoo-main[1].css.3.dr	false		high
http://https://www.verizonmedia.com/policies/us/en/verizonmedia/privacy/index.html	create[1].htm.3.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://s.yimg.com/cv/ae/sports/fonts/2017/Yahoo_Sans-Semibold.woff2)	yahoo-main[1].css.3.dr	false		high
http://https://www.yahoo.com/	create[1].htm.3.dr	false		high
http://https://s.yimg.com/cv/ae/sports/fonts/2017/Yahoo_Sans-Light.eot);src:url(https://s.yimg.com/cv/ae/sp	yahoo-main[1].css.3.dr	false		high
http://https://s.yimg.com/wm/mbr/52e318e4b7eb24ab3105befa60106819f8864e34/bundle.js	create[1].htm.3.dr	false		high
http://https://www.yahoo.com	create[1].htm.3.dr, ~DFDC14B9469AEC2819.TMP.1.dr	false		high
http://https://login.yahoo.com/?specId=yidreg&intl=us&done=https%3A%2F%2Fwww.yahoo.c	create[1].htm.3.dr	false		high
http://https://s.yimg.com/cv/ae/sports/fonts/2017/Yahoo_Sans-ExtraLight.woff2)	yahoo-main[1].css.3.dr	false		high
http://https://s.yimg.com/cv/ae/sports/fonts/2017/Yahoo_Sans-ExtraLight.woff)	yahoo-main[1].css.3.dr	false		high
http://https://s.yimg.com/cv/ae/sports/fonts/2017/Yahoo_Sans-Medium.woff)	yahoo-main[1].css.3.dr	false		high
http://https://s.yimg.com/wm/mbr/js/rapid-3.53.17.js	create[1].htm.3.dr	false		high
http://https://s.yimg.com/cv/ae/sports/fonts/2017/Yahoo_Sans-ExtraBold.eot);src:url(https://s.yimg.com/cv/a	yahoo-main[1].css.3.dr	false		high
http://https://s.yimg.com/cv/ae/sports/fonts/2017/Yahoo_Sans-Bold.woff2)	yahoo-main[1].css.3.dr	false		high
http://https://s.yimg.com/rz/p/yahoo_frontpage_en-US_s_f_w_bestfit_frontpage_2x.png	create[1].htm.3.dr	false		high
http://https://s.yimg.com/cv/ae/sports/fonts/2017/Yahoo_Sans-Medium.woff2)	yahoo-main[1].css.3.dr	false		high
http://https://s.yimg.com/cv/ae/sports/fonts/2017/Yahoo_Sans-Regular.eot);src:url(https://s.yimg.com/cv/ae/	yahoo-main[1].css.3.dr	false		high
http://https://s.yimg.com/wm/mbr/images/yahoo-apple-touch-v0.0.2.png	create[1].htm.3.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
188.125.72.139	geo-atsv2.media.g03.yahoodns.net	United Kingdom		34010	YAHOO-IRDGB	false
87.248.118.23	edge.gycpi.b.yahoodns.net	United Kingdom		203220	YAHOO-DEBDE	false
212.82.100.140	ds-ats.member.g02.yahoodns.net	United Kingdom		34010	YAHOO-IRDGB	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	412851
Start date:	13.05.2021
Start time:	01:21:48
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 5s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	receipt319.html
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:	30
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:	mal64.phis.evad.winHTML@3/18@5/4
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .html • Browsing link: https://eu.edit .yahoo.com/registration#yuhead-search
Warnings:	Show All • Excluded IPs from analysis (whitelisted): 204.79.197.200, 13.107.21.200, 93.184.220.29, 104.42.151.234, 20.82.210.154, 40.88.32.150, 88.221.62.148, 142.250.186.170, 23.218.208.56, 152.199.19.161, 92.122.145.220, 2.20.143.16, 2.20.142.209, 92.122.213.194, 92.122.213.247, 20.50.102.62, 20.54.26.129, 20.82.209.183, 52.155.217.156 • TCP Packets have been reduced to 100 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, cs9.wac.phicdn.net, store-images.s-microsoft.com-c.edgekey.net, iris-de-prod-azsc-neu-b.northeurope.cloudapp.azure.com, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcoleus15.cloudapp.net, e12564.dspb.akamaiedge.net, go.microsoft.com, ocsp.digicert.com, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, iris-de-prod-azsc-neu.northeurope.cloudapp.azure.com, fs.microsoft.com, dual-a-0001.a-msedge.net, ajax.googleapis.com, ie9comview.vo.msecnd.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, iris-de-prod-azsc-uks.uksouth.cloudapp.azure.com, ris.api.iris.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, skypedataprdcolwus16.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net, cs9.wpc.v0cdn.net • 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
188.125.72.139	http://us.i1.yimg.com	Get hash	malicious	Browse	• geo.yahoo.com/b?s=1197757129&t=1605726109892&err_url=http%3A%2F%2Fus.i1.yimg.com%2F&err=404&test=-&ats_host=e11.ycpi.deb.yahoo.com&rid=-&message=Not%20Found%20on%20Accelerator&source=brb
87.248.118.23	http://www.prophecyhour.com	Get hash	malicious	Browse	• us.i1.yimg.com/us.yimg.com/i/yg/img/i/us/ui/join.gif
	http://www.forestforum.co.uk/showthread.php?t=47811&page=19	Get hash	malicious	Browse	• yui.yahooapis.com/2.9.0/build/animation/animation-min.js?v=4110
	http://ducvinhqb.com/service.html	Get hash	malicious	Browse	• us.i1.yimg.com/us.yimg.com/i/us/my/addtomyyahoo4.gif

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
edge.gycpi.b.yahoodns.net	50eba5e3_by_Libranalysis.dll	Get hash	malicious	Browse	• 87.248.118.23
	6f61bc36_by_Libranalysis.dll	Get hash	malicious	Browse	• 87.248.118.22
	GmCEpa2M7R.dll	Get hash	malicious	Browse	• 87.248.118.22
	756a6d0d_by_Libranalysis.dll	Get hash	malicious	Browse	• 87.248.118.23
	756a6d0d_by_Libranalysis.dll	Get hash	malicious	Browse	• 87.248.118.22
	XUfPBMTKmF.dll	Get hash	malicious	Browse	• 87.248.118.23
	XUfPBMTKmF.dll	Get hash	malicious	Browse	• 87.248.118.23
	1.dll	Get hash	malicious	Browse	• 87.248.118.22
	1.dll	Get hash	malicious	Browse	• 87.248.118.22
	receipt748.html	Get hash	malicious	Browse	• 87.248.118.22
	9DwsbuAvOT.dll	Get hash	malicious	Browse	• 87.248.118.22
	receipt156.html	Get hash	malicious	Browse	• 87.248.118.22
	f6#Uff09.exe	Get hash	malicious	Browse	• 87.248.118.22
	23cfb512_by_Libranalysis.dll	Get hash	malicious	Browse	• 87.248.118.22
	4af51e1230519e63f96e7dbbbd8b688575bddd2c33bbf.dll	Get hash	malicious	Browse	• 87.248.118.23
	352fbf0bc54cdd36e9241b632267002e0cb9568505e9e.dll	Get hash	malicious	Browse	• 87.248.118.23
	c6d47c1f4051999dda951902c21130bf7a95982fb9a8e.dll	Get hash	malicious	Browse	• 87.248.118.22
	9beb1b3b4e8b86c245f0088e5aaef7a123650668607ec.dll	Get hash	malicious	Browse	• 87.248.118.22
	344c6aed9945a611ec6e8dba62e7c0c4a0bd8ef573acd.dll	Get hash	malicious	Browse	• 87.248.118.22
	011bc15db92fe83fcbb0904253ef539e88a54d6e6ccef.dll	Get hash	malicious	Browse	• 87.248.118.22
geo-atsv2.media.g03.yahoodns.net	receipt748.html	Get hash	malicious	Browse	• 188.125.72.139
	receipt156.html	Get hash	malicious	Browse	• 188.125.72.139
	http://https://survey.alchemer.com/s3/6089047/Contract-Addendum	Get hash	malicious	Browse	• 188.125.72.139
	http://https://performoverlyrefinedapplication.icu/CizCEYfXXsFZDea6dskVLfEdY6BHDc59rTngFTpi7WA?clck=d1b1d4dc-5066-446f-b596-331832cbbdd0&sid=l84343	Get hash	malicious	Browse	• 188.125.72.139
	http://searchlf.com	Get hash	malicious	Browse	• 188.125.72.139

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://us.i1.yimg.com	Get hash	malicious	Browse	• 188.125.72.139
	098BA8ECDC89.exe	Get hash	malicious	Browse	• 188.125.72.139
	http://t.info.clubmed.com/r/?id=h238e54e0,4a3b683d,4a3b6841&p1=millennialsmobile.com/infosispe/admin/67374657068656e2e736865706c6579406368742e6e68732e756b/c3RlcGhlbi5zaGVwbGV5QGNodC5uaHMudWs=	Get hash	malicious	Browse	• 188.125.72.139
ds-ats.member.g02.yahoodns.net	receipt748.html	Get hash	malicious	Browse	• 212.82.100.140
	receipt156.html	Get hash	malicious	Browse	• 212.82.100.140
	http://t.info.clubmed.com/r/?id=h238e54e0,4a3b683d,4a3b6841&p1=millennialsmobile.com/infosispe/admin/67374657068656e2e736865706c6579406368742e6e68732e756b/c3RlcGhlbi5zaGVwbGV5QGNodC5uaHMudWs=	Get hash	malicious	Browse	• 212.82.100.140
	x68H54J7U1.exe	Get hash	malicious	Browse	• 212.82.100.140
	setup.exe	Get hash	malicious	Browse	• 212.82.100.140
	http://https://u.to/swotFQ	Get hash	malicious	Browse	• 212.82.100.140
udc-ats.media.g03.yahoodns.net	receipt748.html	Get hash	malicious	Browse	• 188.125.72.139
	receipt156.html	Get hash	malicious	Browse	• 188.125.72.139
	http://https://survey.alchemer.com/s3/6089047/Contract-Addendum	Get hash	malicious	Browse	• 188.125.72.139
	http://searchlf.com	Get hash	malicious	Browse	• 188.125.72.139
	http://t.info.clubmed.com/r/?id=h238e54e0,4a3b683d,4a3b6841&p1=millennialsmobile.com/infosispe/admin/67374657068656e2e736865706c6579406368742e6e68732e756b/c3RlcGhlbi5zaGVwbGV5QGNodC5uaHMudWs=	Get hash	malicious	Browse	• 87.248.100.136

