ID: 323932
Sample Name: INVOICE.html
Cookbook:
defaultwindowshtmlcookbook.jbs
Time: 21:43:42
Date: 27/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

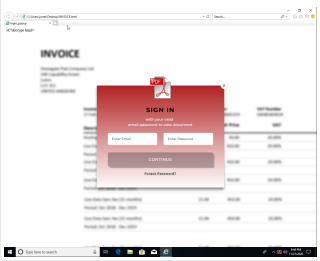
Analysis Report INVOICE.html

Overview

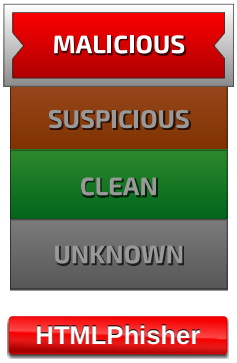
General Information

Sample Name:	INVOICE.html
Analysis ID:	323932
MD5:	c23676897af888d.
SHA1:	425fd76dd126543.
SHA256:	662992de22ac11..

Most interesting Screenshot:



Detection

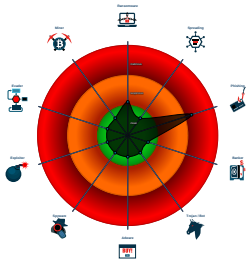


Score:	48
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected HtmlPhish_10
- HTML body contains low number of …
- JA3 SSL client fingerprint seen in co…
- No HTML title found
- None HTTPS page querying sensitiv…
- Suspicious form URL found

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 6944 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6992 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6944 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

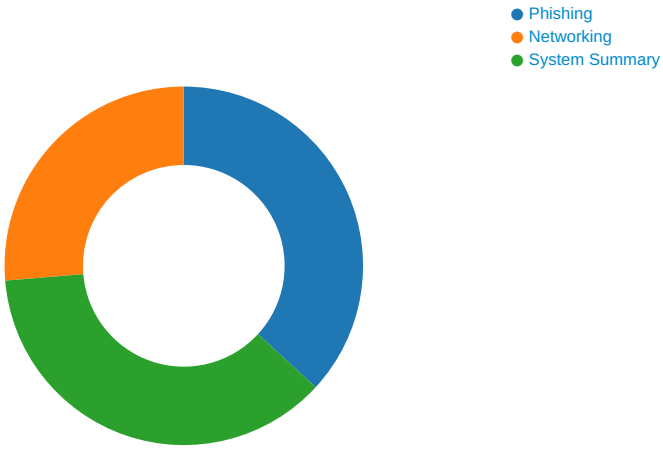
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

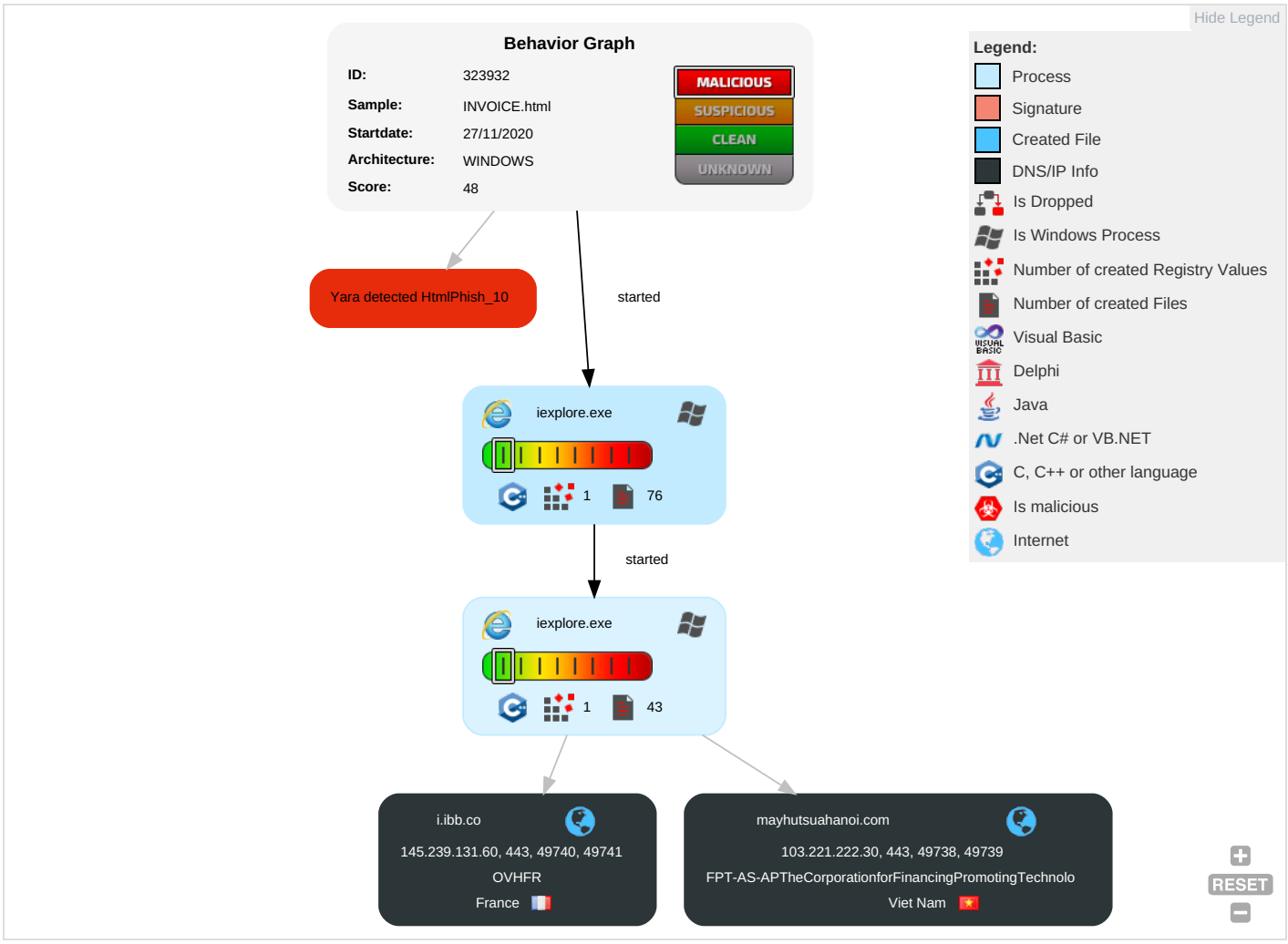
Phishing:

Yara detected HtmlPhish_10

Mitre Att&ck Matrix

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

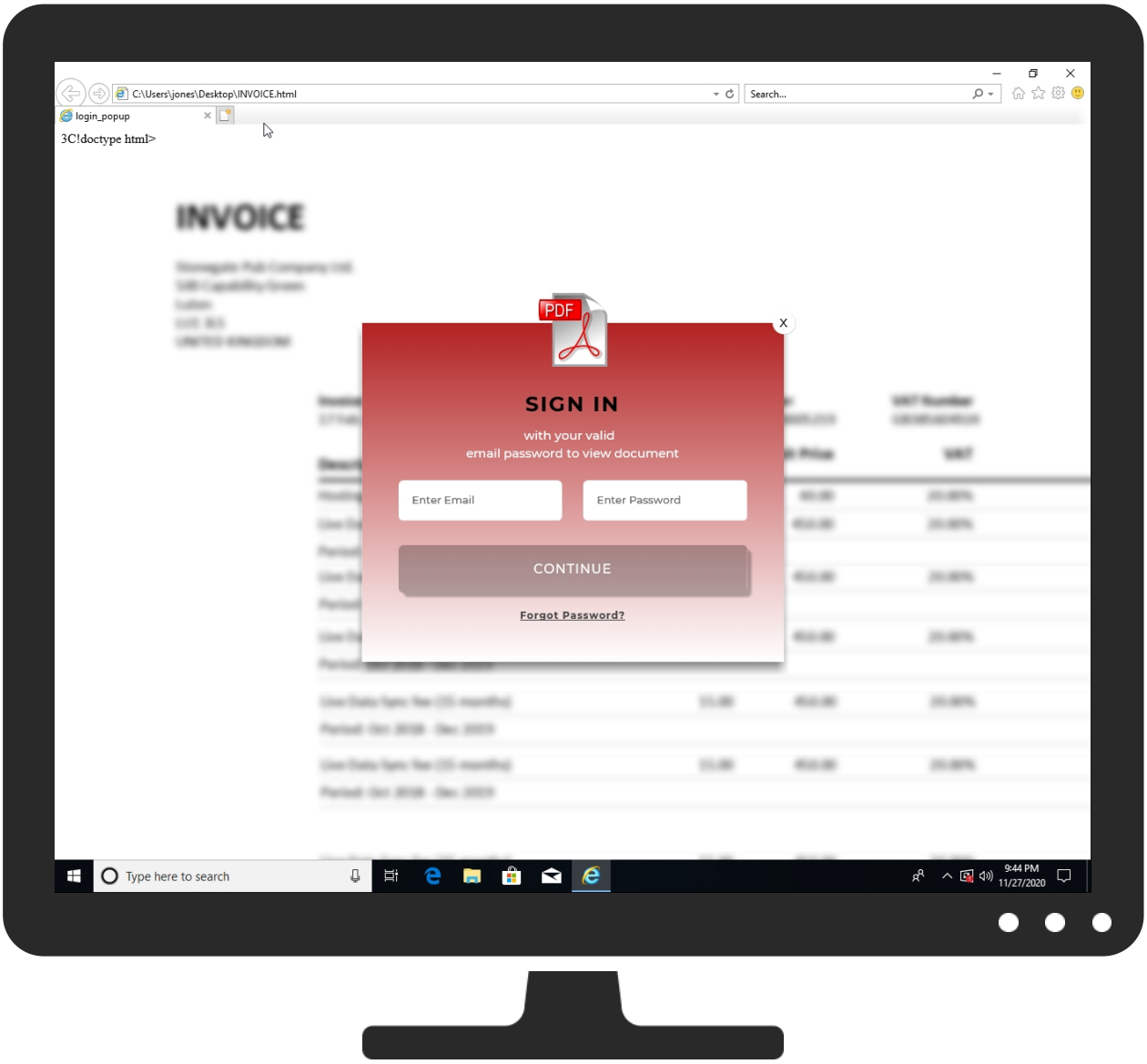
Behavior Graph



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

Source	Detection	Scanner	Label	Link
INVOICE.html	2%	Virustotal		Browse
INVOICE.html	0%	ReversingLabs		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
mayhutsuahanoi.com	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mayhutsuahanoi.com	103.221.222.30	true	false	• 1%, Virustotal, Browse	unknown
i.ibb.co	145.239.131.60	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
file:///C:/Users/user/Desktop/INVOICE.html	true		low

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.wikipedia.com/	msapplication.xml6.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.amazon.com/	msapplication.xml.1.dr	false		high
http://www.nytimes.com/	msapplication.xml3.1.dr	false		high
http://www.live.com/	msapplication.xml2.1.dr	false		high
http://www.reddit.com/	msapplication.xml4.1.dr	false		high
http://www.twitter.com/	msapplication.xml5.1.dr	false		high
http://www.youtube.com/	msapplication.xml7.1.dr	false		high