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
YAHOO-IRDGB	receipt748.html	Get hash	malicious	Browse	• 212.82.100.140
	receipt156.html	Get hash	malicious	Browse	• 212.82.100.140
	espn.html	Get hash	malicious	Browse	• 212.82.100.176
	Install.exe	Get hash	malicious	Browse	• 212.82.100.181
	Ug6Q3IejBj.exe	Get hash	malicious	Browse	• 212.82.100.181
	Five.exe	Get hash	malicious	Browse	• 212.82.100.181
	6BympvyPAv.exe	Get hash	malicious	Browse	• 212.82.100.181
	Three.exe	Get hash	malicious	Browse	• 212.82.100.181
	Four.exe	Get hash	malicious	Browse	• 212.82.100.181
	Six.exe	Get hash	malicious	Browse	• 212.82.100.181
	One.exe	Get hash	malicious	Browse	• 212.82.100.181
	Five.exe	Get hash	malicious	Browse	• 212.82.100.181
	Two.exe	Get hash	malicious	Browse	• 212.82.100.181
	SecuriteInfo.com.Variant.Bulz.385171.11582.exe	Get hash	malicious	Browse	• 212.82.100.181
	Information_76612.xlsb	Get hash	malicious	Browse	• 87.248.100.215
	Attachment_.xlsb	Get hash	malicious	Browse	• 87.248.100.216
	Information.xlsb	Get hash	malicious	Browse	• 87.248.100.215
	GMMs2zuyG4.exe	Get hash	malicious	Browse	• 87.248.100.215
	Info_148977.xlsb	Get hash	malicious	Browse	• 87.248.100.215
	Attachment_145854.xlsb	Get hash	malicious	Browse	• 87.248.100.215
YAHOO-DEBDE	50eba5e3_by_Libranalysis.dll	Get hash	malicious	Browse	• 87.248.118.23
	6f61bc36_by_Libranalysis.dll	Get hash	malicious	Browse	• 87.248.118.22
	GmCEpa2M7R.dll	Get hash	malicious	Browse	• 87.248.118.22
	756a6d0d_by_Libranalysis.dll	Get hash	malicious	Browse	• 87.248.118.23
	756a6d0d_by_Libranalysis.dll	Get hash	malicious	Browse	• 87.248.118.22
	XUfPBMTKmF.dll	Get hash	malicious	Browse	• 87.248.118.23
	XUfPBMTKmF.dll	Get hash	malicious	Browse	• 87.248.118.23
	1.dll	Get hash	malicious	Browse	• 87.248.118.22
	1.dll	Get hash	malicious	Browse	• 87.248.118.22
	receipt748.html	Get hash	malicious	Browse	• 87.248.118.22
	9DwsbuAvOT.dll	Get hash	malicious	Browse	• 87.248.118.22
	receipt156.html	Get hash	malicious	Browse	• 87.248.118.22
	f6#Uff09.exe	Get hash	malicious	Browse	• 87.248.118.22
	23cfb512_by_Libranalysis.dll	Get hash	malicious	Browse	• 87.248.118.22
	4af51e1230519e63f96e7dbbbd8b688575bddd2c33bbf.dll	Get hash	malicious	Browse	• 87.248.118.23
	352fbf0bc54cdd36e9241b632267002e0cb9568505e9e.dll	Get hash	malicious	Browse	• 87.248.118.23
	c6d47c1f4051999dda951902c21130bf7a95982fb9a8e.dll	Get hash	malicious	Browse	• 87.248.118.22

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	9beb1b3b4e8b86c245f0088e5aaef7a123650668607ec.dll	Get hash	malicious	Browse	• 87.248.118.22
	344c6aed9945a611ec6e8dba62e7c0c4a0bd8ef573acd.dll	Get hash	malicious	Browse	• 87.248.118.22
	011bc15db92fe83fcbb0904253ef539e88a54d6e6ccef.dll	Get hash	malicious	Browse	• 87.248.118.22

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
9e10692f1b7f78228b2d4e424db3a98c	50eba5e3_by_Libranalysis.dll	Get hash	malicious	Browse	• 188.125.72.139 • 87.248.118.23 • 212.82.100.140
	6f61bc36_by_Libranalysis.dll	Get hash	malicious	Browse	• 188.125.72.139 • 87.248.118.23 • 212.82.100.140
	50eba5e3_by_Libranalysis.dll	Get hash	malicious	Browse	• 188.125.72.139 • 87.248.118.23 • 212.82.100.140
	6f61bc36_by_Libranalysis.dll	Get hash	malicious	Browse	• 188.125.72.139 • 87.248.118.23 • 212.82.100.140
	1ChCpaSGY7.dll	Get hash	malicious	Browse	• 188.125.72.139 • 87.248.118.23 • 212.82.100.140
	595e3339_by_Libranalysis.dll	Get hash	malicious	Browse	• 188.125.72.139 • 87.248.118.23 • 212.82.100.140
	GmCEpa2M7R.dll	Get hash	malicious	Browse	• 188.125.72.139 • 87.248.118.23 • 212.82.100.140
	XPBPS2DL.exe	Get hash	malicious	Browse	• 188.125.72.139 • 87.248.118.23 • 212.82.100.140
	nT5pUwoJSS.dll	Get hash	malicious	Browse	• 188.125.72.139 • 87.248.118.23 • 212.82.100.140
	4xPBZai06p.dll	Get hash	malicious	Browse	• 188.125.72.139 • 87.248.118.23 • 212.82.100.140
	rAd00Nae9w.dll	Get hash	malicious	Browse	• 188.125.72.139 • 87.248.118.23 • 212.82.100.140
	756a6d0d_by_Libranalysis.dll	Get hash	malicious	Browse	• 188.125.72.139 • 87.248.118.23 • 212.82.100.140
	756a6d0d_by_Libranalysis.dll	Get hash	malicious	Browse	• 188.125.72.139 • 87.248.118.23 • 212.82.100.140
	jjbxg8kh5X.exe	Get hash	malicious	Browse	• 188.125.72.139 • 87.248.118.23 • 212.82.100.140
	- FAX ID 74172012198198.htm	Get hash	malicious	Browse	• 188.125.72.139 • 87.248.118.23 • 212.82.100.140
	XUfPBMTKmF.dll	Get hash	malicious	Browse	• 188.125.72.139 • 87.248.118.23 • 212.82.100.140
	XUfPBMTKmF.dll	Get hash	malicious	Browse	• 188.125.72.139 • 87.248.118.23 • 212.82.100.140
	Report000042.htm	Get hash	malicious	Browse	• 188.125.72.139 • 87.248.118.23 • 212.82.100.140
	FuiZSHt8Hx.dll	Get hash	malicious	Browse	• 188.125.72.139 • 87.248.118.23 • 212.82.100.140
	#Ud83d#Udce9-vesna.starcevic.htm	Get hash	malicious	Browse	• 188.125.72.139 • 87.248.118.23 • 212.82.100.140

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\DURNCK2N\login.yahoo[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	13
Entropy (8bit):	2.469670487371862
Encrypted:	false
SSDEEP:	3:D90aKb:JFKb
MD5:	C1DDEA3EF6BBEF3E7060A1A9AD89E4C5
SHA1:	35E3224FCBD3E1AF306F2B6A2C6BBEA9B0867966
SHA-256:	B71E4D17274636B97179BA2D97C742735B6510EB54F22893D3A2DAFF2CEB28DB
SHA-512:	6BE8CEC7C862AFAE5B37AA32DC5BB45912881A3276606DA41BF808A4EF92C318B355E616BF45A257B995520D72B7C08752C0BE445DCEADE5CF79F73480910FE D
Malicious:	false
Reputation:	high, very likely benign file
Preview:	<root></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{5FF79C07-B3C4-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	45144
Entropy (8bit):	1.9472469266465078
Encrypted:	false
SSDEEP:	96:rkZrZv2qWDtrbfzpqKM9yqEwMQvxfKpb6rrj6lEgu4fLpbKMcB3g:rkZrZv2qWDtPfzRMbdJfKMryk5fL8MCg
MD5:	BBE0A6D475C2A4BC6C1561B9FDB780BE
SHA1:	6EAEB45BA1F14FAA9D6A4C170C70586E3948EE2C
SHA-256:	D35F6795F3C6E124511B27ED580C4296398F1F56779A173D284793C2D3091640
SHA-512:	DEE6F733B06D49E99512AF4C29BFB348BEF570B76810E8A6249496AF2EEB490980015083CFB89FE866432CBC492AAC3F26824F0CDAD7AF9B8CDE36454946F52
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\{5FF79C09-B3C4-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	79622
Entropy (8bit):	3.3627399357359917
Encrypted:	false
SSDEEP:	768:Lc2QksS9M4NorfveFoNi3V9qjduH0u/9/rzDbG2Z:LJhsSe4NoDvYI4VQUUu/VHDbn
MD5:	34081615EAE11E51EB849510683A837B
SHA1:	308B4C8206309CD0AFDD1DAD7E1C4A101D985269
SHA-256:	5A356223D2CD8EA593AE6776D47ABF34F6F1085E202AECD4809C59343D12BF5D
SHA-512:	3F24E54992918F081A0194A81E08A971FF348C5168EC9022B1ACF1FF6312D72D422F6F7887B3F979D8FE0880E6E288D0B8F31ED10A2A32B1CF0A5C387FD52830
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\{5FF79C0A-B3C4-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	19032
Entropy (8bit):	1.5856338900644806
Encrypted:	false
SSDEEP:	48:IwDGcprhGwpawG4pQnGrapbSpGQpKWG7HpReTGIpX2wMGApm:r5Z7Qw67BSjABTaFcg