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
145.239.131.60	unknown	France		16276	OVHFR	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
103.221.222.30	unknown	Viet Nam		18403	FPT-AS-APTheCorporationforFinancingPromotingTechnolo	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	323932
Start date:	27.11.2020
Start time:	21:43:42
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 4s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	INVOICE.html
Cookbook file name:	defaultwindowshtmlcookbook.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:	15
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:	mal48.phis.winHTML@3/26@2/2
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .html

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 104.42.151.234, 13.64.90.137, 104.83.120.32, 216.58.215.234, 172.217.168.3, 51.104.139.180, 152.199.19.161, 52.155.217.156, 20.54.26.129, 8.248.147.254, 8.241.9.126, 67.26.81.254, 8.253.204.249, 8.241.9.254, 92.122.213.194, 92.122.213.247 • Excluded domains from analysis (whitelisted): gstaticadssl.l.google.com, arc.msn.com.nsatc.net, a1449.dscg2.akamai.net, arc.msn.com, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, go.microsoft.com, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, fonts.googleapis.com, fonts.gstatic.com, ie9comview.vo.msecnd.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, skypedataprdcolwus16.cloudapp.net, cs9.wpc.v0cdn.net

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
103.221.222.30	http://https://m.box.com/file/702493360747/download?shared_link=https%3A%2F%2Flinbeck.app.box.com%2Fs%2F8yjolj91ewomp9vmklwuluiunx8d5sox	Get hash	malicious	Browse	• vayvontinchap5s.com/createsends/simplebusinesscreators.php

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
i.ibb.co	Direct Deposit.xlsx	Get hash	malicious	Browse	• 145.239.131.51
	Direct Deposit.xlsx	Get hash	malicious	Browse	• 145.239.131.55
	0151-83872-976-67-83872.htm	Get hash	malicious	Browse	• 51.210.112.129
	#Ud83c#Udfb6 18 November, 2020 Pam.Guetschow@citrix.com.wavv.htm	Get hash	malicious	Browse	• 51.210.112.130
	http://https://honcdestruction-shared.com/ViewHonc-SharedInfo	Get hash	malicious	Browse	• 51.210.112.129
	WeTransfer File for info@nanniottavio.it .html	Get hash	malicious	Browse	• 51.210.112.129
	viaseating-666114_xls.HtMl	Get hash	malicious	Browse	• 51.210.112.129
	tetratech-907745_xls.HtMl	Get hash	malicious	Browse	• 51.210.112.130
	http.docx	Get hash	malicious	Browse	• 51.210.112.129

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http.docx	Get hash	malicious	Browse	• 51.210.112.130
	http://https://firebasestorage.googleapis.com/v0/b/r3grwv-r3wv-r3gwv-frgvh5g5-rg.appspot.com/o/5g5r-vr-g3dr-v-3g-rv-3gr%2F5-rf-g3fr-r-g3-wrfg-g.html?alt=media&token=edc9f30a-febb-4fe3-a5bd-46c72408f357#DD_FinanceAP_ASIA@juliusbaer.com	Get hash	malicious	Browse	• 51.210.112.129
	rooney-eng-598583_xls.HtMl	Get hash	malicious	Browse	• 51.210.112.130
	lorino-106812_xls.HtMl	Get hash	malicious	Browse	• 51.210.112.129
	azklima-584035_xls.HtMl	Get hash	malicious	Browse	• 51.210.112.130
	ciechgroup-551288_xls.HtMl	Get hash	malicious	Browse	• 51.210.112.130
	#Ud83d#Udce0683442762782356353_TI.HTM	Get hash	malicious	Browse	• 51.210.112.130
	#Ud83c#Udfb6 03 November, 2020 prodriguez@fnbsm.com.wavv.htm	Get hash	malicious	Browse	• 51.210.112.130
	TtQxnoZhYv.html	Get hash	malicious	Browse	• 51.210.112.130
	qnb-062591_xls.HtMl	Get hash	malicious	Browse	• 51.210.112.130
	27 October, 2020 mschram@wintrust.com.wavv.htm	Get hash	malicious	Browse	• 51.210.112.129

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
FPT-AS-APTheCorporationforFinancingPromotingTechnolo	idWMSrWvoE.exe	Get hash	malicious	Browse	• 118.69.11.81
	cK2ClsvtJE.exe	Get hash	malicious	Browse	• 118.69.11.81
	AXZFXiJCj3.exe	Get hash	malicious	Browse	• 118.69.11.81
	lHuFdWpoMA.exe	Get hash	malicious	Browse	• 118.69.11.81
	0j4pavDJBN.exe	Get hash	malicious	Browse	• 118.69.11.81
	0V9GzUGmwu.exe	Get hash	malicious	Browse	• 118.69.11.81
	1Tkig2z6A1.exe	Get hash	malicious	Browse	• 118.69.11.81
	CDItmDQ5cQ.exe	Get hash	malicious	Browse	• 118.69.11.81
	44KBPHzTuK.exe	Get hash	malicious	Browse	• 118.69.11.81
	W0MyzJBgSK.exe	Get hash	malicious	Browse	• 118.69.11.81
	ye4wKPE8eQ.exe	Get hash	malicious	Browse	• 118.70.15.19
	zRMcU3e368.exe	Get hash	malicious	Browse	• 118.69.11.81
	OAjqRkN1HR.exe	Get hash	malicious	Browse	• 118.69.11.81
	Q288Rfg0M2.exe	Get hash	malicious	Browse	• 118.69.11.81
	veE2lt9ehs.exe	Get hash	malicious	Browse	• 118.69.11.81
	Q1821GOhHS.exe	Get hash	malicious	Browse	• 118.69.11.81
	83mOllQfIS.exe	Get hash	malicious	Browse	• 118.69.11.81
	Cq1u3n1XsJ.exe	Get hash	malicious	Browse	• 118.69.11.81
	1pyhCQUm2u.exe	Get hash	malicious	Browse	• 118.69.11.81
	V0pplnY8ZB.exe	Get hash	malicious	Browse	• 118.69.11.81
OVHFR	Proforma Invoice with Bank Details_pdf.exe	Get hash	malicious	Browse	• 66.70.204.222
	Direct Deposit.xlsx	Get hash	malicious	Browse	• 145.239.131.51
	Direct Deposit.xlsx	Get hash	malicious	Browse	• 145.239.131.55
	http://https://mincast.us-south.cf.appdomain.cloud/redirect/?email=prampon@soteb.fr	Get hash	malicious	Browse	• 149.56.20.211
	Image001.exe	Get hash	malicious	Browse	• 66.70.204.222
	4nfg3g3nwg.exe	Get hash	malicious	Browse	• 66.70.204.222
	due-invoice.xlsm	Get hash	malicious	Browse	• 87.98.154.146
	SHIPPING DOCUMENT & PACKING LIST.exe	Get hash	malicious	Browse	• 51.75.130.83
	anthon.exe	Get hash	malicious	Browse	• 51.38.230.18
	ORDER-207044.xLs.exe	Get hash	malicious	Browse	• 54.37.36.116
	Bulk Order - 1017C.exe	Get hash	malicious	Browse	• 51.75.130.83
	SWIFT Transfer (103) W071323.exe	Get hash	malicious	Browse	• 51.75.130.83
	http://ancien-site-joomla.fr/build2.exe	Get hash	malicious	Browse	• 87.98.154.146
	tarifvertrag_igbce_weihnachtsgeld_k#U00fcndigung.js	Get hash	malicious	Browse	• 51.77.152.34
	tarifvertrag_igbce_weihnachtsgeld_k#U00fcndigung.js	Get hash	malicious	Browse	• 51.77.152.34
	Invoice_Payment Form_948792.xlsm	Get hash	malicious	Browse	• 213.186.33.40
	0151-83872-976-67-83872.htm	Get hash	malicious	Browse	• 51.210.112.129
	SR7UzD8vSg.exe	Get hash	malicious	Browse	• 92.222.121.127
	PAYMENT ADVISE.exe	Get hash	malicious	Browse	• 51.75.130.83
	http://https://eti-salat.com/x/	Get hash	malicious	Browse	• 145.239.6.126

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
9e10692f1b7f78228b2d4e424db3a98c	Final_report_2020.html	Get hash	malicious	Browse	• 145.239.131.60 • 103.221.222.30
	norit.dll	Get hash	malicious	Browse	• 145.239.131.60 • 103.221.222.30
	http://https://tinyurl.com/y9xs2oe6	Get hash	malicious	Browse	• 145.239.131.60 • 103.221.222.30
	http://https://ch1.amorozon.fr/.zz?&78387439&user=jon.parr@syngenta.com	Get hash	malicious	Browse	• 145.239.131.60 • 103.221.222.30
	Direct Deposit.xlsx	Get hash	malicious	Browse	• 145.239.131.60 • 103.221.222.30
	Direct Deposit.xlsx	Get hash	malicious	Browse	• 145.239.131.60 • 103.221.222.30
	http://https://ib.adnxs.com/getuid?https://a.adrsp.net/dsp/ci/2/E8quIp-RUbrsO6XnZMkW-Z82IQ_D_mG3bKHPbyWqDJNAFkp2JZBiBD4qwJcECqeCBYZccMP3y2IGKpMkBSJ3emkLIw/%24UID	Get hash	malicious	Browse	• 145.239.131.60 • 103.221.222.30
	http://fonts.mafia-server.net	Get hash	malicious	Browse	• 145.239.131.60 • 103.221.222.30
	Direct Deposit.xlsx	Get hash	malicious	Browse	• 145.239.131.60 • 103.221.222.30
	INV-FATURA010009.xlsx	Get hash	malicious	Browse	• 145.239.131.60 • 103.221.222.30
	INV-FATURA010009.xlsx	Get hash	malicious	Browse	• 145.239.131.60 • 103.221.222.30
	http://https://alldomainverifications.web.app#paulo.horta@gnbga.pt	Get hash	malicious	Browse	• 145.239.131.60 • 103.221.222.30
	http://https://broughtguarantees.com/1/oZrheD/cHBlcmluaUBhZmZpbmlvbmdyb3VwLmNvbQ%3D%3D&d=DwMDaQ	Get hash	malicious	Browse	• 145.239.131.60 • 103.221.222.30
	http://https://offiubtj7banjz48zrg8d4nz2ns9.web.app/?c=brynjar.t.gudmundsson@landsbanki.is	Get hash	malicious	Browse	• 145.239.131.60 • 103.221.222.30
	http://https://erabansoupala.blogspot.com//?m=0	Get hash	malicious	Browse	• 145.239.131.60 • 103.221.222.30
	http://https://mincast.us-south.cf.appdomain.cloud/redirect/?email=prampon@soteb.fr	Get hash	malicious	Browse	• 145.239.131.60 • 103.221.222.30
	http://https://dagevleri.com/inv	Get hash	malicious	Browse	• 145.239.131.60 • 103.221.222.30
	http://https://dealmaker.pl/au_au.html	Get hash	malicious	Browse	• 145.239.131.60 • 103.221.222.30
	http://https://wilkinsonbutler.tallverse.ga/YW1iZXJAd2lsa2luc29uYnV0bGVyLmNvbQ==	Get hash	malicious	Browse	• 145.239.131.60 • 103.221.222.30
	http://https://wilkinsonbutler.tallverse.ga/YW1iZXJAd2lsa2luc29uYnV0bGVyLmNvbQ==	Get hash	malicious	Browse	• 145.239.131.60 • 103.221.222.30

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{56772179-30F1-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8465902202705173
Encrypted:	false
SSDEEP:	192:rwZ3Zt52t5i9Wt5Hitt5Hx0ift5Hx4UTtzMt5H894yFBt5H834rfDt5H83l4Bsfx:rgJGyUqvqCj6x
MD5:	27268A176B5DA2ABD4B41E7229CDAFA2
SHA1:	E73E8B7640326F36ACFCEC52194FCD6130DA545D
SHA-256:	0577965121FE6EF8B7A91510FF792806A398C5A12CA684FDEDA877F0FAF74CF8
SHA-512:	BA1C710D48DC0C74E76F3732B33B2C43F7CD814D1390CEEBEA5E7DBA08BBD6AF6E02D2D54284270F6F42DFDF113AC1BF5071F0E3ECEBE4C1CA170301D852DFED
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{56772179-30F1-11EB-90EB-ECF4BBEA1588}.dat	
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{5677217B-30F1-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28178
Entropy (8bit):	1.9070117265998872
Encrypted:	false
SSDEEP:	96:r2ZVQt67BSwFjR2AkWYMjYYOrYIWoEoIWo9FgIr:r2ZVQt67kwFjR2AkWYMjYYOrM2Ir
MD5:	E63B69CC45873BA2D74C0C6BE66E9DB8
SHA1:	FCB156B7F79632E0FAD2DC0A6A4C96894D35E948
SHA-256:	83B35156AEB9BBC4035949E1090C832A75A43D3EDEA20560DD949FCCCE7A9A23
SHA-512:	9AB6E71B5AA3DE85F316B5C25A2698CC0BE1715665FBE7BB82B9A546032DC1FA5B5689A9147D396110C452C4DA9D871048AE14A59CCE59583F4BF9AB6B166D 0
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\{5677217C-30F1-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5631767085175443
Encrypted:	false
SSDEEP:	48:IwHGcprCGwpa/G4pQvGrapbSArGQpKOG7HpRqsTGIpG:rtZqQR6zBSAFAJTq4A
MD5:	A9294FADF5666686E2C0A1D6FB65896E
SHA1:	B1E7F425F09E177911FED94477E4EC8DC2051AEF
SHA-256:	E5F08E055CE8CD2361013D8C1A908FCB574C41674AB9923CFC0CC189D03E2972
SHA-512:	0A2BD6587D406BFCD78FCF0B817DF8031374D37F3F3896F474FF165C811D7057A20E576D8E6D15F3AB895DB89DA919D0E9E61D1427DCF812493662B332E23D3
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.083089469074266
Encrypted:	false
SSDEEP:	12:TMHdNMNxOE5JwJUnWimI002EtM3MHdNMNxOE5JwJUnWimI00OYGVbkEtMb:2d6NxO6JwJUSZHKd6NxO6JwJUSZ7YLb
MD5:	D4EB40F19C21A3D1D108B15C0B5A3B81
SHA1:	A7D8A61EE891BBD97C503D896089DA149401EE15
SHA-256:	1DA5284F20813D02A96CB77544726EC0C82A3DE39C95DA957E3626D72CA5F14C
SHA-512:	B6D217CE8EB3DAEFA1FC217B183210F774E1559539164509EA4A8440A34EC59458667E1B2CD586113C8465C9EB8E74B5254E0E5CC3EE11789C948BBA1262A39
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x2cb3f4f4,0x01d6c4fe</date><accdate>0x2cb3f4f4,0x01d6c4fe</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x2cb3f4f4,0x01d6c4fe</date><accdate>0x2cb3f4f4,0x01d6c4fe</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Twitter.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.142993666861389
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kW1SnWimI002EtM3MHdNMNxe2kW1SnWimI00OYGkak6EtMb:2d6NxriSZHKd6NxriSZ7Yza7b
MD5:	024B059C353A3881291C00CB7AB461E4
SHA1:	60D52D94CA48868A4D8C161A3E7351513943486F
SHA-256:	4CEC9883510B76743101231700FBAD96D6A0AEF1D156AE9386D9A5261E90431F
SHA-512:	2E936AFB43A879E8D19C20B1D84270DDCD3CB0CAB9A316535F0E04B78F2D856EEB949DD5D2869EF96AB5C3DA744295692DA5CD22F0765E032592EF5F31DFF49
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x2c9758cb,0x01d6c4fe</date><accdate>0x2c9758cb,0x01d6c4fe</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x2c9758cb,0x01d6c4fe</date><accdate>0x2c9758cb,0x01d6c4fe</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Amazon.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	662
Entropy (8bit):	5.103509253257359
Encrypted:	false
SSDEEP:	12:TMHdNMNxvL5JwJUnWimI002EtM3MHdNMNxvL5JwJUnWimI00OYGmZEtMb:2d6NxvVJwJUSZHKd6NxvVJwJUSZ7Yjb
MD5:	A4B46428EA6084E3106A1678E425E4D1
SHA1:	88723B8CD30B47092BFC44B0899C5F26B3CDB6AC
SHA-256:	308E9A8DDC79440D901EC215FDA94C192BA95B46D88B04E0F36FD01A1A5FCB4F
SHA-512:	3511200CA4F6B189FCEDB0D6BDE2B1FAC10234DED4668B8698B7F99E8E938009B18664213AF30F30D044921E225374D4BC2905305EF169B747BF073F04136F43
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x2cb3f4f4,0x01d6c4fe</date><accdate>0x2cb3f4f4,0x01d6c4fe</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x2cb3f4f4,0x01d6c4fe</date><accdate>0x2cb3f4f4,0x01d6c4fe</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Wikipedia.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	647
Entropy (8bit):	5.113557056117123
Encrypted:	false
SSDEEP:	12:TMHdNMNxi5thtznWimI002EtM3MHdNMNxi5thtznWimI00OYGd5EtMb:2d6NxALNSZHKd6NxALNSZ7YEjb
MD5:	CD9C6116FD523BDADFE38CAE491A5B0A
SHA1:	7034CEC5472D1F9575C22DA4CF35394DE3EF384D
SHA-256:	532742F78FDFB43D60F305507D781FF4FFF878E34B1E2C2CD77F5DFE208F8453
SHA-512:	AC35BDF44EE92A0919D458E62E826A1CDFB8E9B0F9904470A614C43D0953ADF802EF90C6E63C628D8BC60F69EE1359645B7C3D0C803EBCFEE5F39AF115700D9
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x2cb192c7,0x01d6c4fe</date><accdate>0x2cb192c7,0x01d6c4fe</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x2cb192c7,0x01d6c4fe</date><accdate>0x2cb192c7,0x01d6c4fe</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Live.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.140616583282425

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGw5GwGUnWimI002EtM3MHdNMNxhGw5GwGUnWimI00OYG8K075EtMb:2d6NxQOV3SZHKd6NxQOV3SZ7YrKajb
MD5:	80A5E085835C23F8853118D243D1661D
SHA1:	4A37F59A29B4EB317A5540D828FD6B6CE70104B0
SHA-256:	A79F7C3B9B0829C91D799D0A08AED81EEE6246E3C1E64AE09C0AA5F7C505D722
SHA-512:	9A71B38F63D31B1CAA71F643AF3D60B13E00809CB41B82865F10C1EA3989F3842010E2A3CDF51AF50213106A11563482385C5FD8A94FE4FC2BB5F292030847B3
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x2cb65746,0x01d6c4fe</date><accdate>0x2cb65746,0x01d6c4fe</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x2cb65746,0x01d6c4fe</date><accdate>0x2cb65746,0x01d6c4fe</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Youtube.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.086801896355801
Encrypted:	false
SSDEEP:	12:TMHdNMNx0n5JwJUnWimI002EtM3MHdNMNx0n5JwJUnWimI00OYGxEtMb:2d6Nx05JwJUSZHKd6Nx05JwJUSZ7Ygb
MD5:	C0ECBF06326EBD0E2313148860146E56
SHA1:	C74E22D0D98E131854095CC1B3EAAE7A9343EF8A
SHA-256:	8731BC8D3401F02E0FB7853BFE264E35709814159DC5EAC0F122140DA4DE7417
SHA-512:	0B139772A88B43D1E9FE99566EA8375F44BEB46760CED9D6E3329E4C4682FB0CF6D39B84D2FEE44D6924B22BEAE1A52C7907A4077E609650B588C773DAFCCD02
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x2cb3f4f4,0x01d6c4fe</date><accdate>0x2cb3f4f4,0x01d6c4fe</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x2cb3f4f4,0x01d6c4fe</date><accdate>0x2cb3f4f4,0x01d6c4fe</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Reddit.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.14024690155092
Encrypted:	false
SSDEEP:	12:TMHdNMNxx5thtznWimI002EtM3MHdNMNxx5thJUnWimI00OYG6Kq5EtMb:2d6NxrLNSZHKd6NxrLJUSZ7Yhb
MD5:	E993FE3A142088BC96C2877713B53E85
SHA1:	033823372349ADEC3CD3863A6CCEEFE5304885A2
SHA-256:	B913B923A01B7E086BDBA58E4B62A6293DA8194621C2D34A17AC2B4982B4DE13
SHA-512:	409B4BE9A69724C19B1D8E32D217ABB9EB60416F540D8E87807460F20171F59D326C1BC3336EC949A5C341C4B0C08E7306208B6F8E36D096EDB9A7E7CB82AC5
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x2cb192c7,0x01d6c4fe</date><accdate>0x2cb192c7,0x01d6c4fe</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x2cb192c7,0x01d6c4fe</date><accdate>0x2cb3f4f4,0x01d6c4fe</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\NYTimes.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	659
Entropy (8bit):	5.114411621296671
Encrypted:	false
SSDEEP:	12:TMHdNMNxceKlKKnWimI002EtM3MHdNMNxceKlKKnWimI00OYGVEtMb:2d6Nxk4KSZHKd6Nxk4KSZ7Ykb
MD5:	CC6AD61B116CA31D1664AE0BE3F3B732
SHA1:	310D8949735EB8BDFD1578F083FC00E491FF9467
SHA-256:	FF3DAC353ABAE1118A6938927ED5289F18BA19D6389E247784BC760F0CA46CB2