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{5FF79C0A-B3C4-11EB-90E5-ECF4BB570DC9}.dat	
MD5:	42AEE30BCC7D768AA9C3B4CBDC570876
SHA1:	3EDA575A8B7407EEA252762E316943000F7E32F1
SHA-256:	B616DC6506A85D7B78D99A27A1A4AE54F838846B9B3304DB2131D86389315C3B
SHA-512:	0074AD31A724D72D1CD64B54F0F4585021172C61EAA1BB5B28E7F4137ABC74312B0E0B45D2BF389340894A55F29DABB2DE8E5871CDBAC565583E05CB789DB69E
Malicious:	false
Reputation:	low
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\dikxvqf\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	modified
Size (bytes):	1566
Entropy (8bit):	1.9768366693316983
Encrypted:	false
SSDEEP:	12:2otWXrDEj4LM6gyh82eqExk+uvbAzNc14dCV:2mWXv46Jh8lqExkN6cyYV
MD5:	47C039803EF4F928EBFD624B14FEB32D
SHA1:	B9C297F34E55CD1549B5C1CEC8B9471796CB4043
SHA-256:	504A75579BD3453BD70BE666161B19C8DAD9F57A2DE79162CFF4897E81E84966
SHA-512:	A688C3F733731A541C25501190D9AE72CFE5813C6B91EA4A34666FB761CED679A4511C60F20CE21512D9C1C1DB54B1E4D3AB8FE9CDB9BDDE2BCCA1F6A08B3AB
Malicious:	false
Reputation:	low
Preview:	=.h.t.t.p.s.:././.s...y.i.m.g...c.o.m./.w.m./.m.b.r./.i.m.a.g.e.s./.y.a.h.o.o.-.f.a.v.i.c.o.n.-.i.m.g.-.v.0...0...2...i.c.o.~.....h.....(..... .....`...d...f...i...k...m...p...q...s.. s..$v..*z..?...D...M...V..._...b...c...l...v...y...|.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\rapid-3.53.17[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	downloaded
Size (bytes):	48857
Entropy (8bit):	5.367628990985338
Encrypted:	false
SSDEEP:	768:d+YVFXWFNmGd69gsBScjPmsk7jIm9zC3mPsr2X9XbBDmFrhkH7zqDN:A4FhGd69vBDusIjlW3mEr2X9XbBC1hN
MD5:	A554692F884A1B33A1BDC7EEBB3A7F98
SHA1:	66DB96F617A8DD6806646EDCF56C29B4D57FAFE1
SHA-256:	35BD38D45EAF99465A72BB4E02BE6C310BBA85CCBA2660161F410343789A9B0E
SHA-512:	9674EECE51AE0D778880EE822BD56797FB42BC252C1B022364DA341CD9FB62B4BC65CDDBA07278A94083998B0B1BFA5E9731793E4F1338B88E27A788E02F590
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://s.yimg.com/wm/mbr/js/rapid-3.53.17.js
Preview:	!function(){"undefined"!=typeof YAHOO&&YAHOO||(YAHOO={}),YAHOO.i13n=YAHOO.i13n||{},YAHOO.i13n.EventTypes=function(){var e="richview";function t(e,t,n){this.yqlid=e,this.eventName=t,this.spaceidPrefix=n}t.prototype={getYQLID:function(){return this.yqlid},getEventName:function(){return this.eventName}};var n={pageview:new t("pv","pageview",""),simple:new t("lv","event","P"),linkview:new t("lv","linkview","P"),richview:new t(e,e,"R"),contentmodification:new t(e,"contentmodification","R"),dwell:new t("lv","dwell","D")};return{getEventByName:function(e){return n[e]}}}();var se="3.53.17",le="VERSIONED-NON-PROD",ce=[];YAHOO.i13n.__RAPID_INSTANCES__=ce,YAHOO.i13n.__RAPID_INFO__={version:se,comboName:le},YAHOO.i13n.Rapid=function(s){var h={};function e(){}function p(e){this.map={},this.count=0,e&&this.absorb(e)}function g(){this.map={},this.count=0}"undefined"!=typeof console&&void 0!==console.log||(console={log:function(){}}),void 0===console.error&&(console.error=console.log),void 0===console

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\yahoo_frontpage_en-US_s_f_p_bestfit_frontpage_2x[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 240 x 72, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	1346
Entropy (8bit):	7.811113028134073
Encrypted:	false
SSDEEP:	24:DzhV0C4bz+BXH/Adox88K9LDNiF6/LodoLopZYGBLn4AcXGKgF13+2HBoHVMnozC:D9jXBFxfKFljRL0YGBrLcW7F13+MBoHC
MD5:	CD166981C96C6D0F4B5A7D798C25878E
SHA1:	09031C4013138BB8BD54AB9092AC59AA47D7C60C
SHA-256:	0FDEFE26BAC6A6B0B06FE67984582F887AF70B7DA25D6CB1B401F9074DB58338

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\yahoo_frontpage_en-US_s_f_p_bestfit_frontpage_2x[1].png	
SHA-512:	6D217A81DFDCFD601C3F6D9CDE3F1BE0C4D4FFEF85B02B06208014101456CA730EF759BD51637966C9F2572080B79E8A2F9D45A2087DDC40DF015F8C052DA5(
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://s.yimg.com/rz/p/yahoo_frontpage_en-US_s_f_p_bestfit_frontpage_2x.png
Preview:	.PNG.....IHDR.....H.....*PLTEGpLa..a..a..r..`..`..`..`..b..a..`..e..`....I.....tRNS.T{j....*=...Pau>....IDATx...#).F.....'.&.1..5.-...t.....9....]0.....3.....,o..8p...r^<v....v.n.....Z....:,..p...%kw..y.;p..~w.H..m..%kw`.....)%...V.z....n.%.}.....G.C....Q...W.....G:_]..r4..^.Bh.$.F.;R.,+.R......"s..I.T. ..I.5..H..N.c>.Q.....<...G.w.....U.]R.!pP.Y.:T..Q.H.qU..... t....\|...hD...'...?.YEe.....A.U.t.....F.,1.:...:lU....k M*.b...;...{.....b..F..O...i_.?.V..~."....>..h.da...e.I.....5.\..#...*./7....1...t.8....U..... g9nZ..lR..d.\|...l.T..@.$J.....E.J.....%kt.j.s.J.0 .d..7...3O.....I..u..1p6$.X....$f .N.b.j..t.....ZqI...A)@...9qn..zj.|F...<...S\...$.t.$3=.C.....IV.....mIm....eKo.A.E.`.....do..._..(FRg..[....<~...a...Y;..~`o....2...s..ZK\~/G.g.-Z..p 0..m..../H.....%....o.;.xU_.q^.(.....&%..jn...n:..dE.g6..y-2'n..... .q..e``.^.$.^...X| ..(>!.EvI.....r.I.N...;.....Q...+....x.Uw....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\fuji-spinner-1.0.1[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	4853
Entropy (8bit):	5.004932223281782
Encrypted:	false
SSDEEP:	24:t4ptffMVPFhjD2naMxoFnaRhxokr9xoNxohroSmmoNmkoXcUo76jxoYxotLMVPFe:olU7C0EyP96OA7C0EyP96qIV
MD5:	1371FB7EA1D9F283B0964F6D9FEDF183
SHA1:	3A4AD980032FE8E6277087FCDA87C4E0A699DA97
SHA-256:	186034DA48941B64B5F6B4D8A0176FB86E2AD6ADDA436B8EEEF521B0166D06C5
SHA-512:	427495C5914ECFC85ACCC176A5C3DDA83D7E4E2ABADA45414399A5F4B30D9A656AF823B5A4E6ABADC69FFC35C3DC99A7ADBADD422C453865E9E5A9C5FBE2 A58E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://s.yimg.com/wm/modern/images/fuji-spinner-1.0.1.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="100%" height="100%" viewBox="-25 -25 100 100" version="1.1"><g><path d="M25 0 A25 25 0 0 0 25 50" stroke-dasharray="79" stroke="#eeeeee" stroke-width="4" stroke-linecap="round" fill="none"> Expanding and contracting of the arc --><animate id="a1" attributeType="XML" attr ibuteName="stroke-dashoffset" from="9" to="76" dur="625ms" begin="0s; a2.end" fill="freeze" calcMode="spline" keyTimes="0;1" keySplines="0.215, 0.61, 0.355, 1"/> <animate id="a2" attributeType="XML" attributeName="stroke-dashoffset" from="76" to="9" dur="625ms" begin="a1.end" fill="freeze" calcMode="spline" keyTimes="0;1" keySplines="0.215, 0.61, 0.355, 1"/> Change of the stroke width --><animate id="a3" attributeType="XML" attributeName="stroke-width" from="4" to="8" dur="625ms" begin="0s; a4.end" fill="freeze" calcMode="spline" keyTimes="0;1" keySplines="0.215, 0.61, 0.355, 1"/><animate id="a4" attributeType="XML" attributeName="stroke-wid th" from="8" to="4" dur="6