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml	
SHA-512:	8D4157869484420F54B39E5033B1C5E0DC8B1F9D2E3F49C84AA1A3CAF80CBC7C0893CF2F80CF9C19C1DC0CC24E599DACF25FA4BD551E4EB0EB7DC962AEC5E1A
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x2c99bb30,0x01d6c4fe</date><accdate>0x2c99bb30,0x01d6c4fe</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x2c99bb30,0x01d6c4fe</date><accdate>0x2c99bb30,0x01d6c4fe</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Facebook.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.098862002831288
Encrypted:	false
SSDEEP:	12:TMHdNMNxfn5thtznWimI002EtM3MHdNMNxfn5thtznWimI00OYGe5EtMb:2d6NxxLNSZHKd6NxxLNSZ7YLjb
MD5:	ABE2A5FEC7912D5EAAC7CB77530B0A57
SHA1:	9672C2111B7223E3862E0BC40B2EB40878D17339
SHA-256:	FEF0F884953F422EB9DC59C95AF5632BEF50E32CD88F896992AD91132D770DE1
SHA-512:	894F430B93A1DD1066EC1611F4FB3C22660C12D80336D39DD14DA254B8066ECEE42FAC70EBA6D6A1BC5128CFB4AA226497CFE3850BCA40569E5CADD50F9F5B5
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x2cb192c7,0x01d6c4fe</date><accdate>0x2cb192c7,0x01d6c4fe</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x2cb192c7,0x01d6c4fe</date><accdate>0x2cb192c7,0x01d6c4fe</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Google.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\JTURjIg1_i6t8kCHKm45_bZF3gnD-A[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 23628, version 1.1
Category:	downloaded
Size (bytes):	23628
Entropy (8bit):	7.97652223541331
Encrypted:	false
SSDEEP:	384:aWXmwssTJH1/G6rbr24Jln5GTJO8XWSN2OyyW/nGGxnslEYe3cB68HOeHS9AVqmT:aW2wdx1/HPCQln5F8XL2frP5pMB68H/N
MD5:	7C839D15A6F54E7025BA8C0C4B333E8F
SHA1:	09FC9F1CA6B859952A3641EDBFB1424E1C873F5D
SHA-256:	46226ABFCDE5DB2598FED8FD0DE77AF9B96C8242DC0E72242971F0BBCF566A38
SHA-512:	239EDDCB1FE723077F1FDC76B265A3D5E6F946F5258C968B15AB99CDD817D0D67D85248DA13820D9EBF0EA256F1E29ADB975894707E1901BCBDB0C2908ABC8C2
Malicious:	false
Reputation:	moderate, very likely benign file
IE Cache URL:	http://https://fonts.gstatic.com/s/montserrat/v15/JTURjIg1_i6t8kCHKm45_bZF3gnD-A.woff
Preview:	wOFF.....\L.....GDEF.....G...X.g.^GPOS.....2....!GSUB.....,.OS/2...|...M...`Ti.mcmap.....h.cvt .....d....2...fpgm.....F...mM$.\|gasp...<..... ...glyf...D..4..._.F.1.head..S....6...6.Z..hhea..S@... ...$....hmtx..S`...$...>*...loca..U....!...(N.e.maxp..W.... ... .h.Wname..W.....+.FOpost..X.....D.z.prep..[.....K..x.%.... P.....@:D...$..]!....h.....2/.$....D.^.F..ua.].N....%>./...x...p.I....RK..Z-...m.-.= .a.....1.0..n.....-h....C!.....Wm.F3....J~/..\|.....*..._]F....Y.x.._.....s.w!.S...'..9d...(...5.).O. z.>...OQ..7J'....>...J.:..K$a6. .._P.lXP."....6....le.sY5.n.t"'.C..-..5.2...4.}..H.P....w.....OX.....)8....7?..H..I.@|.....R.'..#R.:....{C}....V.%.i...v.L9K..C.....N".r.P.../..7.UN..'..0...- .Q..M..o.6.....-.&l..B.w..x.....e>....CB....&.....&..P.S....3..Y...Q>/..e...B.+..|.o0..I.#L.]a...../.....&..gLz....J...g!.,$..4#...2L..>.P...gF.67.@.}...IX.&....?Vi....ORR

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\JTURjIg1_i6t8kCHKm45_c5H3gnD-A[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 23872, version 1.1
Category:	downloaded
Size (bytes):	23872
Entropy (8bit):	7.9789410515218915
Encrypted:	false
SSDEEP:	384:WCPZ9khezoAK1PfDV/cGTJO8gpFu2KobVfXpH2h1AdWJ8OjcmB2SrOFbYvaUP5KR:WCPUwzj0jV/cF8CFubobVf5WEdCjvBFw
MD5:	9A9BEFCF50D64F9D2D19D8B1D1984ADD
SHA1:	1DAD9D9EFE7BC0B3BA089BE10B8F9741A02312A3
SHA-256:	2849C719C361F2EC1A04BF5B262BCBEDD3DF46BF35F5B4CAE8F75EA0AC500111
SHA-512:	5EC89892CC2453CBC6B9F64C3A261491B3EFF35EA65586B65200D8F3FFB31A727A4F7592D4BD86519EED54FDA35D6A79799300CB2537E5602D5D5AC908C5639
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\JTURjIg1_i6t8kCHKm45_c5H3gnD-A[1].woff	
Reputation:	moderate, very likely benign file
IE Cache URL:	http://https://fonts.gstatic.com/s/montserrat/v15/JTURjIg1_i6t8kCHKm45_c5H3gnD-A.woff
Preview:	wOFF.....]@.....l.....GDEF.....G...X.g.^GPOS.....2..=.GSUB.....,.OS/2.....O...`U6..cmap.....h.cvt .....e....56..fpgm.....F...mM$.|gasp...D..... ..glyf...L..4...aZ-...head..S....6...6.t..hhea..T0... ...$....hmtx..TP...%...><..Eloca..Vx.....(y...maxp..X.... ... .[.Mname..X.....+.G.post..Y.....D.z.prep..\.....K..x.%....P .....@:D...$..]!....h.....2/.$.....D.^.F..ua.].N....%>./...x...p#.....c....L..33333333. .....y...T.u.Og.Y0t..rMY.s.....c. ..<.....'Rz..^.J._..7..[..0#.R_.>!.W.....B.l.yRmD.B.P..ap. Y.v.S....bC6m.m..YBd....m..6..W.@..Q....C..Uq.2.;.HH..N*..@.]D...Pb..... .. ..[o'..*.{..x.*&uf.W.$@...U`.b.!.....W.=i.....T.....0.3V...)Q.S.`..{?....u\.0.....&$..'"`X.9&2. .L...".... ..z>(.|H.....V>.z....G"....v~*....S..".....Q.L..Y...9.",.../.Xd.Td.\t....[..W..'../Z8 .9(Z8$.....2....T...c....0)b..iL...,P.. ..0.Y...6.eZ....Ln..l;.D.BhU..k.O..... .by1..*.F.g..M.]...M...!.n.-.;.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\JTURjIg1_i6t8kCHKm45_cJD3gnD-A[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 23256, version 1.1
Category:	downloaded
Size (bytes):	23256
Entropy (8bit):	7.977753236160612
Encrypted:	false
SSDEEP:	384:2gMWysI22L2wL/yhGTJO87uvLzyBFvQ3dol9ET1Em9FOgBhkIkYaUpIJ8eQ0iUiJ:2gMWX12LvDyhF87GzUvSCjYD9FOgvsYl
MD5:	8DC95FAB9CF98D02CA8D76E97D3DFF60
SHA1:	FA51AFC9A31F67078FAA9124BEF881655DF4317B
SHA-256:	25F8F00A6FE95DED91A8E33E70154AEE1562760D0D969368D4BAD84BFE85F8D0
SHA-512:	992131CBE01D3DC13831557DD59368B6870BEE453D0C753A5814D001B11327DB60CDEB8D71E4B579E1A5C0238F08E07DF1267CB645738C96197C808E24443A4E
Malicious:	false
Reputation:	moderate, very likely benign file
IE Cache URL:	http://https://fonts.gstatic.com/s/montserrat/v15/JTURjIg1_i6t8kCHKm45_cJD3gnD-A.woff
Preview:	wOFF.....Z.....@.....GDEF.....G...X.g.^GPOS.....2....yGSUB.....,.OS/2...L...O...`S6.Mcmap.....h.cvt ...`...b.....:.Gfpgm.....F...mM$.|gasp..... ...glyf.....2...[H.xz.head..Q....6...6.<.ehhea..Q.... ...$....hmtx..R.....>....loca..T.....(.J.-maxp..V8... ... .h.Zname..VX.....)!Etpost..WD.....D.z.prep..Z.....K..x.%.... P.....@:D...$..]!....h.....2/.$.....D.^.F..ua.].N....%>./...x...p[I...'=..3[.G._.....WpL..... `.#o.)g9g.....2._=..==._.D@..x.....o....~.....{..)N$.0.Q...M...?..OQ.X..xo.i..Z...s...n".hI.K .%.a...m..U..l.....6...s...6..<...Z....@myrT...q.${....@.Sl1.@.....N/...k=`?...X..3G$.Z.@=^WK.....c..[a..@[hG.T.I...jF...NVqB..V..+....(...7h.^.i.rB.k.`'{.>.W....B..B.n!.W.h.F. '.=a...r.@.....?.j..0...3....."?..s.....d*W.1Ws..\+d.N.....n....[h.V!.6!.....+..._.".h.e.TV.....X%4.Zh.]hf.PO..g#.4~.0.2]*w.u.".....$.....-Q.%4...C....hf>.....6"..A.)S.....dK...N. ..._X.G....3.....*.uA

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\JTURjIg1_i6t8kCHKm45_dJE3gnD-A[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 23836, version 1.1
Category:	downloaded
Size (bytes):	23836
Entropy (8bit):	7.979463633723131
Encrypted:	false
SSDEEP:	384:1JCJnpTwnH5O+5hR1GTJO8Ir7BxLJMmel49Ryt+3qiixubNtKBG2DWmkahwV:1w56nZO+5hbF8I5xLJ649MabNCpDkCwV
MD5:	80F10BD382F0DF1CD650FEC59F3C9394
SHA1:	46F6D60D4AC25FC1AA385513C42A58D89BAB45BA
SHA-256:	2A5AFDAC758F2E6A3FD3709719001951708D9F27E7E55ADF9C33B69814A4CD50
SHA-512:	0597EDDF1926C95D792772D3797646AA1E6A294BF023B179CDA1396690AB8B7EAB5394FC896D49A77C161B59D45AB69C53269D869EF40AE83812AC03AA6593B
Malicious:	false
IE Cache URL:	http://https://fonts.gstatic.com/s/montserrat/v15/JTURjIg1_i6t8kCHKm45_dJE3gnD-A.woff
Preview:	wOFF.....].....GDEF.....G...X.g.^GPOS.....2....GSUB.....,.OS/2...l...O...`T.Ycmap.....h.cvt .....e....3..=fpgm.....F...mM$.|gasp...0..... .glyf...8..4..._...qhead..S....6...6.i..hhea..T.... ...$....hmtx..T8...&...>37.hloca..V`.....(Wjn.maxp..X.... ... .[.Mname..X.....*SE.post..Y.....D.z.prep..\`.....K..x.%....P.. ....@:D...$..]!....h.....2/.$.....D.^.F..ua.].N....%>./...x...p.I.E_..z.-....4f.....!.0..i.ye...5..l+.j.n..p.f.y.....*UuK.6....^B.Q.y.(....x.....w...D.f>+.E...{.....S[...g...Q...v.ap.....&....Q.T.. [...v.]o.v....P.....? K..l.|.HD.....e.Q....Yl.i...D, ...n.OR.|.[....p+.PF}....D@D3.{.....l..'Mv.bE.L.....E.0.....Hl.....~P+R.....Np.s..KH..''...9!r...=..^..U|B..b....|Z...(.Y1...|^..... .,~.B~./).+..k~C...1..<.:....\"....h.r.q.....kE..E.....N....nQ....^..>.H.hb....!.S.(..1.'D-gD.Y..#f.+j.d.. .....AtW.whb..`...M..Rb..Fo.....:.*.['y.y._.n...w....m...P..EV..I6..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\css[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	1538
Entropy (8bit):	5.212336098192914
Encrypted:	false
SSDEEP:	48:nOOS7iOOJEOOW+HEOOLVOOgauOOxTkOOCLOOw6W:nOOS7iOOJEOOW+HEOOLVOOgauOOxTkOG
MD5:	539812A7B7DC64066B13E481FC603497
SHA1:	0CF448BFE27BE46DEB47A88D6C02B18703B3E0AA
SHA-256:	BE2D1095FCBD9D62862AAA227171B2DF700A625F13226136D0C114269C01711B
SHA-512:	B2A1BBE42F4CC4E8B18CBB5E9122E8964E5F89DCF603B63BB54134112E0468C2DD343F52A2177784FAFBD9AEEA637B080D39881AEECA13F8038B7472B1C731D C
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\css[1].css	
Preview:	@font-face {. font-family: 'Montserrat';. font-style: normal;. font-weight: 100;. src: url(https://fonts.gstatic.com/s/montserrat/v15/JTUQjIg1_i6t8kCHKm45_QpRyS7g.woff) format('woff');.}.@font-face {. font-family: 'Montserrat';. font-style: normal;. font-weight: 200;. src: url(https://fonts.gstatic.com/s/montserrat/v15/JTURjIg1_i6t8kCHKm45_aZA3gnD-A.woff) format('woff');.}.@font-face {. font-family: 'Montserrat';. font-style: normal;. font-weight: 300;. src: url(https://fonts.gstatic.com/s/montserrat/v15/JTURjIg1_i6t8kCHKm45_cJD3gnD-A.woff) format('woff');.}.@font-face {. font-family: 'Montserrat';. font-style: normal;. font-weight: 400;. src: url(https://fonts.gstatic.com/s/montserrat/v15/JTUSjIg1_i6t8kCHKm459WlhzQ.woff) format('woff');.}.@font-face {. font-family: 'Montserrat';. font-style: normal;. font-weight: 500;. src: url(https://fonts.gstatic.com/s/montserrat/v15/JTURjIg1_i6t8kCHKm45_ZpC3gnD-A.woff) format('woff');.}.@font-face {. font-family: 'Montserrat';

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\JTUQjIg1_i6t8kCHKm45_QpRyS7g[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 22500, version 1.1
Category:	downloaded
Size (bytes):	22500
Entropy (8bit):	7.977478630884967
Encrypted:	false
SSDEEP:	384:qF14bCC33a2W8VT2+GTJO86XMfb0kqRQ6o7aaxESXN22ujw6lYkkjt9UwV:qF142Cy8VT2+F86XiwkoQNaaxLA2u0tt
MD5:	370318464551D5F25B0F0A78F374FAAC
SHA1:	20F4EC409A5E86EA89FE26BE42FDABFD11DC867C
SHA-256:	0B89EA33174D7ACB702309A88B66B3422189BDDC0BB5961A90116A21A98E848A
SHA-512:	B15A41753EF3AEB7355C647C5A40D30A65FBE9F347EFEAE9505D7C789B9447F2A58168F14F0BBC2CC8204274FF317F2305C35075833021C1308707796566FB24
Malicious:	false
IE Cache URL:	http://https://fonts.gstatic.com/s/montserrat/v15/JTUQjIg1_i6t8kCHKm45_QpRyS7g.woff
Preview:	wOFF.....W.....GDEF.....G...X.g.^GPOS.....2..1..7.GSUB.....,.OS/2.....L...`S..@cmap.....h.cvt .....\...,...fpgm...,...F...mM$.\|gasp...t..... ..glyf...\|..21.._.=.V.head..N....6...6.0.Yhhea..N.... ...$....hmtx..O.....>...]loca..Q$.....(>RU$maxp..SD... ... .h.\name..Sd.....)JD.post..TP.....D.z.prep..W(.....K..x.%....P .....@:D...$..]!....h.....2/.$.....D.^.F..ua.].N....%>./...x...l$...F..mw...=`.L/..13333333333.2.O...\|:.`yW~..O...)U.ny<^.....J.....d.'S....H.g.../d.....s.U.^.\E<P.)Sy..^.b...@..Zo.<..Th V.#'R...*..}.....jo....r`.....b...5....#.....]..}5.....N...s>.R..t.O]Z.((R...N.....r..R-..s._s..6e."tR)./.V.tm.z..W.. ..k..../...e%q.9"f=.4^b..X.....rQ..b....*\..r]..y"W.H....;.C.30...yw` ....yo`....x.`;..l.{.2...L..@...c2~....@...2~.h..@..5c.&P.6..LpB`+'..rJ`..s&.....@.y.&..F. .d!0..2.....$K.I...&...+.%...;..B.?.g.JY).I...H.zI..Kz...n.uk....{..U..] '.X....Z..Y..(7W...?.9.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\JTURjIg1_i6t8kCHKm45_ZpC3gnD-A[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 23576, version 1.1
Category:	downloaded
Size (bytes):	23576
Entropy (8bit):	7.979995638545985
Encrypted:	false
SSDEEP:	384:evykH+9E9B49CndLoAUlGTJO8OzoRb1Jrb7ZlZ/EYh93e1rRykMKAZir2k4lyPmo:eqP9sC2dXUlF8Ozc5JrbNr/EM93eZRhl
MD5:	8B763220218FFC11C57C84DDB80E7B26
SHA1:	E85E6898C8FD8B095BD694B3F1350342C7BB3F35
SHA-256:	299E5F2B6E651BFD7B4C74AA12B06BB10A1200757CC4EBD1FC4C0D9D1AAFA00D
SHA-512:	4A93693CDE6B4BAEAD17A78C6B3FF7BD9F7489D20E5BE3815751B4A1E4E034E7BB54249DEF7F8E06B3ADE41E4333F45FDB232E67971C1817F66151F1440BDE32
Malicious:	false
IE Cache URL:	http://https://fonts.gstatic.com/s/montserrat/v15/JTURjIg1_i6t8kCHKm45_ZpC3gnD-A.woff
Preview:	wOFF.....\.....GDEF.....G...X.g.^GPOS.....2....GSUB.....,.OS/2...I...O...`T..acmap.....h.cvt .....b....0...fpgm.....F...mM$.\|gasp...,..... ..glyf...4..3...\.)...head..R....6...6.P.xhhea..S.... ...$....hmtx..S,...'...>"...loca..UT.....(...maxp..Wt... ... .h.Wname..W.....*.Elpost..X.....D.z.prep..[\.....K..x.%....P.....@:D.. .$..]!....h.....2/.$.....D.^.F..ua.].N....%>./...x..ex#.....<..d.e.-.1..33333333..y...T.`.V^p.m._.{..9...z..z..5... .<....|...<.-.}9./..._....f.P.J?F.....d...b..DzFm.....&b...!...H..;a.XI.=6gEB..6 N.....]6.I...J..w.hU\6...I.u*ei..@..J.n. .2.D3.. .(ay.....<..j>....s@.n.....Z.U.H@.v..e.....!..s.`wW...u4.8P...x.r...z4...h.....H@.;.g.....,1..)..E.}".S.5..X.{E....._.....".D...=|D..Q... D7...q>.\ .\.E.s.Hp.Hr...r.....+..f..q...\+:.Q..,Bn...g#.l..l..l.i..&v.4;E..D=...I.....R.O.1-.fDDA.1+j8...A.D...?M..w.|.&F.f..1..z....j-o9.V.y.em...vRO.^..-.S..f.q.....j...c....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\JTURjIg1_i6t8kCHKm45_aZA3gnD-A[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 23276, version 1.1
Category:	downloaded
Size (bytes):	23276
Entropy (8bit):	7.978722054298751
Encrypted:	false
SSDEEP:	384:boRxPu4aCGTJO87w6QBiPmWZRAtkRc44kjix7m8bRWca7ztugWPwV:bktu4aCF87mBibZRfRcVkOx5bRVa7ztp
MD5:	1FC98E126A3D152549240E6244D7E669
SHA1:	F77707F0EEB7086952F287C45E0FBA4FC01F1C53
SHA-256:	94221B9AB3055AB8D736B35D9D1573B89BB1EF89A37D4EDC395404E2EA5E4701
SHA-512:	B921DDAF4DEEE17899E67973F49E9EC0C45E50158180F794A115B386BA52CC0CE0DFA961E433624EB2E5F672AD94532F770CA355AB4B942FFA6C5B49C283B0C3
Malicious:	false
IE Cache URL:	http://https://fonts.gstatic.com/s/montserrat/v15/JTURjIg1_i6t8kCHKm45_aZA3gnD-A.woff

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\JTURjIg1_i6t8kCHKm45_aZA3gnD-A[1].woff	
Preview:	wOFF......Z........l.......................GDEF.......G...X.g.^GPOS.......P..2....hGSUB............,.OS/2.......L...`S..Ecmap...(.........h.cvt ....\....-P.mfpgm...H...F...mM$.\|gasp............ ...glyf......3...]R...head..Q....6...6.5._hhea..Q.... ...$....hmtx..R........>...nloca..T(... ...(....maxp..VH... ... .h.Zname..Vh........-ZG.post..WX........D.z.prep..Z0.........K..x.%....P ......@:D...$..]!....h.....2/.$.....D.^.F..ua.].N....%>./...x...p[Y...'...$.%..43.2333333.,...3.4wW..q.cw...r.J...T.Ug.....H....sA...w.{&.r....%_.5.B....~.-?..s.B. .R].:..?....s.?:..qoe...A .....OS..A......hB\..DD7.':.!..j.T......?.s....<..!.A.b.\.N.*.r7Ib.=.d<O=......Q..@....9..l.6....x.-..<.98....e..zZ..*.......tjgXz.d(...h...(.N........e.i..[.%\RP.....r..,q..E...E..pR.Y.%....h...?...c Q.O.Z.T..31......._...J4.k............y..YTx...mb...5.C..N..8..%.#j<&..(.(...^....b=..0G.(.%.8*F..c...../.....Xd.....8'r..I......a<..Q.........1v.5...{b/.dq..hG.ft....SBe.P#W-.o...I.X.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\JTUSjIg1_i6t8kCHKm459WlhzQ[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 23480, version 1.1
Category:	downloaded
Size (bytes):	23480
Entropy (8bit):	7.981253427621622
Encrypted:	false
SSDEEP:	384:lEfDbJfERirQIhTVId2GTJO8Z84zUE8EW3md2T0LuYXDbMdK3OLmvTHc5qawV:lEf3JPrQI8d2F8WDE9w0FLTbMdK+Cvj3
MD5:	8102C4838F9E3D08DAD644290A9CB701
SHA1:	5AF1938D1327395F47C84E57B6BA7756234D2262
SHA-256:	60CEBEA4C9183F51FBD323F14DD729E18768BE4F6395467013216AE36526CF9C
SHA-512:	E8A0D6B72163E407DE82170E4560044CAE90116D1DD3CFA20F140E4379C8AABDC5BEAC6DD965D0E925CA673E41C42A858975C47F1F8152637958569D239E91F
Malicious:	false
IE Cache URL:	http://https://fonts.gstatic.com/s/montserrat/v15/JTUSjIg1_i6t8kCHKm459WlhzQ.woff
Preview:	wOFF......[........8.......................GDEF.......G...X.g.^GPOS..........2.....GSUB............,.OS/2...\...N...`S..Ucmap.............h.cvt ...p...\..../R.Hfpgm.......F...mM$.\|gasp............ ...glyf......3X..].,..$head..Rt...6...6.F.nhhea..R.... ...$....hmtx..R....%...>.x..loca..T........(..*0maxp..W.... ... .h.Yname..W4........-5H.post..X$........D.z.prep..Z..........K..x.%.... P......@:D...$..]!....h.....2/.$.....D.^.F..ua.].N....%>./...x..ut.I......e+..o...g.^..13333333333.-.e/.cgYAs....R.{.G..^.L......j.......R.z..D..o...~......$.`.BY.21.W.......9...f.C..(..M.!..D....1rT ...w6cG.J....U.......]..>........q..jhT\l..;,M.zYK..x:.n.R...(........g)..~...Xl#`......-.#..T...]..Tw........k.7....I.....@..$..r....X.\..L......_.H.2".V... .1..."._d.#R..4c"...2> ..A..D;..e>".|Tt.1. ....8...._.K..+........Y~'r.A.....D.../..W..ob.....[.8K.8Gtq..0...|....D.KE+..".V.....\vr.._-.Se..=..A.1$...<.E.CL..%QB.8.9.....,.Jv.=,...%.i..:U*V..U.b..]N.D..O..'...1.$.....<