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\fuji-spinner-dark-1.0.0[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	8495
Entropy (8bit):	3.7849183274465985
Encrypted:	false
SSDEEP:	48:03F7QwnVs40c5pkoRc4PTfd7QwnVs40c5pkoRc4PTVUV:017+8m017+8m0W
MD5:	14086B7195375BCCE2BDE04674B9B9B4
SHA1:	1E76715EEFCD39440DC1DB5C75562A5AC3D4A205
SHA-256:	DFDFC7BDB98046A73135708556FBC93E2053A86165F76BEE2A76D99539402A46
SHA-512:	1A7B643C60319E404B53FAD8B094D794A933FCCA6D3F3EEFE1EDE9473550F2ADECC33247CF9A2337D24E6F46180377610D445622021DAF7CEC0FA3A9403F133
Malicious:	false
IE Cache URL:	http://https://s.yimg.com/wm/modern/images/fuji-spinner-dark-1.0.0.svg
Preview:	<svg width="100%" height="100%" viewBox="-25 -25 100 100" xmlns="http://www.w3.org/2000/svg" version="1.1">. <g>. <path d="M25,0 A25,25 0 0,0 25,50" s troke-dasharray="79" stroke="#b9bdc5" stroke-width="4" stroke-linecap="round" fill="none">. Expanding and contracting of the arc -->. <animate id="a1" attributeType="XML". attributeName="stroke-dashoffset". from="9". to="76". dur="625ms". begin="0s; a2.end". fill="freeze". calcMode="spline". keyTimes="0;1". keySplines="0.215, 0.61, 0.355, 1". />. <animate id="a2" attributeTyp e="XML". attributeName="stroke-dashoffset". from="76". to="9". dur="625ms". begin="a1.end". fill="freeze". calcMode="spline". keyTimes="0;1". k

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\jquery.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	85578
Entropy (8bit):	5.366055229017455
Encrypted:	false
SSDEEP:	1536:EYE1JVoiB9JqZdXXe2pD3PgoIiulrUndZ6a4tfOR7WpfWBZ2BJda4w9W3qG9a986:v4J+OlfOhWppCW6G9a98Hr2
MD5:	2F6B11A7E914718E0290410E85366FE9
SHA1:	69BB69E25CA7D5EF0935317584E6153F3FD9A88C
SHA-256:	05B85D96F41FFF14D8F608DAD03AB71E2C1017C2DA0914D7C59291BAD7A54F8E

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\jquery.min[1].js	
SHA-512:	0D40BCCAA59FEDECF7243D63B33C42592541D0330FEFC78EC81A4C6B9689922D5B211011CA4BE23AE22621CCE4C658F52A1552C92D7AC3615241EB640F8514B
Malicious:	false
IE Cache URL:	http://https://ajax.googleapis.com/ajax/libs/jquery/2.2.4/jquery.min.js
Preview:	/*! jQuery v2.2.4 | (c) jQuery Foundation | jquery.org/license */!function(a,b){"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a document");return b(a)}:b(a)}("undefined"!=typeof window?window:this,function(a,b){var c=[],d=a.document,e=c.slice,f=c.concat,g=c.push,h=c.indexOf,i={},j=i.toString,k=i.hasOwnProperty,l={},m="2.2.4",n=function(a,b){return new n.fn.init(a,b)},o=/^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g,p=/^-ms-/,q=/-([\da-z])/gi,r=function(a,b){return b.toUpperCase()};n.fn=n.prototype={jquery:m,constructor:n,selector:"",length:0,toArray:function(){return e.call(this)},get:function(a){return null!=a?0>a?this[a+this.length]:this[a]:e.call(this)},pushStack:function(a){var b=n.merge(this.constructor(),a);return b.prevObject=this,b.context=this.context,b},each:function(a){return n.each(this,a)},map:function(a){return this.pushStack(n.map(this,function(b,c){return a.call

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\bundle[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	171069
Entropy (8bit):	5.383049736315531
Encrypted:	false
SSDEEP:	1536:CE9TaOeZnqw1/AN0nVxRxjh0bVm2hegWuVF2RQZ2W6RPoO0EWJdrDaCQnCnzuJyD:Z9TfebDLeVzW02DwIdY+9B5m
MD5:	DE8C59A0F142B9C87CA8C65D517FB1B0
SHA1:	89D6D592DEB77B048FBCDBDA3167B2A9FE576CD7
SHA-256:	E2A2CB1B44E79B82DA9D40CA3C618E54D819B3F332511921022E77BC9C23AD58
SHA-512:	EF58CB9453A09BC4CB4523FE3A31E5C7A96F1439551FF32A12DC6DBC7B74269BFCEDB0024FE90EF0AAD0772E24A8C52B8426E2570D36B3F03DF7CCCBFADD057
Malicious:	false
IE Cache URL:	http://https://s.yimg.com/wm/mbr/52e318e4b7eb24ab3105befa60106819f8864e34/bundle.js
Preview:	(function(){function r(e,n,t){function o(i,f){if(!n[i]){if(!e[i]){var c="function"==typeof require&&require;if(!f&&c)return c(i,!0);if(u)return u(i,!0);var a=new Error("Cannot find module '"+i+"'");throw a.code="MODULE_NOT_FOUND",a}var p=n[i]={exports:{}};e[i][0].call(p.exports,function(r){var n=e[i][1][r];return o(n||r)},p,p.exports,r,e,n,t)}return n[i].exports}for(var u="function"==typeof require&&require,i=0;i<t.length;i++)o(t[i]);return o}return r})()({1:[function(require,module,exports){.!function(e,t,n){"use strict";"undefined"!=typeof window&&"function"==typeof define&&define.amd?define(n):"undefined"!=typeof module&&module.exports?module.exports=n():t.exports?t.exports=n():t.Fingerprint2=n()}(0,this,function(){"use strict";var e=function(e,t){e=[e[0]>>>16,65535&e[0],e[1]>>>16,65535&e[1]],t=[t[0]>>>16,65535&t[0],t[1]>>>16,65535&t[1]];var n=[0,0,0,0];return n[3]+=e[3]+t[3],n[2]+=n[3]>>>16,n[3]&=65535,n[2]+=e[2]+t[2],n[1]+=n[2]>>>16,n[2]&=65535,n[1]+=e[1]+t[1],n[0]+=n[1]>>>16,n[1]

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\yahoo-favicon-img-v0.0.2[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 1 icon, 16x16, 8 bits/pixel
Category:	downloaded
Size (bytes):	1406
Entropy (8bit):	1.6826987302732233
Encrypted:	false
SSDEEP:	6:ZM6MdN4jF8VGH0xnYOqEiCNc/+O1t+KbAzNct/XTXP0zyQ59:ZM6gyh82eqExk+uvbAzNc14d
MD5:	B6814AE5582D7953821ACBD76E977BB4
SHA1:	75A33FC706C2C6BA233E76C17337E466949F403C
SHA-256:	4A491ACD00880C407A2B749619003716C87E9C25AC344E5934C13E8F9AA0E8B3
SHA-512:	958268F22E72875B97C42D8927E6A1D6168C94FE2184DE906029688A9D63038301DF2E3DE57E571A3D0ECC7AD41178401823E5C54576936D37C84C7A3ED8EF6B
Malicious:	false
IE Cache URL:	http://https://s.yimg.com/wm/mbr/images/yahoo-favicon-img-v0.0.2.ico
Preview:	.....h.....(..... .....`...d...f...i...k...m...p...q...s.. s..$v..*z..?...D...M...V..._...b...c...l...v...y...|..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\create[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines
Category:	dropped
Size (bytes):	63923
Entropy (8bit):	5.826804742941375
Encrypted:	false
SSDEEP:	1536:ZS1FcbCYdJlb07t7HPNCWkQGUmqhzT5hk8y61U:ZYm6tvuUmqhzfOJ
MD5:	9F77F9B640DF34F100D4601114747B87
SHA1:	17BC41F781C2B90AB27C2ADBD0600D5DF3471414
SHA-256:	867AB318792CE27D5BCFCCC9E349CD2F06BB65965451230C67DA8EAAB44C27E8
SHA-512:	CCE177B427838042B246EFE0BA9D2179A0F01022293F6BF4B85AC2828B26B5D66C3BC64B4CA190BB98C064DF255CA9C14084557D650492F6FE87D0869AA5E9B
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\create[1].htm	
Preview:	<!DOCTYPE html>.<html id="Stencil" class="no-js light-theme ">. <head>. <meta charset="utf-8">. <meta name="viewport" content="initial-scale=1, maximum-scale=1, user-scalable=0, shrink-to-fit=no"/>. <meta name="format-detection" content="telephone=no">. <meta name="referrer" content="origin">. <title> Yahoo</title>. <meta name="description" content="Yahoo" />. <link rel="dns-prefetch" href="//gstatic.com">. <link rel="dns-prefetch" href="//google.com">. <link rel="dns-prefetch" href="//s.yimg.com">. <link rel="dns-prefetch" href="//y.analytics.yahoo.com">. <link rel="dns-prefetch" href="//ucs.query.yahoo.com">. <link rel="dns-prefetch" href="//geo.query.yahoo.com">. <link rel="dns-prefetch" href="//geo.yahoo.com">. <link rel="icon" type="image/x-icon" href="https://s.yimg.com/wm/mbr/images/yahoo-favicon-img-v0.0.2.ico">. <link rel="shortcut icon" type="image/x-icon" href="https://

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\yahoo-main[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	472057
Entropy (8bit):	5.581767981003796
Encrypted:	false
SSDEEP:	6144:4LZrmuBvlMv6BNvVHqrgrSpB+vtraoY6vBZVi:crmuzaNB+vtraoYsZVi
MD5:	D23C05BF97AF8A566967F5E485209C70
SHA1:	23CEC0CF2798A5E56F74C13EC3B17B1086DF8881
SHA-256:	F24B67ABEB9533E60A8ECB516DE56DC64A360587E19707C3E368779E3FCED537
SHA-512:	868F47A88A235136E8AB723D98F308A3EFAA89BAAA079411C8BA51FF381CE0F8090156805A325712997649CC701EDA925B2A2FB3BC069801D2768F2A9A08F1F5
Malicious:	false
IE Cache URL:	http://https://s.yimg.com/wm/mbr/52e318e4b7eb24ab3105befa60106819f8864e34/yahoo-main.css
Preview:	@font-face{font-family:"Yahoo Sans";font-display:block;src:url(https://s.yimg.com/cv/ae/sports/fonts/2017/Yahoo_Sans-ExtraLight.eot);src:url(https://s.yimg.com/cv/ae/sports/fonts/2017/Yahoo_Sans-ExtraLight.eot?#iefix) format("embedded-opentype"),url(https://s.yimg.com/cv/ae/sports/fonts/2017/Yahoo_Sans-ExtraLight.woff2) format("woff2"),url(https://s.yimg.com/cv/ae/sports/fonts/2017/Yahoo_Sans-ExtraLight.woff) format("woff");font-weight:200;font-style:normal}@font-face{font-family:"Yahoo Sans";font-display:block;src:url(https://s.yimg.com/cv/ae/sports/fonts/2017/Yahoo_Sans-Light.eot);src:url(https://s.yimg.com/cv/ae/sports/fonts/2017/Yahoo_Sans-Light.eot?#iefix) format("embedded-opentype"),url(https://s.yimg.com/cv/ae/sports/fonts/2017/Yahoo_Sans-Light.woff2) format("woff2"),url(https://s.yimg.com/cv/ae/sports/fonts/2017/Yahoo_Sans-Light.woff) format("woff");font-weight:300;font-style:normal}@font-face{font-family:"Yahoo Sans";font-display:block;src:url(https://s.yimg.com/cv/ae/sports/f

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\yahoo_frontpage_en-US_s_f_w_bestfit_frontpage_2x[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 240 x 72, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	1391
Entropy (8bit):	7.763598788410441
Encrypted:	false
SSDEEP:	24:tE18rshgbc3xtnee6jtTln6li6OvjcARaInltdmmGG0I5kCr/G7:rrsCbc3xtextl6pObcARaIXmmGhIG7
MD5:	DD31F56B9E4DFF40EB87447C3DC55B84
SHA1:	1908B34AF2D15440D33DFC81FCB93AA9B271DC58
SHA-256:	4F47EF8FF3DAD2A78360AB207CF35FF2905622511C0426109F6E225052CF5637
SHA-512:	057D2DCD66C48A2BB43D7B62BC38E4DACD3D7F3FDAA103AF178FDBC737BE91A81A369158BF02AB59C46F507F538536D01D5FC179D681375F9B77EE814E54447
Malicious:	false
IE Cache URL:	http://https://s.yimg.com/rz/p/yahoo_frontpage_en-US_s_f_w_bestfit_frontpage_2x.png
Preview:	.PNG........IHDR.......H............3PLTEGpL..a....tRNS......=..T.*v.h.#......IDATx^... ..9J...?m.....eL.ig..w.8.O.I.U.....(.S....R..I8N...\...=...yw`..I... (p...P...k.....<d...)oP{..;p..N...C...X).....,.v.N..>..9..0.,....>.....w1K........0......}.B.....&.J.......t..Q.....mn...,....=. ..<.)4.1..(.(H...O.....[.u^~c;.*L...8."....k.q...6d....X.....wFs.,y!..b....j. ........,.'F..C....CP2.'.$.M..A.].>.`m9.`...H<..Va.%SD6.*0......a...W..p".q.P..a..yik...f..e..fe.<>.s..S... *.%...N....<zaX...4..A..\lV.K......<'.G.D.duq..i........{.......M..f.3......?...4..d!..k.... .....C$...b.Y.RwC.Q.a....'..p.k..@x..{`o.r..7..K.-..D.k.J.....R"..0E).p../..0X...N....J.2.....n..j~v..HuA.sK._..feg....Ib...0....\...U....0k.J.....'....s.+5.k1...!.x^wl..&....P.6...\~....E...^..'wm... #U..p{.l.~.....i.......t..?..q..<%...d....WN\."[........5...Y....[.QH..$.k>....."........t#..W........&..</.y...+ .w.X...!...}..G.......q...E$..:..v..

C:\Users\user\AppData\Local\Temp\~DFAC985E6BE807E211.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	29745
Entropy (8bit):	0.2920107282763179
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laAC9laAC9lrz:kBqoxxJhHWSVSEabeQ2y
MD5:	CE909A43525B3843C907DCBE55E9D7DD
SHA1:	8B6E53CCBAAB132FF8100ECB696282F011402047
SHA-256:	540A8B39EAF1EF9CF341697FC4CDABBEBDED17B16321398C539639FD17EE1602
SHA-512:	027F1DF5288441E3BFF63ABABD90521E2A72DC20FFAC545E0F180483761229D13254375ADA525D3C5155C1BAC6602117B24617A160C4B9D21C30721B9DF17446
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFB79DB137339A7974.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13173
Entropy (8bit):	0.5740148319176536
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loNC9loNy9lWNzQFpH/:kBqoINtNrNEFN/
MD5:	9E1580C454D7F23C4D8C91DA7E2360C7
SHA1:	5E1C65FE51D535DAABECD4FA281D325011BAC6B2
SHA-256:	E86B8038AC399EEB67E169DA32DEDE961FA5F68ACC1386768521CEA85A81F42F
SHA-512:	BF6759EA7EE5453AD4AAD671A4A8A3DEF42497F4221A54E042215289D29CD5C707446E530212F3EFA188C8D4DEEAF0165927CA031EFB20DFCAA328D82EEAF94
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFDC14B9469AEC2819.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	84638
Entropy (8bit):	2.326283663322139
Encrypted:	false
SSDEEP:	768:Ec2QksS9M4NorfveFoNi3V9qjduH0u/9/rzDbG2:EJhsSe4NoDvYI4VQUUu/VHDb
MD5:	2AA63CAA9C629309BC05A68A8F98D1EC
SHA1:	52A9AF473D8B8FF578DAFBCFA5ADB74AEC61BE66
SHA-256:	CC5C6C84A7E3DFDD10CAA3958CBFB0958D9499DE556BE11F2D6D726284189023
SHA-512:	DF6F1042DA7CFF23EF50FCA9F98B12CA48BEB372C4FDA185507CA46BB591CF77D1CD8DF90DF55579B32B8F313B57B20CF501906A0A4271EBEC18874EE34E28CC
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

Static File Info

General

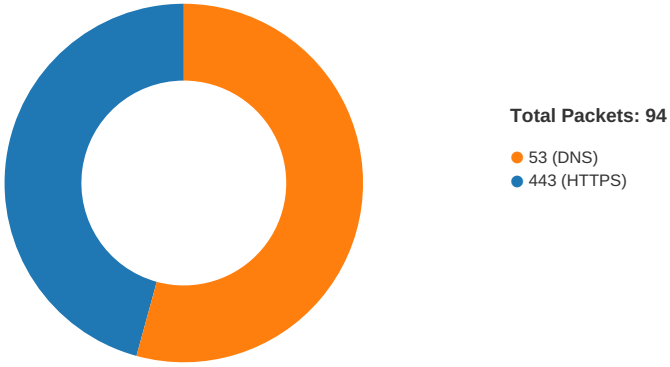
File type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Entropy (8bit):	3.3649442908320784
TrID:	
File name:	receipt319.html
File size:	151682
MD5:	2c2e3af2ecfca319e8848c1043b7bc35
SHA1:	3ebe21a94454b1d2704377ef0aab769be50c31d2
SHA256:	b80c548232c20ab1f8311f28661b5dba637df57e19cbb7f29a87c59fa294b635
SHA512:	959071f39f1a2b74235153c144f3efff73b8df64e2aacd42cafaae3d4d0652777f0e4ca23ea2e64de38c58db389fd0ddedfee571968aa13c376a133f7713fefc
SSDEEP:	768:AEZ+Y1tmbodvCh5gbd7yp8XgDbE101DAWWsI9Yq1ozV9OhnENUnXkXK4o1wU7w2f:B16bGsIYzDC0+
File Content Preview:	<script language="javascript"> ..document.write(unescape('%3c%21%44%4f%43%54%59%50%45%20%48%54%4d%4c%20%50%55%42%4c%49%43%20%22%2d%2f%2f%57%33%43%2f%2f%44%54%44%20%48%54%4d%4c%20%34%2e%30%31%20%54%72%61%6e%73%69%74%69%6f%6e%61%6c%2f%2f%45%4e%22%3e%0d%0a%3