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\bg[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 1754 x 1241, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	151257
Entropy (8bit):	7.864872000040117
Encrypted:	false
SSDEEP:	3072:LVVVVVVVVVVSuVVPh30+BXVVVV0dvq1n4FUn8Cd/DDyEpvtQ++IDwQe9hFa5RmOg:LVVVVVVVVVVSuVVPhk+BXVVVVGFUnT1M
MD5:	023FED3CB03DA29F36AC3C954CD09C56
SHA1:	A059278B9FFBC9FD1E57B75A2AD8F9AB8FCC89BB
SHA-256:	CEC810BF14B7FE0E573C237B30E8EEBBDB22C2D0A96420D3928E0B4150C0D06A
SHA-512:	F95AA0B4C910E785ED0A1E3C2B05C6841B72017AEBDAAA78FA26E0963EE3F0AD67544A31342AF59B9DE0C637C536D59831B06A7837E955061EF3FD2D29AD5C 5
Malicious:	false
IE Cache URL:	http://https://mayhutsuahanoi.com/wp-admin/images/bg.png
Preview:	.PNG........IHDR.............Zs.%....sRGB.........gAMA......a.....pHYs...t...t..f.x....IDATx^......a.H....s.s..L.$.....\|...h..j..Z{...v...%rG...O.H.$I.$I.$Iz..~.J.$I.$I.$Iz..m.$I.$I.$I....$I.$I.$I..., .I.$I.$I.$I'Xh.$I.$I.$I.N..&I.$I.$I.$.`.M.$I.$I.$I:.B.$I.$I.$I.t..6I.$I.$I.$...m.$I.$I.$I....$I.$I.$I...,.I.$I.$I.$I'Xh.$I.$I.$I.N..&I.$I.$I.$.`.M.$I.$I.$I:.B.$I.$I.$I.t..6I.$I.$I.$...m.$I.$I.$I....$I .$I.$I...,.I.$I.$I.$I'Xh.$I.$I.$I.N..&I.$I.$I.$.`.M.$I.$I.$I:.B.$I.$I.$I.t..6I.$I.$I.$...m.$I.$I.$I....$I.$I.$I...,.I.$I.$I.$I'Xh.$I.$I.$I.N..&I.$I.$I.$.`.M.$I.$I.$I:.B.$I.$I.$I.t..6I.$I.$I.$...m.$I.$ I.$I....$I.$I.$I...,.I.$I.$I.$I'Xh.$I.$I.$I.N..&I.$I.$I.$.`.M.$I.$I.$I:.B.$I.$I.$I.t..6I.$I.$I.$...m.$I.$I.$I....$I.$I.$I...,.I.$I.$I.$I'Xh.$I.$I.$I.N..&I.$I.$I.$.`.M.$I.$I.$I:.B.$I.$I.$I.t..6I.$I.$I. $...m.$I.$I.$I....$I.$I.$I...,.I.$I.$I.$I'Xh.$I.$I.$I.N..&I.$I.$I.$.`.M.$I.$I.$I:.B.$I.$I.$I.t..6I.$I.$I.$...m.$I.$I.$I....$I.$I.$I...,.I.$I.$I.$I'Xh.$I.$I.$I.N..&I.$I.$I.$.`.M.$I.$I.$I:.B.$I.$I

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\login02-popup[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 85 x 91, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	6814
Entropy (8bit):	7.955540757983621
Encrypted:	false
SSDEEP:	192:cQk/Uaeo9OwYofHP7afr9L5wJwX2fpewJKjVuolk7:tkv9Z3fHP7K5McdwJIVTla
MD5:	4471AF82137EBFF6EA410E89494B26CD
SHA1:	2F096294635A945E92C04C033879558C5AEBF425
SHA-256:	466A3C3DE2F7C452C01308B5DB8A1532FB14E8372F3EE44D9B2EE4F991249B4C
SHA-512:	F27D6694DFE85926F03296A958F26C812FEB8CC2C12001E8BA22E4CA29BE3C70F455C2DB251E954B4E9DCC9CCC39AAABF661864E7AF236D57F279750DDDD73 D
Malicious:	false
IE Cache URL:	http://https://i.ibb.co/9nnrtWy/login02-popup.png
Preview:	.PNG........IHDR...U...[........*...eIDATx^..t.U..3//...P..%.H.f.......(.....V.=(...z...*..Y...,,,.......r(.DQz ....@z....|of...W.%.-...N.{w.......-....f..,..4...;?..w...}.$I.6....K...zu.9..>...%.5}T. ...M6..%.,.?a.]..g..C.....KR....>J..6...S.L)..`.6....z....8q.*(...c.<?.UW.........#&&..,k.P.<...."XXz.....S.....V_.gz.6k....-....n...Rk(..".."^.....hJk.V....RKj]...I.&.E...g(...b.>}......].%h. {...M.z..Y^^~....mz...#.....z..../.....9.)--ENN.M.5O].....)S.{..K[.z.QQpX,u^.i.PQQ.C..!;;....0.LZ>.N.s..>.S h...6...@5.Z.<...._.1...._.@.o...>........0U.G.......<.t....'...5....Ng.O.....;.. .k...F.}Cz..Zz.V.%.;..3.P.*b.)h.I.....PY?...l.../I.a..<t.......t..%._$....?.TU...p)?}....].u..]..p...Q.......`....._...i...<...v.....~T...I.zO.81'.....^..j.e....M.*T...?0./.......K..SR..]&......WG.>..c.... {/..={...#..&M..U0.....\.C=.GXD....J..iv..3PQ.L?..+.J..-].(..3...[0r.H]..x."..........y..R$.{.}z._...R/._NI...Q...5?9./^...!...n.......::.u.FM....%$.!O=...;...].]..`....p..^.9.W

C:\Users\user\AppData\Local\Temp\~DF5036BE639DAA6BD0.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.27918767598683664
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laA:kBqoxxJhHWSVSEab
MD5:	AB889A32AB9ACD33E816C2422337C69A
SHA1:	1190C6B34DED2D295827C2A88310D10A8B90B59B
SHA-256:	4D6EC54B8D244E63B0F04FBE2B97402A3DF722560AD12F218665BA440F4CEFDA
SHA-512:	BD250855747BB4CEC61814D0E44F810156D390E3E9F120A12935EFDF80ACA33C4777AD66257CCA4E4003FEF0741692894980B9298F01C4CDD2D8A9C7BB522FB
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFCC1AE6323AC17F44.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	35939
Entropy (8bit):	0.591160687945792
Encrypted:	false
SSDEEP:	48:kBqoxKAuvScS+npLC2I2MAntzIWoEGzIW2KRK1c0:kBqoxKAuvScS+npLCJt4IWoEoIWo9
MD5:	E9A57A694F9E8E5C423720175D3FEAEE
SHA1:	3DCFD92FAD56C6E51D421371BD177E0F298A8B88
SHA-256:	78D630BEB882C12E277E976E288EC58115E2708518299D5DA64658C4E66E8172
SHA-512:	9996E5270B8CD01456D04C8C9089711E9F70474F9695A34D32C92AB91C880D2E4CE3081F3689E141738D7C0F935D80AC4C647E7EFA5B57E13046B00E2A9AA1A5
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFD78511B2F90E11B4.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.474195121871003
Encrypted:	false
SSDEEP:	48:kBqoIVfdVfbVfhf/fJf4f/f8fmf8fvfdf4fdf3:kBqoItdtbt5nx4n8u83l4l3
MD5:	987F20E5D953D0CFA20955AF13B1E782
SHA1:	0F373B8FC8F8E18F4D5BD918739E64FB6380FE4E
SHA-256:	51344F23F270CAC3536E8D5D93BED39A3F6D0BE8D12259D2C627F5D07DBA0D29
SHA-512:	04DDEE1FAE3CB8C274E9B3E107020E5BADD07B03BE4441BF792C988F14D1E75DC631075311A5927ACC73615E6E314F45991C5A67942F9256688817BC868BF138
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

Static File Info

General

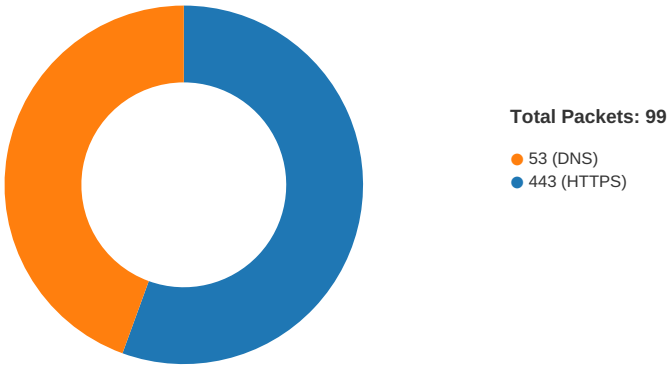
File type:	HTML document, ASCII text, with very long lines, with no line terminators
Entropy (8bit):	4.769692508644787
TrID:	• HyperText Markup Language (28028/1) 100.00%
File name:	INVOICE.html
File size:	8952

General

MD5:	c23676897af888d51882cc82cdb613f5
SHA1:	425fd76dd126543ba5e2548090e701d387d0fd0a
SHA256:	662992de22ac1118ff3ef15bf9f2505aab3de92012e2850b89dac517ec35f532
SHA512:	2431f1d88235696bf0beb2f88380cd387ee3a74ae40179a654366573344ba145782202c9c6c4278a154097d79d3d1a55718c3fc984b609975787ab4d7128fc01
SSDEEP:	192:ZaDaYGZlQpakMQAC66WaoOMt7D09AfaXBruabH5q:3YG4pmBnml
File Content Preview:	<script language=javascript>document.write(unescape('3C!doctype%20html%3E%0A%3Chtml%3E%0A%3Chead%3E%0A%3Cmeta%20charset%3D%22utf-8%22%3E%0A%3Cmeta%20name%3D%22viewport%22%20content%3D%22width%3Ddevice-width%2C%20initial-scale%3D1%2C%20maximum-scale%3D1%2C