File Icon

Icon Hash:	f8c89c9a9a998cb8

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 01:22:58.934811115 CEST	49711	443	192.168.2.5	212.82.100.140
May 13, 2021 01:22:58.934987068 CEST	49712	443	192.168.2.5	212.82.100.140
May 13, 2021 01:22:59.017759085 CEST	443	49712	212.82.100.140	192.168.2.5
May 13, 2021 01:22:59.017848969 CEST	49712	443	192.168.2.5	212.82.100.140
May 13, 2021 01:22:59.018892050 CEST	49712	443	192.168.2.5	212.82.100.140
May 13, 2021 01:22:59.018965006 CEST	443	49711	212.82.100.140	192.168.2.5
May 13, 2021 01:22:59.019109964 CEST	49711	443	192.168.2.5	212.82.100.140
May 13, 2021 01:22:59.020704985 CEST	49711	443	192.168.2.5	212.82.100.140
May 13, 2021 01:22:59.103281021 CEST	443	49712	212.82.100.140	192.168.2.5
May 13, 2021 01:22:59.104417086 CEST	443	49712	212.82.100.140	192.168.2.5
May 13, 2021 01:22:59.104451895 CEST	443	49712	212.82.100.140	192.168.2.5
May 13, 2021 01:22:59.104477882 CEST	443	49712	212.82.100.140	192.168.2.5
May 13, 2021 01:22:59.104495049 CEST	443	49712	212.82.100.140	192.168.2.5
May 13, 2021 01:22:59.104511976 CEST	443	49712	212.82.100.140	192.168.2.5
May 13, 2021 01:22:59.104547977 CEST	49712	443	192.168.2.5	212.82.100.140
May 13, 2021 01:22:59.104579926 CEST	49712	443	192.168.2.5	212.82.100.140
May 13, 2021 01:22:59.106349945 CEST	443	49711	212.82.100.140	192.168.2.5
May 13, 2021 01:22:59.113459110 CEST	443	49711	212.82.100.140	192.168.2.5
May 13, 2021 01:22:59.113507032 CEST	443	49711	212.82.100.140	192.168.2.5
May 13, 2021 01:22:59.113548994 CEST	443	49711	212.82.100.140	192.168.2.5
May 13, 2021 01:22:59.113575935 CEST	443	49711	212.82.100.140	192.168.2.5
May 13, 2021 01:22:59.113585949 CEST	49711	443	192.168.2.5	212.82.100.140
May 13, 2021 01:22:59.113611937 CEST	49711	443	192.168.2.5	212.82.100.140
May 13, 2021 01:22:59.113612890 CEST	443	49711	212.82.100.140	192.168.2.5
May 13, 2021 01:22:59.113655090 CEST	49711	443	192.168.2.5	212.82.100.140
May 13, 2021 01:22:59.122546911 CEST	49712	443	192.168.2.5	212.82.100.140
May 13, 2021 01:22:59.123262882 CEST	49712	443	192.168.2.5	212.82.100.140
May 13, 2021 01:22:59.131340981 CEST	49711	443	192.168.2.5	212.82.100.140
May 13, 2021 01:22:59.207324028 CEST	443	49712	212.82.100.140	192.168.2.5
May 13, 2021 01:22:59.207401991 CEST	49712	443	192.168.2.5	212.82.100.140
May 13, 2021 01:22:59.208602905 CEST	443	49712	212.82.100.140	192.168.2.5
May 13, 2021 01:22:59.208626986 CEST	443	49712	212.82.100.140	192.168.2.5
May 13, 2021 01:22:59.208642006 CEST	443	49712	212.82.100.140	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 01:22:59.208673954 CEST	49712	443	192.168.2.5	212.82.100.140
May 13, 2021 01:22:59.208719015 CEST	49712	443	192.168.2.5	212.82.100.140
May 13, 2021 01:22:59.214508057 CEST	49712	443	192.168.2.5	212.82.100.140
May 13, 2021 01:22:59.217511892 CEST	443	49711	212.82.100.140	192.168.2.5
May 13, 2021 01:22:59.217601061 CEST	49711	443	192.168.2.5	212.82.100.140
May 13, 2021 01:22:59.293962002 CEST	49714	443	192.168.2.5	212.82.100.140
May 13, 2021 01:22:59.294035912 CEST	49713	443	192.168.2.5	212.82.100.140
May 13, 2021 01:22:59.297285080 CEST	443	49712	212.82.100.140	192.168.2.5
May 13, 2021 01:22:59.378278017 CEST	443	49713	212.82.100.140	192.168.2.5
May 13, 2021 01:22:59.378360987 CEST	49713	443	192.168.2.5	212.82.100.140
May 13, 2021 01:22:59.380013943 CEST	49713	443	192.168.2.5	212.82.100.140
May 13, 2021 01:22:59.381418943 CEST	443	49714	212.82.100.140	192.168.2.5
May 13, 2021 01:22:59.381505966 CEST	49714	443	192.168.2.5	212.82.100.140
May 13, 2021 01:22:59.382114887 CEST	49714	443	192.168.2.5	212.82.100.140
May 13, 2021 01:22:59.463232994 CEST	443	49713	212.82.100.140	192.168.2.5
May 13, 2021 01:22:59.464412928 CEST	443	49713	212.82.100.140	192.168.2.5
May 13, 2021 01:22:59.464446068 CEST	443	49713	212.82.100.140	192.168.2.5
May 13, 2021 01:22:59.464471102 CEST	443	49713	212.82.100.140	192.168.2.5
May 13, 2021 01:22:59.464488983 CEST	443	49713	212.82.100.140	192.168.2.5
May 13, 2021 01:22:59.464505911 CEST	443	49713	212.82.100.140	192.168.2.5
May 13, 2021 01:22:59.464514971 CEST	49713	443	192.168.2.5	212.82.100.140
May 13, 2021 01:22:59.464549065 CEST	49713	443	192.168.2.5	212.82.100.140
May 13, 2021 01:22:59.464598894 CEST	49713	443	192.168.2.5	212.82.100.140
May 13, 2021 01:22:59.468646049 CEST	49713	443	192.168.2.5	212.82.100.140
May 13, 2021 01:22:59.469176054 CEST	443	49714	212.82.100.140	192.168.2.5
May 13, 2021 01:22:59.469604969 CEST	49713	443	192.168.2.5	212.82.100.140
May 13, 2021 01:22:59.470408916 CEST	443	49714	212.82.100.140	192.168.2.5
May 13, 2021 01:22:59.470443010 CEST	443	49714	212.82.100.140	192.168.2.5
May 13, 2021 01:22:59.470464945 CEST	443	49714	212.82.100.140	192.168.2.5
May 13, 2021 01:22:59.470479965 CEST	443	49714	212.82.100.140	192.168.2.5
May 13, 2021 01:22:59.470495939 CEST	443	49714	212.82.100.140	192.168.2.5
May 13, 2021 01:22:59.470573902 CEST	49714	443	192.168.2.5	212.82.100.140
May 13, 2021 01:22:59.470634937 CEST	49714	443	192.168.2.5	212.82.100.140
May 13, 2021 01:22:59.476068020 CEST	49714	443	192.168.2.5	212.82.100.140
May 13, 2021 01:22:59.551170111 CEST	443	49713	212.82.100.140	192.168.2.5
May 13, 2021 01:22:59.551292896 CEST	49713	443	192.168.2.5	212.82.100.140
May 13, 2021 01:22:59.561638117 CEST	443	49714	212.82.100.140	192.168.2.5
May 13, 2021 01:22:59.561719894 CEST	49714	443	192.168.2.5	212.82.100.140
May 13, 2021 01:22:59.591561079 CEST	443	49713	212.82.100.140	192.168.2.5
May 13, 2021 01:22:59.612087011 CEST	443	49713	212.82.100.140	192.168.2.5
May 13, 2021 01:22:59.612123013 CEST	443	49713	212.82.100.140	192.168.2.5
May 13, 2021 01:22:59.612143993 CEST	443	49713	212.82.100.140	192.168.2.5
May 13, 2021 01:22:59.612163067 CEST	443	49713	212.82.100.140	192.168.2.5
May 13, 2021 01:22:59.612184048 CEST	443	49713	212.82.100.140	192.168.2.5
May 13, 2021 01:22:59.612206936 CEST	443	49713	212.82.100.140	192.168.2.5
May 13, 2021 01:22:59.612227917 CEST	443	49713	212.82.100.140	192.168.2.5
May 13, 2021 01:22:59.612250090 CEST	443	49713	212.82.100.140	192.168.2.5
May 13, 2021 01:22:59.612251043 CEST	49713	443	192.168.2.5	212.82.100.140
May 13, 2021 01:22:59.612274885 CEST	443	49713	212.82.100.140	192.168.2.5
May 13, 2021 01:22:59.612292051 CEST	49713	443	192.168.2.5	212.82.100.140
May 13, 2021 01:22:59.612377882 CEST	49713	443	192.168.2.5	212.82.100.140
May 13, 2021 01:22:59.635469913 CEST	443	49713	212.82.100.140	192.168.2.5
May 13, 2021 01:22:59.635507107 CEST	443	49713	212.82.100.140	192.168.2.5
May 13, 2021 01:22:59.635571957 CEST	49713	443	192.168.2.5	212.82.100.140
May 13, 2021 01:22:59.635606050 CEST	49713	443	192.168.2.5	212.82.100.140
May 13, 2021 01:22:59.696345091 CEST	443	49713	212.82.100.140	192.168.2.5
May 13, 2021 01:22:59.696387053 CEST	443	49713	212.82.100.140	192.168.2.5
May 13, 2021 01:22:59.696408987 CEST	443	49713	212.82.100.140	192.168.2.5
May 13, 2021 01:22:59.696429014 CEST	443	49713	212.82.100.140	192.168.2.5
May 13, 2021 01:22:59.696450949 CEST	443	49713	212.82.100.140	192.168.2.5
May 13, 2021 01:22:59.696474075 CEST	443	49713	212.82.100.140	192.168.2.5
May 13, 2021 01:22:59.696476936 CEST	49713	443	192.168.2.5	212.82.100.140
May 13, 2021 01:22:59.696500063 CEST	49713	443	192.168.2.5	212.82.100.140
May 13, 2021 01:22:59.696501017 CEST	443	49713	212.82.100.140	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 01:22:59.696525097 CEST	443	49713	212.82.100.140	192.168.2.5
May 13, 2021 01:22:59.696549892 CEST	443	49713	212.82.100.140	192.168.2.5
May 13, 2021 01:22:59.696558952 CEST	49713	443	192.168.2.5	212.82.100.140

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 01:22:31.024516106 CEST	54302	53	192.168.2.5	8.8.8.8
May 13, 2021 01:22:31.088318110 CEST	53	54302	8.8.8.8	192.168.2.5
May 13, 2021 01:22:31.193875074 CEST	53784	53	192.168.2.5	8.8.8.8
May 13, 2021 01:22:31.243221045 CEST	65307	53	192.168.2.5	8.8.8.8
May 13, 2021 01:22:31.245842934 CEST	53	53784	8.8.8.8	192.168.2.5
May 13, 2021 01:22:31.295545101 CEST	53	65307	8.8.8.8	192.168.2.5
May 13, 2021 01:22:32.427314043 CEST	64344	53	192.168.2.5	8.8.8.8
May 13, 2021 01:22:32.487313032 CEST	53	64344	8.8.8.8	192.168.2.5
May 13, 2021 01:22:33.611594915 CEST	62060	53	192.168.2.5	8.8.8.8
May 13, 2021 01:22:33.667287111 CEST	53	62060	8.8.8.8	192.168.2.5
May 13, 2021 01:22:34.848226070 CEST	61805	53	192.168.2.5	8.8.8.8
May 13, 2021 01:22:34.910830975 CEST	53	61805	8.8.8.8	192.168.2.5
May 13, 2021 01:22:35.724313021 CEST	54795	53	192.168.2.5	8.8.8.8
May 13, 2021 01:22:35.786853075 CEST	53	54795	8.8.8.8	192.168.2.5
May 13, 2021 01:22:36.278959036 CEST	49557	53	192.168.2.5	8.8.8.8
May 13, 2021 01:22:36.331075907 CEST	53	49557	8.8.8.8	192.168.2.5
May 13, 2021 01:22:37.447849989 CEST	61733	53	192.168.2.5	8.8.8.8
May 13, 2021 01:22:37.508202076 CEST	53	61733	8.8.8.8	192.168.2.5
May 13, 2021 01:22:38.480092049 CEST	65447	53	192.168.2.5	8.8.8.8
May 13, 2021 01:22:38.534476995 CEST	53	65447	8.8.8.8	192.168.2.5
May 13, 2021 01:22:39.066457033 CEST	52441	53	192.168.2.5	8.8.8.8
May 13, 2021 01:22:39.128705025 CEST	53	52441	8.8.8.8	192.168.2.5
May 13, 2021 01:22:39.514343977 CEST	62176	53	192.168.2.5	8.8.8.8
May 13, 2021 01:22:39.568207979 CEST	53	62176	8.8.8.8	192.168.2.5
May 13, 2021 01:22:40.812211037 CEST	59596	53	192.168.2.5	8.8.8.8
May 13, 2021 01:22:40.884438992 CEST	53	59596	8.8.8.8	192.168.2.5
May 13, 2021 01:22:49.634377956 CEST	65296	53	192.168.2.5	8.8.8.8
May 13, 2021 01:22:49.708141088 CEST	53	65296	8.8.8.8	192.168.2.5
May 13, 2021 01:22:50.184803009 CEST	63183	53	192.168.2.5	8.8.8.8
May 13, 2021 01:22:50.240185022 CEST	53	63183	8.8.8.8	192.168.2.5
May 13, 2021 01:22:51.075179100 CEST	60151	53	192.168.2.5	8.8.8.8
May 13, 2021 01:22:51.133483887 CEST	53	60151	8.8.8.8	192.168.2.5
May 13, 2021 01:22:52.247179985 CEST	56969	53	192.168.2.5	8.8.8.8
May 13, 2021 01:22:52.301040888 CEST	53	56969	8.8.8.8	192.168.2.5
May 13, 2021 01:22:58.635860920 CEST	55161	53	192.168.2.5	8.8.8.8
May 13, 2021 01:22:58.716551065 CEST	53	55161	8.8.8.8	192.168.2.5
May 13, 2021 01:22:58.866580963 CEST	54757	53	192.168.2.5	8.8.8.8
May 13, 2021 01:22:58.932636976 CEST	53	54757	8.8.8.8	192.168.2.5
May 13, 2021 01:22:59.225752115 CEST	49992	53	192.168.2.5	8.8.8.8
May 13, 2021 01:22:59.291196108 CEST	53	49992	8.8.8.8	192.168.2.5
May 13, 2021 01:22:59.641168118 CEST	60075	53	192.168.2.5	8.8.8.8
May 13, 2021 01:22:59.699301004 CEST	53	60075	8.8.8.8	192.168.2.5
May 13, 2021 01:23:01.059499979 CEST	55016	53	192.168.2.5	8.8.8.8
May 13, 2021 01:23:01.067807913 CEST	64345	53	192.168.2.5	8.8.8.8
May 13, 2021 01:23:01.123581886 CEST	53	55016	8.8.8.8	192.168.2.5
May 13, 2021 01:23:01.134547949 CEST	53	64345	8.8.8.8	192.168.2.5
May 13, 2021 01:23:09.000077963 CEST	57128	53	192.168.2.5	8.8.8.8
May 13, 2021 01:23:09.055052042 CEST	53	57128	8.8.8.8	192.168.2.5
May 13, 2021 01:23:09.300730944 CEST	54791	53	192.168.2.5	8.8.8.8
May 13, 2021 01:23:09.363972902 CEST	53	54791	8.8.8.8	192.168.2.5
May 13, 2021 01:23:09.928386927 CEST	50463	53	192.168.2.5	8.8.8.8
May 13, 2021 01:23:09.985930920 CEST	53	50463	8.8.8.8	192.168.2.5
May 13, 2021 01:23:09.993355036 CEST	57128	53	192.168.2.5	8.8.8.8
May 13, 2021 01:23:10.049602032 CEST	53	57128	8.8.8.8	192.168.2.5
May 13, 2021 01:23:10.930811882 CEST	50463	53	192.168.2.5	8.8.8.8
May 13, 2021 01:23:10.994019032 CEST	53	50463	8.8.8.8	192.168.2.5
May 13, 2021 01:23:11.010433912 CEST	57128	53	192.168.2.5	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 01:23:11.070888042 CEST	53	57128	8.8.8.8	192.168.2.5
May 13, 2021 01:23:11.984844923 CEST	50463	53	192.168.2.5	8.8.8.8
May 13, 2021 01:23:12.040060997 CEST	53	50463	8.8.8.8	192.168.2.5
May 13, 2021 01:23:13.096175909 CEST	57128	53	192.168.2.5	8.8.8.8
May 13, 2021 01:23:13.148653984 CEST	53	57128	8.8.8.8	192.168.2.5
May 13, 2021 01:23:13.993410110 CEST	50463	53	192.168.2.5	8.8.8.8
May 13, 2021 01:23:14.048343897 CEST	53	50463	8.8.8.8	192.168.2.5
May 13, 2021 01:23:17.087569952 CEST	57128	53	192.168.2.5	8.8.8.8
May 13, 2021 01:23:17.139874935 CEST	53	57128	8.8.8.8	192.168.2.5
May 13, 2021 01:23:17.359474897 CEST	50394	53	192.168.2.5	8.8.8.8
May 13, 2021 01:23:17.419900894 CEST	53	50394	8.8.8.8	192.168.2.5
May 13, 2021 01:23:18.009169102 CEST	50463	53	192.168.2.5	8.8.8.8
May 13, 2021 01:23:18.064184904 CEST	53	50463	8.8.8.8	192.168.2.5
May 13, 2021 01:23:26.932185888 CEST	58530	53	192.168.2.5	8.8.8.8
May 13, 2021 01:23:27.014359951 CEST	53	58530	8.8.8.8	192.168.2.5
May 13, 2021 01:23:36.970531940 CEST	53813	53	192.168.2.5	8.8.8.8
May 13, 2021 01:23:37.038655043 CEST	53	53813	8.8.8.8	192.168.2.5
May 13, 2021 01:24:05.195225000 CEST	63732	53	192.168.2.5	8.8.8.8
May 13, 2021 01:24:05.259252071 CEST	53	63732	8.8.8.8	192.168.2.5
May 13, 2021 01:24:08.549659967 CEST	57344	53	192.168.2.5	8.8.8.8
May 13, 2021 01:24:08.611876965 CEST	53	57344	8.8.8.8	192.168.2.5
May 13, 2021 01:24:12.645581007 CEST	54450	53	192.168.2.5	8.8.8.8
May 13, 2021 01:24:12.706248999 CEST	53	54450	8.8.8.8	192.168.2.5
May 13, 2021 01:24:29.399266958 CEST	59261	53	192.168.2.5	8.8.8.8
May 13, 2021 01:24:29.462377071 CEST	53	59261	8.8.8.8	192.168.2.5
May 13, 2021 01:24:45.802722931 CEST	57151	53	192.168.2.5	8.8.8.8
May 13, 2021 01:24:45.863392115 CEST	53	57151	8.8.8.8	192.168.2.5
May 13, 2021 01:24:47.995682001 CEST	59413	53	192.168.2.5	8.8.8.8
May 13, 2021 01:24:48.056054115 CEST	53	59413	8.8.8.8	192.168.2.5
May 13, 2021 01:25:11.003973007 CEST	60516	53	192.168.2.5	8.8.8.8
May 13, 2021 01:25:11.068418026 CEST	53	60516	8.8.8.8	192.168.2.5
May 13, 2021 01:25:11.597130060 CEST	51649	53	192.168.2.5	8.8.8.8
May 13, 2021 01:25:11.663592100 CEST	53	51649	8.8.8.8	192.168.2.5
May 13, 2021 01:25:12.503696918 CEST	65086	53	192.168.2.5	8.8.8.8
May 13, 2021 01:25:12.564174891 CEST	53	65086	8.8.8.8	192.168.2.5
May 13, 2021 01:25:12.942796946 CEST	56432	53	192.168.2.5	8.8.8.8
May 13, 2021 01:25:13.006242037 CEST	53	56432	8.8.8.8	192.168.2.5
May 13, 2021 01:25:13.468628883 CEST	52929	53	192.168.2.5	8.8.8.8
May 13, 2021 01:25:13.529165030 CEST	53	52929	8.8.8.8	192.168.2.5
May 13, 2021 01:25:14.015954018 CEST	64317	53	192.168.2.5	8.8.8.8
May 13, 2021 01:25:14.073452950 CEST	53	64317	8.8.8.8	192.168.2.5
May 13, 2021 01:25:14.466211081 CEST	61004	53	192.168.2.5	8.8.8.8
May 13, 2021 01:25:14.528661966 CEST	53	61004	8.8.8.8	192.168.2.5
May 13, 2021 01:25:15.157279968 CEST	56895	53	192.168.2.5	8.8.8.8