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 21:44:28.981460094 CET	49738	443	192.168.2.4	103.221.222.30
Nov 27, 2020 21:44:28.981544971 CET	49739	443	192.168.2.4	103.221.222.30
Nov 27, 2020 21:44:29.118773937 CET	49740	443	192.168.2.4	145.239.131.60
Nov 27, 2020 21:44:29.118820906 CET	49741	443	192.168.2.4	145.239.131.60
Nov 27, 2020 21:44:29.144484997 CET	443	49741	145.239.131.60	192.168.2.4
Nov 27, 2020 21:44:29.144505024 CET	443	49740	145.239.131.60	192.168.2.4
Nov 27, 2020 21:44:29.144623995 CET	49741	443	192.168.2.4	145.239.131.60
Nov 27, 2020 21:44:29.144679070 CET	49740	443	192.168.2.4	145.239.131.60
Nov 27, 2020 21:44:29.145786047 CET	49741	443	192.168.2.4	145.239.131.60
Nov 27, 2020 21:44:29.146142006 CET	49740	443	192.168.2.4	145.239.131.60
Nov 27, 2020 21:44:29.172574043 CET	443	49741	145.239.131.60	192.168.2.4
Nov 27, 2020 21:44:29.172702074 CET	443	49740	145.239.131.60	192.168.2.4
Nov 27, 2020 21:44:29.173850060 CET	443	49741	145.239.131.60	192.168.2.4
Nov 27, 2020 21:44:29.173871994 CET	443	49741	145.239.131.60	192.168.2.4
Nov 27, 2020 21:44:29.173942089 CET	49741	443	192.168.2.4	145.239.131.60
Nov 27, 2020 21:44:29.173971891 CET	49741	443	192.168.2.4	145.239.131.60
Nov 27, 2020 21:44:29.175134897 CET	443	49740	145.239.131.60	192.168.2.4
Nov 27, 2020 21:44:29.175153971 CET	443	49740	145.239.131.60	192.168.2.4
Nov 27, 2020 21:44:29.175225973 CET	49740	443	192.168.2.4	145.239.131.60
Nov 27, 2020 21:44:29.175302982 CET	443	49740	145.239.131.60	192.168.2.4
Nov 27, 2020 21:44:29.175362110 CET	49740	443	192.168.2.4	145.239.131.60
Nov 27, 2020 21:44:29.183963060 CET	443	49741	145.239.131.60	192.168.2.4
Nov 27, 2020 21:44:29.184071064 CET	49741	443	192.168.2.4	145.239.131.60

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 21:44:29.185733080 CET	49740	443	192.168.2.4	145.239.131.60
Nov 27, 2020 21:44:29.186032057 CET	443	49738	103.221.222.30	192.168.2.4
Nov 27, 2020 21:44:29.186153889 CET	49738	443	192.168.2.4	103.221.222.30
Nov 27, 2020 21:44:29.186198950 CET	443	49739	103.221.222.30	192.168.2.4
Nov 27, 2020 21:44:29.186286926 CET	49739	443	192.168.2.4	103.221.222.30
Nov 27, 2020 21:44:29.186655998 CET	49740	443	192.168.2.4	145.239.131.60
Nov 27, 2020 21:44:29.187936068 CET	49741	443	192.168.2.4	145.239.131.60
Nov 27, 2020 21:44:29.188236952 CET	49740	443	192.168.2.4	145.239.131.60
Nov 27, 2020 21:44:29.188591003 CET	49738	443	192.168.2.4	103.221.222.30
Nov 27, 2020 21:44:29.188869953 CET	49739	443	192.168.2.4	103.221.222.30
Nov 27, 2020 21:44:29.189172983 CET	49741	443	192.168.2.4	145.239.131.60
Nov 27, 2020 21:44:29.211302042 CET	443	49740	145.239.131.60	192.168.2.4
Nov 27, 2020 21:44:29.211324930 CET	443	49740	145.239.131.60	192.168.2.4
Nov 27, 2020 21:44:29.211460114 CET	49740	443	192.168.2.4	145.239.131.60
Nov 27, 2020 21:44:29.212220907 CET	443	49740	145.239.131.60	192.168.2.4
Nov 27, 2020 21:44:29.212325096 CET	49740	443	192.168.2.4	145.239.131.60
Nov 27, 2020 21:44:29.212389946 CET	49740	443	192.168.2.4	145.239.131.60
Nov 27, 2020 21:44:29.213526964 CET	443	49741	145.239.131.60	192.168.2.4
Nov 27, 2020 21:44:29.213640928 CET	49741	443	192.168.2.4	145.239.131.60
Nov 27, 2020 21:44:29.213807106 CET	443	49741	145.239.131.60	192.168.2.4
Nov 27, 2020 21:44:29.213887930 CET	49741	443	192.168.2.4	145.239.131.60
Nov 27, 2020 21:44:29.214040995 CET	443	49740	145.239.131.60	192.168.2.4
Nov 27, 2020 21:44:29.214071989 CET	443	49740	145.239.131.60	192.168.2.4
Nov 27, 2020 21:44:29.214097023 CET	443	49740	145.239.131.60	192.168.2.4
Nov 27, 2020 21:44:29.214128971 CET	443	49740	145.239.131.60	192.168.2.4
Nov 27, 2020 21:44:29.214142084 CET	49740	443	192.168.2.4	145.239.131.60
Nov 27, 2020 21:44:29.214184046 CET	49740	443	192.168.2.4	145.239.131.60
Nov 27, 2020 21:44:29.214226007 CET	443	49740	145.239.131.60	192.168.2.4
Nov 27, 2020 21:44:29.214234114 CET	49740	443	192.168.2.4	145.239.131.60
Nov 27, 2020 21:44:29.214258909 CET	443	49740	145.239.131.60	192.168.2.4
Nov 27, 2020 21:44:29.214301109 CET	49740	443	192.168.2.4	145.239.131.60
Nov 27, 2020 21:44:29.214310884 CET	443	49740	145.239.131.60	192.168.2.4
Nov 27, 2020 21:44:29.214320898 CET	49740	443	192.168.2.4	145.239.131.60
Nov 27, 2020 21:44:29.214376926 CET	49740	443	192.168.2.4	145.239.131.60
Nov 27, 2020 21:44:29.214771032 CET	443	49741	145.239.131.60	192.168.2.4
Nov 27, 2020 21:44:29.214844942 CET	49741	443	192.168.2.4	145.239.131.60
Nov 27, 2020 21:44:29.215220928 CET	49741	443	192.168.2.4	145.239.131.60
Nov 27, 2020 21:44:29.279225111 CET	443	49740	145.239.131.60	192.168.2.4
Nov 27, 2020 21:44:29.282238007 CET	443	49741	145.239.131.60	192.168.2.4
Nov 27, 2020 21:44:29.393018961 CET	443	49738	103.221.222.30	192.168.2.4
Nov 27, 2020 21:44:29.393194914 CET	443	49739	103.221.222.30	192.168.2.4
Nov 27, 2020 21:44:29.395075083 CET	443	49738	103.221.222.30	192.168.2.4
Nov 27, 2020 21:44:29.395148993 CET	49738	443	192.168.2.4	103.221.222.30
Nov 27, 2020 21:44:29.395201921 CET	443	49738	103.221.222.30	192.168.2.4
Nov 27, 2020 21:44:29.395265102 CET	49738	443	192.168.2.4	103.221.222.30
Nov 27, 2020 21:44:29.395266056 CET	443	49738	103.221.222.30	192.168.2.4
Nov 27, 2020 21:44:29.395322084 CET	49738	443	192.168.2.4	103.221.222.30
Nov 27, 2020 21:44:29.395831108 CET	443	49739	103.221.222.30	192.168.2.4
Nov 27, 2020 21:44:29.395881891 CET	443	49739	103.221.222.30	192.168.2.4
Nov 27, 2020 21:44:29.395911932 CET	49739	443	192.168.2.4	103.221.222.30
Nov 27, 2020 21:44:29.395927906 CET	443	49739	103.221.222.30	192.168.2.4
Nov 27, 2020 21:44:29.395942926 CET	49739	443	192.168.2.4	103.221.222.30
Nov 27, 2020 21:44:29.395982027 CET	49739	443	192.168.2.4	103.221.222.30
Nov 27, 2020 21:44:29.403800011 CET	49739	443	192.168.2.4	103.221.222.30
Nov 27, 2020 21:44:29.404153109 CET	49739	443	192.168.2.4	103.221.222.30
Nov 27, 2020 21:44:29.404280901 CET	49739	443	192.168.2.4	103.221.222.30
Nov 27, 2020 21:44:29.404686928 CET	49738	443	192.168.2.4	103.221.222.30
Nov 27, 2020 21:44:29.405138016 CET	49738	443	192.168.2.4	103.221.222.30
Nov 27, 2020 21:44:29.608855009 CET	443	49739	103.221.222.30	192.168.2.4
Nov 27, 2020 21:44:29.608905077 CET	443	49739	103.221.222.30	192.168.2.4
Nov 27, 2020 21:44:29.608973026 CET	49739	443	192.168.2.4	103.221.222.30
Nov 27, 2020 21:44:29.609011889 CET	49739	443	192.168.2.4	103.221.222.30
Nov 27, 2020 21:44:29.609082937 CET	443	49739	103.221.222.30	192.168.2.4
Nov 27, 2020 21:44:29.609124899 CET	443	49739	103.221.222.30	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 21:44:29.609152079 CET	49739	443	192.168.2.4	103.221.222.30
Nov 27, 2020 21:44:29.609164000 CET	443	49739	103.221.222.30	192.168.2.4
Nov 27, 2020 21:44:29.609191895 CET	49739	443	192.168.2.4	103.221.222.30
Nov 27, 2020 21:44:29.609203100 CET	443	49739	103.221.222.30	192.168.2.4
Nov 27, 2020 21:44:29.609213114 CET	49739	443	192.168.2.4	103.221.222.30
Nov 27, 2020 21:44:29.609251022 CET	443	49739	103.221.222.30	192.168.2.4
Nov 27, 2020 21:44:29.609257936 CET	49739	443	192.168.2.4	103.221.222.30
Nov 27, 2020 21:44:29.609293938 CET	443	49739	103.221.222.30	192.168.2.4
Nov 27, 2020 21:44:29.609304905 CET	49739	443	192.168.2.4	103.221.222.30
Nov 27, 2020 21:44:29.609333038 CET	443	49739	103.221.222.30	192.168.2.4
Nov 27, 2020 21:44:29.609348059 CET	49739	443	192.168.2.4	103.221.222.30
Nov 27, 2020 21:44:29.609374046 CET	443	49739	103.221.222.30	192.168.2.4
Nov 27, 2020 21:44:29.609395027 CET	49739	443	192.168.2.4	103.221.222.30

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 21:44:22.242194891 CET	55854	53	192.168.2.4	8.8.8.8
Nov 27, 2020 21:44:22.269285917 CET	53	55854	8.8.8.8	192.168.2.4
Nov 27, 2020 21:44:23.198626041 CET	64549	53	192.168.2.4	8.8.8.8
Nov 27, 2020 21:44:23.225927114 CET	53	64549	8.8.8.8	192.168.2.4
Nov 27, 2020 21:44:24.232242107 CET	63153	53	192.168.2.4	8.8.8.8
Nov 27, 2020 21:44:24.259491920 CET	53	63153	8.8.8.8	192.168.2.4
Nov 27, 2020 21:44:25.381820917 CET	52991	53	192.168.2.4	8.8.8.8
Nov 27, 2020 21:44:25.417251110 CET	53	52991	8.8.8.8	192.168.2.4
Nov 27, 2020 21:44:26.534337044 CET	53700	53	192.168.2.4	8.8.8.8
Nov 27, 2020 21:44:26.561408043 CET	53	53700	8.8.8.8	192.168.2.4
Nov 27, 2020 21:44:27.576468945 CET	51726	53	192.168.2.4	8.8.8.8
Nov 27, 2020 21:44:27.613470078 CET	53	51726	8.8.8.8	192.168.2.4
Nov 27, 2020 21:44:27.851814032 CET	56794	53	192.168.2.4	8.8.8.8
Nov 27, 2020 21:44:27.887622118 CET	53	56794	8.8.8.8	192.168.2.4
Nov 27, 2020 21:44:28.928096056 CET	56534	53	192.168.2.4	8.8.8.8
Nov 27, 2020 21:44:28.928242922 CET	56627	53	192.168.2.4	8.8.8.8
Nov 27, 2020 21:44:28.935795069 CET	56621	53	192.168.2.4	8.8.8.8
Nov 27, 2020 21:44:28.968302011 CET	53	56534	8.8.8.8	192.168.2.4
Nov 27, 2020 21:44:28.974812031 CET	53	56621	8.8.8.8	192.168.2.4
Nov 27, 2020 21:44:29.115983009 CET	53	56627	8.8.8.8	192.168.2.4
Nov 27, 2020 21:44:29.169317961 CET	63116	53	192.168.2.4	8.8.8.8
Nov 27, 2020 21:44:29.192260981 CET	64078	53	192.168.2.4	8.8.8.8
Nov 27, 2020 21:44:29.196367025 CET	53	63116	8.8.8.8	192.168.2.4
Nov 27, 2020 21:44:29.236166000 CET	53	64078	8.8.8.8	192.168.2.4
Nov 27, 2020 21:44:31.164314985 CET	64801	53	192.168.2.4	8.8.8.8
Nov 27, 2020 21:44:31.191586018 CET	53	64801	8.8.8.8	192.168.2.4
Nov 27, 2020 21:44:32.493155956 CET	61721	53	192.168.2.4	8.8.8.8
Nov 27, 2020 21:44:32.520593882 CET	53	61721	8.8.8.8	192.168.2.4
Nov 27, 2020 21:44:33.502993107 CET	51255	53	192.168.2.4	8.8.8.8
Nov 27, 2020 21:44:33.530256987 CET	53	51255	8.8.8.8	192.168.2.4
Nov 27, 2020 21:44:34.498765945 CET	61522	53	192.168.2.4	8.8.8.8
Nov 27, 2020 21:44:34.534538984 CET	53	61522	8.8.8.8	192.168.2.4
Nov 27, 2020 21:44:35.613050938 CET	52337	53	192.168.2.4	8.8.8.8
Nov 27, 2020 21:44:35.640363932 CET	53	52337	8.8.8.8	192.168.2.4
Nov 27, 2020 21:44:37.393728018 CET	55046	53	192.168.2.4	8.8.8.8
Nov 27, 2020 21:44:37.420867920 CET	53	55046	8.8.8.8	192.168.2.4
Nov 27, 2020 21:44:48.095825911 CET	49612	53	192.168.2.4	8.8.8.8
Nov 27, 2020 21:44:48.122984886 CET	53	49612	8.8.8.8	192.168.2.4
Nov 27, 2020 21:44:57.594000101 CET	49285	53	192.168.2.4	8.8.8.8
Nov 27, 2020 21:44:57.629358053 CET	53	49285	8.8.8.8	192.168.2.4
Nov 27, 2020 21:44:58.288794994 CET	50601	53	192.168.2.4	8.8.8.8
Nov 27, 2020 21:44:58.324775934 CET	53	50601	8.8.8.8	192.168.2.4
Nov 27, 2020 21:44:58.901660919 CET	49285	53	192.168.2.4	8.8.8.8
Nov 27, 2020 21:44:58.937349081 CET	53	49285	8.8.8.8	192.168.2.4
Nov 27, 2020 21:44:59.303368092 CET	50601	53	192.168.2.4	8.8.8.8
Nov 27, 2020 21:44:59.339160919 CET	53	50601	8.8.8.8	192.168.2.4
Nov 27, 2020 21:44:59.938147068 CET	49285	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 21:44:59.973670959 CET	53	49285	8.8.8.8	192.168.2.4
Nov 27, 2020 21:45:00.303601027 CET	50601	53	192.168.2.4	8.8.8.8
Nov 27, 2020 21:45:00.330765963 CET	53	50601	8.8.8.8	192.168.2.4
Nov 27, 2020 21:45:01.964128017 CET	49285	53	192.168.2.4	8.8.8.8
Nov 27, 2020 21:45:01.999398947 CET	53	49285	8.8.8.8	192.168.2.4
Nov 27, 2020 21:45:02.320821047 CET	50601	53	192.168.2.4	8.8.8.8
Nov 27, 2020 21:45:02.356447935 CET	53	50601	8.8.8.8	192.168.2.4
Nov 27, 2020 21:45:06.335321903 CET	50601	53	192.168.2.4	8.8.8.8
Nov 27, 2020 21:45:06.358910084 CET	49285	53	192.168.2.4	8.8.8.8
Nov 27, 2020 21:45:06.362626076 CET	53	50601	8.8.8.8	192.168.2.4
Nov 27, 2020 21:45:06.394789934 CET	53	49285	8.8.8.8	192.168.2.4
Nov 27, 2020 21:45:08.658987045 CET	60875	53	192.168.2.4	8.8.8.8
Nov 27, 2020 21:45:08.716712952 CET	53	60875	8.8.8.8	192.168.2.4
Nov 27, 2020 21:45:09.173458099 CET	56448	53	192.168.2.4	8.8.8.8
Nov 27, 2020 21:45:09.208954096 CET	53	56448	8.8.8.8	192.168.2.4
Nov 27, 2020 21:45:09.613929987 CET	59172	53	192.168.2.4	8.8.8.8
Nov 27, 2020 21:45:09.683044910 CET	53	59172	8.8.8.8	192.168.2.4
Nov 27, 2020 21:45:09.955521107 CET	62420	53	192.168.2.4	8.8.8.8
Nov 27, 2020 21:45:09.991105080 CET	53	62420	8.8.8.8	192.168.2.4
Nov 27, 2020 21:45:10.282727957 CET	60579	53	192.168.2.4	8.8.8.8
Nov 27, 2020 21:45:10.320560932 CET	53	60579	8.8.8.8	192.168.2.4
Nov 27, 2020 21:45:10.697557926 CET	50183	53	192.168.2.4	8.8.8.8
Nov 27, 2020 21:45:10.733212948 CET	53	50183	8.8.8.8	192.168.2.4
Nov 27, 2020 21:45:10.813157082 CET	61531	53	192.168.2.4	8.8.8.8
Nov 27, 2020 21:45:10.856971025 CET	53	61531	8.8.8.8	192.168.2.4
Nov 27, 2020 21:45:11.136790991 CET	49228	53	192.168.2.4	8.8.8.8
Nov 27, 2020 21:45:11.174238920 CET	53	49228	8.8.8.8	192.168.2.4
Nov 27, 2020 21:45:11.744468927 CET	59794	53	192.168.2.4	8.8.8.8
Nov 27, 2020 21:45:11.780534029 CET	53	59794	8.8.8.8	192.168.2.4
Nov 27, 2020 21:45:11.837768078 CET	55916	53	192.168.2.4	8.8.8.8
Nov 27, 2020 21:45:11.864813089 CET	53	55916	8.8.8.8	192.168.2.4
Nov 27, 2020 21:45:12.616653919 CET	52752	53	192.168.2.4	8.8.8.8
Nov 27, 2020 21:45:12.652565956 CET	53	52752	8.8.8.8	192.168.2.4
Nov 27, 2020 21:45:12.942754984 CET	60542	53	192.168.2.4	8.8.8.8
Nov 27, 2020 21:45:12.978254080 CET	53	60542	8.8.8.8	192.168.2.4
Nov 27, 2020 21:45:26.179752111 CET	60689	53	192.168.2.4	8.8.8.8
Nov 27, 2020 21:45:26.216738939 CET	53	60689	8.8.8.8	192.168.2.4
Nov 27, 2020 21:45:59.195632935 CET	64206	53	192.168.2.4	8.8.8.8
Nov 27, 2020 21:45:59.222784996 CET	53	64206	8.8.8.8	192.168.2.4
Nov 27, 2020 21:46:00.891171932 CET	50904	53	192.168.2.4	8.8.8.8
Nov 27, 2020 21:46:00.927114964 CET	53	50904	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 27, 2020 21:44:28.928242922 CET	192.168.2.4	8.8.8.8	0x336	Standard query (0)	i.ibb.co	A (IP address)	IN (0x0001)
Nov 27, 2020 21:44:28.935795069 CET	192.168.2.4	8.8.8.8	0xe01c	Standard query (0)	mayhutsuah anoi.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 27, 2020 21:44:28.974812031 CET	8.8.8.8	192.168.2.4	0xe01c	No error (0)	mayhutsuah anoi.com		103.221.222.30	A (IP address)	IN (0x0001)
Nov 27, 2020 21:44:29.115983009 CET	8.8.8.8	192.168.2.4	0x336	No error (0)	i.ibb.co		145.239.131.60	A (IP address)	IN (0x0001)
Nov 27, 2020 21:44:29.115983009 CET	8.8.8.8	192.168.2.4	0x336	No error (0)	i.ibb.co		145.239.131.51	A (IP address)	IN (0x0001)
Nov 27, 2020 21:44:29.115983009 CET	8.8.8.8	192.168.2.4	0x336	No error (0)	i.ibb.co		145.239.131.55	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
Nov 27, 2020 21:44:29.175302982 CET	145.239.131.60	443	192.168.2.4	49740	CN=ibb.co CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Fri Oct 02 08:53:44 CEST 2020 Thu Mar 17 17:40:46 CET 2016	Thu Dec 31 07:53:44 CET 2020 Wed Mar 17 17:40:46 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 17 17:40:46 CET 2016	Wed Mar 17 17:40:46 CET 2021		
Nov 27, 2020 21:44:29.183963060 CET	145.239.131.60	443	192.168.2.4	49741	CN=ibb.co CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Fri Oct 02 08:53:44 CEST 2020 Thu Mar 17 17:40:46 CET 2016	Thu Dec 31 07:53:44 CET 2020 Wed Mar 17 17:40:46 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 17 17:40:46 CET 2016	Wed Mar 17 17:40:46 CET 2021		
Nov 27, 2020 21:44:29.395201921 CET	103.221.222.30	443	192.168.2.4	49738	CN=mayhutsuahanoi.com CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Mon Oct 19 21:26:59 CEST 2020 Thu Mar 17 17:40:46 CET 2016	Sun Jan 17 20:26:59 CET 2021 Wed Mar 17 17:40:46 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 17 17:40:46 CET 2016	Wed Mar 17 17:40:46 CET 2021		
Nov 27, 2020 21:44:29.395881891 CET	103.221.222.30	443	192.168.2.4	49739	CN=mayhutsuahanoi.com CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Mon Oct 19 21:26:59 CEST 2020 Thu Mar 17 17:40:46 CET 2016	Sun Jan 17 20:26:59 CET 2021 Wed Mar 17 17:40:46 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 17 17:40:46 CET 2016	Wed Mar 17 17:40:46 CET 2021		

Code Manipulations

Statistics

Behavior

● iexplore.exe
● iexplore.exe

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 6944 Parent PID: 800

General

Start time:	21:44:26
Start date:	27/11/2020
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff6e5fd0000
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: 6992 Parent PID: 6944

General

Start time:	21:44:27

Start date:	27/11/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6944 CREDAT:17410 /prefetch:2
Imagebase:	0xb10000
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