May 13, 2021 01:25:15.220101118 CEST	53	56895	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 13, 2021 01:22:58.866580963 CEST	192.168.2.5	8.8.8.8	0xeb8a	Standard query (0)	eu.edit.yahoo.com	A (IP address)	IN (0x0001)
May 13, 2021 01:22:59.225752115 CEST	192.168.2.5	8.8.8.8	0xad93	Standard query (0)	login.yahoo.com	A (IP address)	IN (0x0001)
May 13, 2021 01:22:59.641168118 CEST	192.168.2.5	8.8.8.8	0xf4be	Standard query (0)	s.yimg.com	A (IP address)	IN (0x0001)
May 13, 2021 01:23:01.059499979 CEST	192.168.2.5	8.8.8.8	0xa032	Standard query (0)	udc.yahoo.com	A (IP address)	IN (0x0001)
May 13, 2021 01:23:01.067807913 CEST	192.168.2.5	8.8.8.8	0x57ff	Standard query (0)	geo.yahoo.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 13, 2021 01:22:58.932636976 CEST	8.8.8.8	192.168.2.5	0xeb8a	No error (0)	eu.edit.yahoo.com	edit.yahoo.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 13, 2021 01:22:58.932636976 CEST	8.8.8.8	192.168.2.5	0xeb8a	No error (0)	edit.yahoo.com	login.yahoo.com		CNAME (Canonical name)	IN (0x0001)
May 13, 2021 01:22:58.932636976 CEST	8.8.8.8	192.168.2.5	0xeb8a	No error (0)	login.yahoo.com	ds-ats.member.g02.yahoodns.net		CNAME (Canonical name)	IN (0x0001)
May 13, 2021 01:22:58.932636976 CEST	8.8.8.8	192.168.2.5	0xeb8a	No error (0)	ds-ats.member.g02.yahoodns.net		212.82.100.140	A (IP address)	IN (0x0001)
May 13, 2021 01:22:59.291196108 CEST	8.8.8.8	192.168.2.5	0xad93	No error (0)	login.yahoo.com	ds-ats.member.g02.yahoodns.net		CNAME (Canonical name)	IN (0x0001)
May 13, 2021 01:22:59.291196108 CEST	8.8.8.8	192.168.2.5	0xad93	No error (0)	ds-ats.member.g02.yahoodns.net		212.82.100.140	A (IP address)	IN (0x0001)
May 13, 2021 01:22:59.699301004 CEST	8.8.8.8	192.168.2.5	0xf4be	No error (0)	s.yimg.com	edge.gycpi.b.yahoodns.net		CNAME (Canonical name)	IN (0x0001)
May 13, 2021 01:22:59.699301004 CEST	8.8.8.8	192.168.2.5	0xf4be	No error (0)	edge.gycpi.b.yahoodns.net		87.248.118.23	A (IP address)	IN (0x0001)
May 13, 2021 01:22:59.699301004 CEST	8.8.8.8	192.168.2.5	0xf4be	No error (0)	edge.gycpi.b.yahoodns.net		87.248.118.22	A (IP address)	IN (0x0001)
May 13, 2021 01:23:01.123581886 CEST	8.8.8.8	192.168.2.5	0xa032	No error (0)	udc.yahoo.com	udc-ats.media.g03.yahoodns.net		CNAME (Canonical name)	IN (0x0001)
May 13, 2021 01:23:01.123581886 CEST	8.8.8.8	192.168.2.5	0xa032	No error (0)	udc-ats.media.g03.yahoodns.net		188.125.72.139	A (IP address)	IN (0x0001)
May 13, 2021 01:23:01.134547949 CEST	8.8.8.8	192.168.2.5	0x57ff	No error (0)	geo.yahoo.com	geo-atsv2.media.g03.yahoodns.net		CNAME (Canonical name)	IN (0x0001)
May 13, 2021 01:23:01.134547949 CEST	8.8.8.8	192.168.2.5	0x57ff	No error (0)	geo-atsv2.media.g03.yahoodns.net		188.125.72.139	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
May 13, 2021 01:22:59.104477882 CEST	212.82.100.140	443	192.168.2.5	49712	CN=*.login.yahoo.com, O=Oath Inc, L=Sunnyvale, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Jan 25 01:00:00 CET 2021	Wed Jul 21 01:59:59 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
May 13, 2021 01:22:59.113548994 CEST	212.82.100.140	443	192.168.2.5	49711	CN=*.login.yahoo.com, O=Oath Inc, L=Sunnyvale, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Jan 25 01:00:00 CET 2021	Wed Jul 21 01:59:59 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 13, 2021 01:22:59.464471102 CEST	212.82.100.140	443	192.168.2.5	49713	CN=*.login.yahoo.com, O=Oath Inc, L=Sunnyvale, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Jan 25 01:00:00 CET 2021 Tue Oct 22 14:00:00 CEST 2013	Wed Jul 21 01:59:59 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
May 13, 2021 01:22:59.470464945 CEST	212.82.100.140	443	192.168.2.5	49714	CN=*.login.yahoo.com, O=Oath Inc, L=Sunnyvale, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Jan 25 01:00:00 CET 2021 Tue Oct 22 14:00:00 CEST 2013	Wed Jul 21 01:59:59 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
May 13, 2021 01:22:59.839662075 CEST	87.248.118.23	443	192.168.2.5	49717	CN=*.yahoo.com, O=Oath Inc, L=Sunnyvale, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon May 03 02:00:00 CEST 2021 Tue Oct 22 14:00:00 CEST 2013	Thu Jun 24 01:59:59 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
May 13, 2021 01:22:59.846745014 CEST	87.248.118.23	443	192.168.2.5	49716	CN=*.yahoo.com, O=Oath Inc, L=Sunnyvale, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon May 03 02:00:00 CEST 2021 Tue Oct 22 14:00:00 CEST 2013	Thu Jun 24 01:59:59 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
May 13, 2021 01:22:59.848289967 CEST	87.248.118.23	443	192.168.2.5	49715	CN=*.yahoo.com, O=Oath Inc, L=Sunnyvale, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon May 03 02:00:00 CEST 2021 Tue Oct 22 14:00:00 CEST 2013	Thu Jun 24 01:59:59 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 13, 2021 01:22:59.863804102 CEST	87.248.118.23	443	192.168.2.5	49718	CN=*.yahoo.com, O=Oath Inc, L=Sunnyvale, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon May 03 02:00:00 CEST 2021 Tue Oct 22 14:00:00 CEST 2013	Thu Jun 24 01:59:59 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
May 13, 2021 01:22:59.866856098 CEST	87.248.118.23	443	192.168.2.5	49719	CN=*.yahoo.com, O=Oath Inc, L=Sunnyvale, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon May 03 02:00:00 CEST 2021 Tue Oct 22 14:00:00 CEST 2013	Thu Jun 24 01:59:59 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
May 13, 2021 01:23:01.380901098 CEST	188.125.72.139	443	192.168.2.5	49720	CN=analytics.query.yahoo.com, O=Oath Inc, L=Sunnyvale, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Mar 08 01:00:00 CET 2021 Tue Oct 22 14:00:00 CEST 2013	Thu Sep 02 01:59:59 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
May 13, 2021 01:23:01.633302927 CEST	188.125.72.139	443	192.168.2.5	49722	CN=analytics.query.yahoo.com, O=Oath Inc, L=Sunnyvale, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Mar 08 01:00:00 CET 2021 Tue Oct 22 14:00:00 CEST 2013	Thu Sep 02 01:59:59 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
May 13, 2021 01:23:01.636317968 CEST	188.125.72.139	443	192.168.2.5	49721	CN=analytics.query.yahoo.com, O=Oath Inc, L=Sunnyvale, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Mar 08 01:00:00 CET 2021 Tue Oct 22 14:00:00 CEST 2013	Thu Sep 02 01:59:59 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 4192 Parent PID: 792

General

Start time:	01:22:37
Start date:	13/05/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff7f7ae0000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: iexplore.exe PID: 4636 Parent PID: 4192

General

Start time:	01:22:38
Start date:	13/05/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4192 CREDAT:17410 /prefetch:2
Imagebase:	0xc40000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly