

ID: 321119
Sample Name:
AccountStatements.html
Cookbook:
defaultwindowshtmlcookbook.jbs
Time: 11:24:35
Date: 20/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

Table of Contents 2
Analysis Report AccountStatements.html 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Yara Overview 4
Initial Sample 4
Sigma Overview 4
Signature Overview 4
Phishing: 5
Mitre Att&ck Matrix 5
Behavior Graph 5
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 7
URLs 7
Domains and IPs 8
Contacted Domains 8
Contacted URLs 8
URLs from Memory and Binaries 8
Contacted IPs 9
Public 9
General Information 9
Simulations 10
Behavior and APIs 10
Joe Sandbox View / Context 10
IPs 10
Domains 10
ASN 11
JA3 Fingerprints 11
Dropped Files 12
Created / dropped Files 12
Static File Info 18
General 18
Network Behavior 19
Network Port Distribution 19
TCP Packets 19
UDP Packets 21
DNS Queries 22
DNS Answers 22
HTTPS Packets 23
Code Manipulations 23
Statistics 23
Behavior 24
System Behavior 24
Analysis Process: iexplore.exe PID: 5276 Parent PID: 792 24
General 24

File Activities 24
Registry Activities 24
Analysis Process: iexplore.exe PID: 5600 Parent PID: 5276 25
General 25
File Activities 25
Registry Activities 25
Disassembly 25

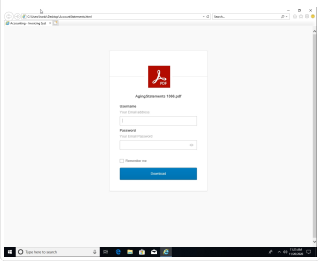
Analysis Report AccountStatements.html

Overview

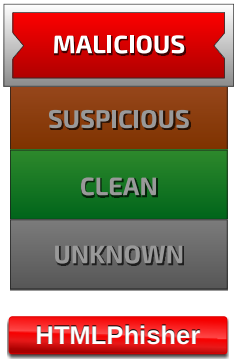
General Information

Sample Name:	AccountStatements.html
Analysis ID:	321119
MD5:	c7f8f17bcf5d265…
SHA1:	4e2bf200592a580.
SHA256:	9df63134e160a49.

Most interesting Screenshot:



Detection

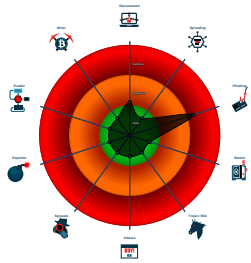


Score:	48
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected HtmlPhish_10
- HTML body contains low number of …
- HTML title does not match URL
- JA3 SSL client fingerprint seen in co…
- None HTTPS page querying sensitiv…
- Suspicious form URL found

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 5276 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5600 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5276 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

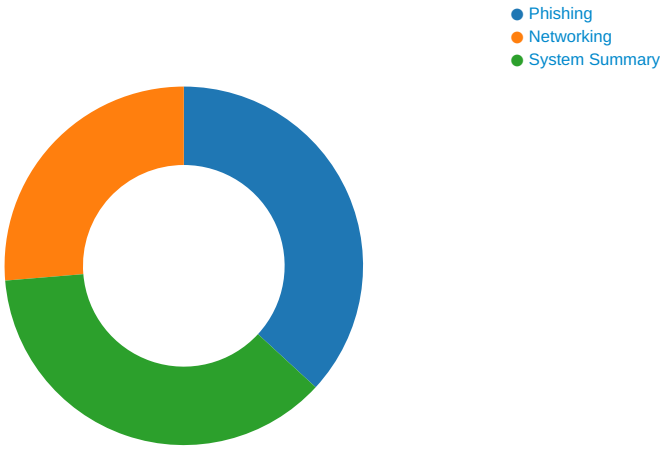
Initial Sample

Source	Rule	Description	Author	Strings
AccountStatements.html	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

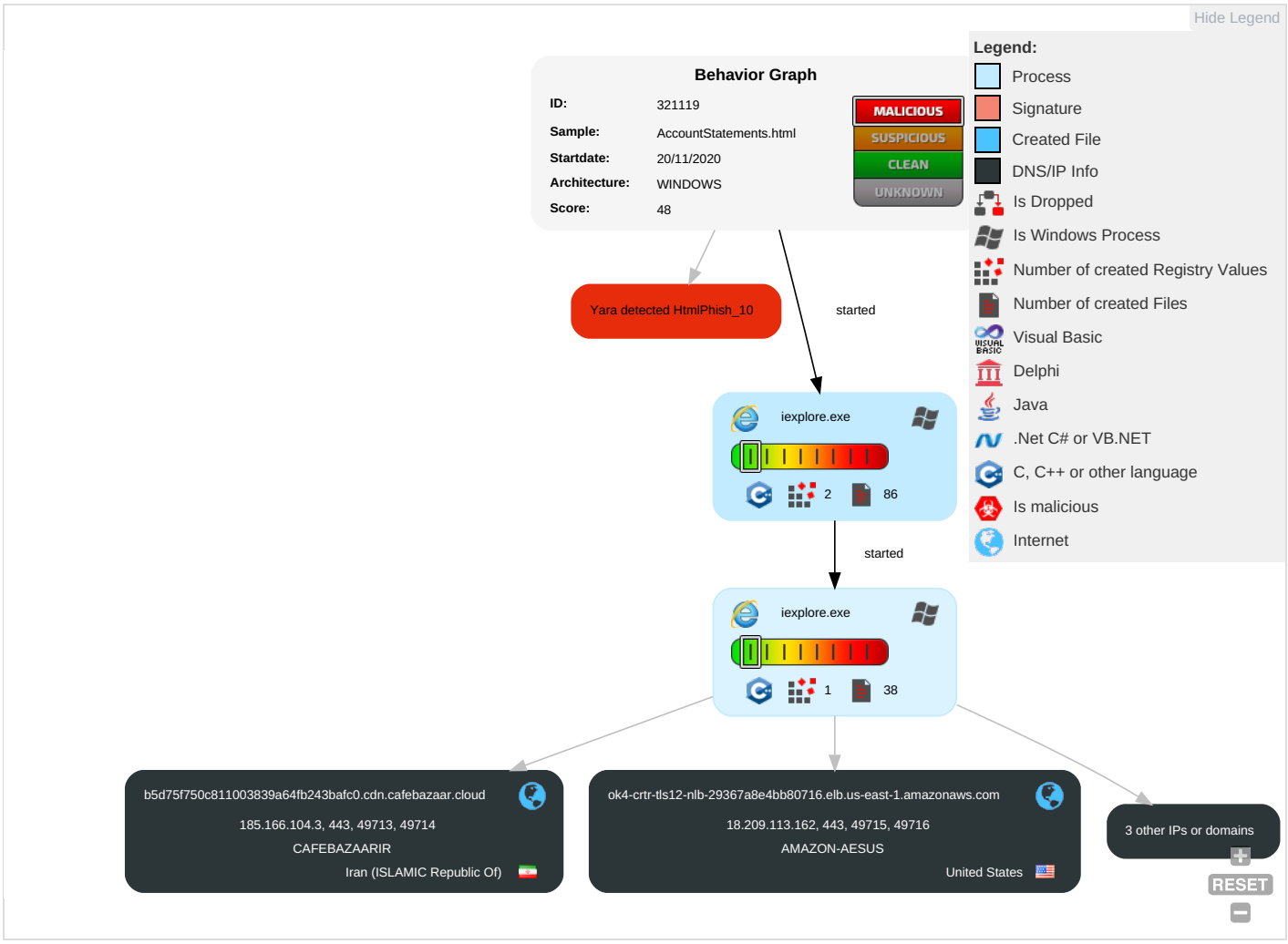
Phishing:

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

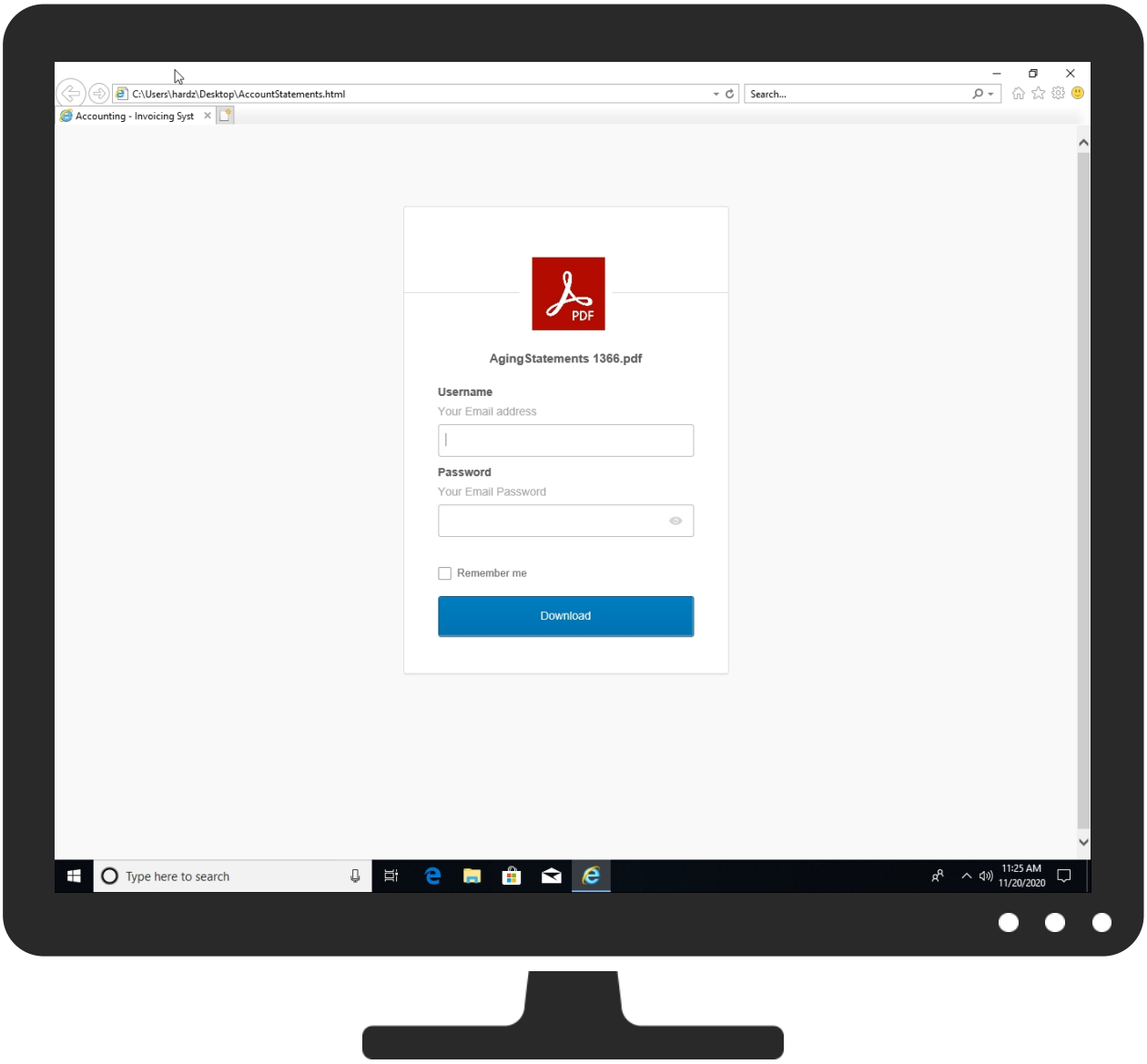


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
b5d75f750c811003839a64fb243bafc0.cdn.cafebazaar.cloud	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://typingdna.com	0%	Virustotal		Browse
http://typingdna.com	0%	Avira URL Cloud	safe	
http://https://coco-fleur.net/hell/oracle.php	0%	Avira URL Cloud	safe	
http://https://api.typingdna.com/scripts/typingdna.js	0%	Avira URL Cloud	safe	

Copyright null 2020

Source	Detection	Scanner	Label	Link
http://https://typingdna.com/scripts/typingdna.js	0%	Avira URL Cloud	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
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
ok4-crtr-tls12-nlb-29367a8e4bb80716.elb.us-east-1.amazonaws.com	18.209.113.162	true	false		high
b5d75f750c811003839a64fb243bafc0.cdn.cafebazaar.cloud	185.166.104.3	true	false	• 0%, Virustotal, Browse	unknown
s.cafebazaar.ir	unknown	unknown	false		high
atcocorp.okta.com	unknown	unknown	false		high

Contacted URLs

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

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://typingdna.com	initLoginPage.pack.34c59a55bb3a42c88a91a86c33d95ad4[1].js.3.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	initLoginPage.pack.34c59a55bb3a42c88a91a86c33d95ad4[1].js.3.dr	false		high
http://www.nytimes.com/	msapplication.xml3.2.dr	false		high
http://jquery.org/license	initLoginPage.pack.34c59a55bb3a42c88a91a86c33d95ad4[1].js.3.dr	false		high
http://sizzlejs.com/	initLoginPage.pack.34c59a55bb3a42c88a91a86c33d95ad4[1].js.3.dr	false		high
http://https://s.cafebazaar.ir/1/icons/com.adobe.reader_512x512.png	AccountStatements.html	false		high
http://www.amazon.com/	msapplication.xml.2.dr	false		high
http://www.apache.org/licenses/LICENSE-2.0.	initLoginPage.pack.34c59a55bb3a42c88a91a86c33d95ad4[1].js.3.dr	false		high
http://www.twitter.com/	msapplication.xml5.2.dr	false		high
http://github.com/kriskowal/q/raw/master/LICENSE	initLoginPage.pack.34c59a55bb3a42c88a91a86c33d95ad4[1].js.3.dr	false		high
http://https://coco-fleur.net/hell/oracle.php	AccountStatements.html	false	• Avira URL Cloud: safe	unknown
http://www.opensource.org/licenses/mit-license.html	initLoginPage.pack.34c59a55bb3a42c88a91a86c33d95ad4[1].js.3.dr	false		high
http://https://github.com/gabceb/jquery-browser-plugin	initLoginPage.pack.34c59a55bb3a42c88a91a86c33d95ad4[1].js.3.dr	false		high
http://https://support.okta.com/help/articles/Knowledge_Article/24532952-Platforms---Browser-and-OS-Support	AccountStatements.html	false		high
http://www.youtube.com/	msapplication.xml7.2.dr	false		high
http://https://github.com/gabceb	initLoginPage.pack.34c59a55bb3a42c88a91a86c33d95ad4[1].js.3.dr	false		high
http://https://api.typingdna.com/scripts/typingdna.js	initLoginPage.pack.34c59a55bb3a42c88a91a86c33d95ad4[1].js.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://atcocorp.okta.com/assets/loginpage/css/okta-login-page.min.0f4b9922bfa70975cc884fea7cbd71fa.	AccountStatements.html	false		high
http://https://typingdna.com/scripts/typingdna.js	initLoginPage.pack.34c59a55bb3a42c88a91a86c33d95ad4[1].js.3.dr	false	• Avira URL Cloud: safe	unknown
http://www.wikipedia.com/	msapplication.xml6.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://atcocorp.okta.com/assets/js/mvc/loginpage/initLoginPage.pack.34c59a55bb3a42c88a91a86c33d95ad	AccountStatements.html	false		high
http://https://github.com/js-cookie/js-cookie	initLoginPage.pack.34c59a55bb3a42c88a91a86c33d95ad4[1].js.3.dr	false		high
http://www.live.com/	msapplication.xml2.2.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.reddit.com/	msapplication.xml4.2.dr	false		high
http://jquery.com/	initLoginPage.pack.34c59a55bb3a42c88a91a86c33d95ad4[1].js.3.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.166.104.3	unknown	Iran (ISLAMIC Republic Of)		202319	CAFEBAZAARIR	false
18.209.113.162	unknown	United States		14618	AMAZON-AESUS	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	321119
Start date:	20.11.2020
Start time:	11:24:35
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 5s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	AccountStatements.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:	26
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

Copyright null 2020

Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal48.phis.winHTML@3/20@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, MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 52.255.188.83, 168.61.161.212, 104.108.39.131, 51.104.139.180, 23.210.248.85, 152.199.19.161, 52.155.217.156, 20.54.26.129, 95.101.22.134, 95.101.22.125, 51.104.144.132 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.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, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, fs.microsoft.com, ie9comview.vo.msecnd.net, db3p-ris-pf-prod-atm.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ris.api.iris.microsoft.com, umwatsonrouting.trafficmanager.net, skypedataprdcoleus17.cloudapp.net, go.microsoft.com.edgekey.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
185.166.104.3	202010074 - AccountStatements502 - Holt.html	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
b5d75f750c811003839a64fb243bafc0.cdn.cafebazaar.cloud	202010074 - AccountStatements502 - Holt.html	Get hash	malicious	Browse	• 185.166.104.3

Copyright null 2020

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ok4-crtr-tls12-nlb-29367a8e4bb80716.elb.us-east-1.amazonaws.com	202010074 - AccountStatements502 - Holt.html	Get hash	malicious	Browse	• 18.209.113.161

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CAFEBAZAARIR	202010074 - AccountStatements502 - Holt.html	Get hash	malicious	Browse	• 185.166.104.3
AMAZON-AESUS	a7UZzCVWKO.exe	Get hash	malicious	Browse	• 54.204.14.42
	QKLQkaCe9M.exe	Get hash	malicious	Browse	• 50.19.252.36
	sAPuJAvs52.exe	Get hash	malicious	Browse	• 54.243.161.145
	JlgyVmPWZr.exe	Get hash	malicious	Browse	• 174.129.214.20
	EIUOzWW2JX.exe	Get hash	malicious	Browse	• 174.129.214.20
	RVAgYSH2qh.exe	Get hash	malicious	Browse	• 54.235.142.93
	yCyc4rN0u8.exe	Get hash	malicious	Browse	• 54.235.83.248
	9cXAnovmQX.exe	Get hash	malicious	Browse	• 54.225.66.103
	T2HDck1Mmy.exe	Get hash	malicious	Browse	• 54.235.142.93
	Purchase Order 40,7045$.exe	Get hash	malicious	Browse	• 52.71.133.130
	Payment Advice Note from 19.11.2020.exe	Get hash	malicious	Browse	• 23.21.126.66
	phy__1__31629__2649094674__1605642612.exe	Get hash	malicious	Browse	• 23.21.126.66
	BBVA confirming Aviso de pago Eur5780201120.exe	Get hash	malicious	Browse	• 50.19.252.36
	Ejgvvuwuu8.exe	Get hash	malicious	Browse	• 54.225.169.28
	PO N0.1500243224._PDF.exe	Get hash	malicious	Browse	• 54.204.14.42
	Avion Quotation Request.doc	Get hash	malicious	Browse	• 54.204.14.42
	zRHI9DJ0YKlPfBX.exe	Get hash	malicious	Browse	• 54.235.182.194
	{REQUEST FOR QUOTATION-local lot.1,2,3,4,6container..exe	Get hash	malicious	Browse	• 174.129.214.20
	chib(1).exe	Get hash	malicious	Browse	• 54.225.153.147
	dede.exe	Get hash	malicious	Browse	• 184.73.247.141

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
9e10692f1b7f78228b2d4e424db3a98c	http://banchio.com/common/imgbrowser/update/index.php	Get hash	malicious	Browse	• 185.166.104.3 • 18.209.113.162
	robertophotopng.dll	Get hash	malicious	Browse	• 185.166.104.3 • 18.209.113.162
	http://https://u19114248.ct.sendgrid.net/ls/click?upn=1kMFt-2Foese19BdzKqBBNxmUiDNiO3l4ozyKR3JHYHjGXyXtR1YgfLizwybC7hwFoy4wlb-2FUZczInc9Ssmzz4dQ-3D-3DuU6r_TCf26aIMQHFUMJSqtVnzlcWBqfQpkiFxCOBj9heiSevnqRkiapxQjkatt3r5u5xw-2FNDgXhA220pIRwcKmyMneET98pBkuhL-2FUwJCaSrvE5mZhnMBtJdZf9Opljklq5t7Y-2BINqElPlJU8bjYLY27qV6L-2FSwA36husfmMqwKagSwOgE04FdniEmY9uEbym50XNhqKw9lgczv6HrSrYNm6ouXnIayW-2FSBLzGYxoTYKe6OA-3D	Get hash	malicious	Browse	• 185.166.104.3 • 18.209.113.162
	http://https://rugbysacele.ro/zz/IK/of1/nhctfwp4x278qkbusvijl6z39y5ema1o0gdr597irqhw4x0fk3uevzlaoj12bdmpsnt8g6yce40h6iv7bprsowxd3z2nmu8kal5gcj1yf9qt?data=dmluY2VudC5kdXNvcmRldEBpbWQub3Jn#aHR0cHM6Ly9ydWdieXNhY2VsZS5yby96ei9JSy9vZjEvNDUzMjY3NzY4JmVtYWlsPXZpbmNlbnQuZHVzb3JkZXRAaW1kLm9yZw==	Get hash	malicious	Browse	• 185.166.104.3 • 18.209.113.162
	noosbt.dll	Get hash	malicious	Browse	• 185.166.104.3 • 18.209.113.162
	temp.dll	Get hash	malicious	Browse	• 185.166.104.3 • 18.209.113.162
	http://https://verify-outlook-web.weebly.com/	Get hash	malicious	Browse	• 185.166.104.3 • 18.209.113.162
	http://https://filmconsultancy.bindwall.ml/mike@filmconsultancy.com	Get hash	malicious	Browse	• 185.166.104.3 • 18.209.113.162
	http://https://trondiamond.co/OMMOM/OM9u8	Get hash	malicious	Browse	• 185.166.104.3 • 18.209.113.162
	http://https://smartdevappoffic.azurewebsites.net/qeBM8A4A6/WuZ2Y/FAjZdg5Nrw/@t1~RGCy/wefxc.php?bbre=d6266420d5a57cc3d73bcb5a9ec80cde	Get hash	malicious	Browse	• 185.166.104.3 • 18.209.113.162
	http://flossdental.com.au	Get hash	malicious	Browse	• 185.166.104.3 • 18.209.113.162

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://t.e.vailresorts.com/r/?id=h1bac782d,59eb410,55e61f1&VRI_v73=96008558&cmpid=EML_OPENDAYS_RESO_000_OK_SR_REN1Y_000000_TG0001_20201118_V00_EX001_LOCA_ANN_00000_000	Get hash	malicious	Browse	• 185.166.104.3 • 18.209.113.162
	http://https://www.canva.com/design/DAEN9RlD8Vk/acBvt6UoL-DafjXmQk38pA/view?utm_content=DAEN9RlD8Vk&utm_campaign=designshare&utm_medium=link&utm_source=publishsharelink	Get hash	malicious	Browse	• 185.166.104.3 • 18.209.113.162
	http://https://app.box.com/s/mk1t9s05ty9ba7rvsdbstgc46rb4fod7	Get hash	malicious	Browse	• 185.166.104.3 • 18.209.113.162
	http://https://bit.ly/2UDM1To	Get hash	malicious	Browse	• 185.166.104.3 • 18.209.113.162
	http://https://gazeta-echo.ru/wp-includes/assets/<>/?mail=tfagot@dupaco.com	Get hash	malicious	Browse	• 185.166.104.3 • 18.209.113.162
	http://https://t.e.vailresorts.com/r/?id=hda0e43a,3501a2a,3501f68&VRI_v73=Y25veWVzQDk5cmVzdGF1cmFudHMuY29t&cmpid=EML_SNOWALRT_OTHR_000_NW_00_00000_000000_000000_20200110_v01&p1=www.snow.com%40h-is.xyz	Get hash	malicious	Browse	• 185.166.104.3 • 18.209.113.162
	http://https://go.pardot.com/e/395202/siness-insights-dashboard-html/bnmpz6/1446733421?h=AwLDfNsCVbkjEN13pzY-7AXMPolL_XMigGsJSppGaiM	Get hash	malicious	Browse	• 185.166.104.3 • 18.209.113.162
	http://https://app.box.com/s/gdf36roak3w2fc52cgfbxuq651p0zehy	Get hash	malicious	Browse	• 185.166.104.3 • 18.209.113.162
	http://revitoped.blogspot.com/2013/11/view-reference-and-camera-location.html	Get hash	malicious	Browse	• 185.166.104.3 • 18.209.113.162

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{240BA7A7-2B66-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8532451737308064
Encrypted:	false
SSDEEP:	96:rrZwZK239WjLtjEfjSRMjkjqWjlDfjncX:rrZwZK239WXtgf2RMYGWNfrcX
MD5:	A42D1E5E4A60A9C5A03B4EFCDF3B4E34
SHA1:	8FE049280A3DFEAD45FE80A7B9590EE742442B41
SHA-256:	D31DE5CA76DC4976281A841BD424D7554AAEFB9DEBCBB23BAE9D09229AE94E86
SHA-512:	54FDC3224FD96A0F16216EB00BD7388E4B61CBF7A8406A5C1C0B4A88EDFC8A0C26A601C3B74EA5D665688366F09E4D72C87EE3BA3B2FD2E342969995ECFEF1AF
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\{240BA7A9-2B66-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28528
Entropy (8bit):	1.9520189365903498
Encrypted:	false
SSDEEP:	192:r2ZZQ56rkkFj52skW/MCYjIlw3kN7MKM/MPdr:ry+UwkhIY0CmmqkdMKM/Mh
MD5:	9DC4BCB7081235C9F392632AF3328D8A
SHA1:	1E4F3BCEC8B61CA9B96CD3B2B353C74B834C7887
SHA-256:	515F8BEE87E447D33ECC47190817EBD92F31E71F41F14BCCE8315F63C1333FDB
SHA-512:	677BE03939B9E85B66B441894EA233A5AD5CC1DB52CAE54BA6964AFAA738ADF7AAE4864DF6DAC8444762F5343C9A8E41E79F619651151F45B773599B99504F0A
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{240BA7A9-2B66-11EB-90E4-ECF4BB862DED}.dat	
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{240BA7AA-2B66-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5661919409841059
Encrypted:	false
SSDEEP:	48:IwLhGcprcGwpaPhG4pQNGrapbS+rGQpK8G7HpR+sTGIpG:rLXZUQPz6tBS+FAXT+4A
MD5:	0B9204BA6C10D023DE82A0116857495F
SHA1:	94D560B69AA4D5947F9575F7808400AE62A9E454
SHA-256:	F1C89F71B4893ED26FBBD6CED7ED8BE927F2F1F337E410F4F50AF6045EC166B5
SHA-512:	579761F4C92E9CBAA09AB81F494686E4ED074A2590A52BEEC19613DEA975210E7A13253BFDC912E71D067942B13E078C2B84520AEB9ADC8B574476166655B121
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):	5.078671325225144
Encrypted:	false
SSDEEP:	12:TMHdNMNxOE97JnWimI002EtM3MHdNMNxOE97JnWimI00ObVbkEtMb:2d6NxOC7JSZHKd6NxOC7JSZ76b
MD5:	509B5AFDEC4575A80FB651C480FD1960
SHA1:	E3F12DE55EFA0997C479032F6A1B68590BBE6AE8
SHA-256:	F4A734ACA3A92414AB7BDD983FE14985C2928214057CFEB02C1340BA409764FE
SHA-512:	C867892785B2F7A838A8C1799CB632E0FAC255D0A3DD82FA98C51CAA5AEBFCC99019A5913BAAF45D155F88CB6131D2774B969248275A6D28B59E891F30B881B
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0xfa081cf7,0x01d6bf72</date><accdate>0xfa081cf7,0x01d6bf72</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>0xfa081cf7,0x01d6bf72</date><accdate>0xfa081cf7,0x01d6bf72</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
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.105189522036577
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2k9pZpfnWimI002EtM3MHdNMNxe2k9pZpfnWimI00Obkak6EtMb:2d6NxriHtSZHKd6NxriHtSZ7Aa7b
MD5:	165A6763696C451283AAFA2AD57CF562
SHA1:	3DAE3ECAF255F0268F2209353988085F6F921147
SHA-256:	88CC97B0A8BBA3DE16E596B715AA7B57D34E3B6294A89A6B5BE1F68FB967D2BA
SHA-512:	CE0E780A2E95BC5B28BA979CBD82915D65D7705DE4D6C53B7513FA04E0DFB75BECEBF0CA7D373ACFF7517DB5B8F8E41E716CBDE03F51ECE91C888CCB1C039B5A
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0xfa00f609,0x01d6bf72</date><accdate>0xfa00f609,0x01d6bf72</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>0xfa00f609,0x01d6bf72</date><accdate>0xfa00f609,0x01d6bf72</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):	5.097958599172493
Encrypted:	false
SSDEEP:	12:TMHdNMNxvL97JnWimI002EtM3MHdNMNxvL97JnWimI00ObmZEtMb:2d6NxvB7JSZHKd6NxvB7JSZ7mb
MD5:	F95EFECFB6972F371E18ABD1B9FD5330
SHA1:	D84EE22535D82164EDBF4AB82F9DCDB42C523167
SHA-256:	57376A3E17C604C67B0A45434FC9222A2B8CF4101F5D7D92A26146DD421AA0C7
SHA-512:	D604BDEB7DB1006DD878632F775BFE4AC74CDA180EFB0E210634C8DD9EFA5D77B41C327578F9DDB16255DD5C0A1917F0A2F35575F356800C427034EF0A80BF2
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0xfa081cf7,0x01d6bf72</date><accdate>0xfa081cf7,0x01d6bf72</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>0xfa081cf7,0x01d6bf72</date><accdate>0xfa081cf7,0x01d6bf72</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):	5.114492169218139
Encrypted:	false
SSDEEP:	12:TMHdNMNxi93BS3BmnWimI002EtM3MHdNMNxi93BS3BmnWimI00Obd5EtMb:2d6Nx4xSxmSZHKd6Nx4xSxmSZ7Jjb
MD5:	DD9A7368BD744B094D7251327C60B0AE
SHA1:	E3499593A9D39CF532B4B03CB83AB4A8DEDE9096
SHA-256:	299CFA27E964E6F620D4591CDDE7792A658B08C4E447A2DC164C2A6F60D79636
SHA-512:	8DC9113FA5083D0378E8FDF1D5408A637AE33DC87CA7C72043AF426A53CBD2749044AEC32D6082668444O2CBEBE30C7A0D165432C7B2A9A94BDF13896100216
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0xfa05ba88,0x01d6bf72</date><accdate>0xfa05ba88,0x01d6bf72</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>0xfa05ba88,0x01d6bf72</date><accdate>0xfa05ba88,0x01d6bf72</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):	5.104070059744012
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGw9DBnWimI002EtM3MHdNMNxhGw9DBnWimI00Ob8K075EtMb:2d6NxQuDBSZHKd6NxQuDBSZ7YKajb
MD5:	EB5DBC3C8954DD8971EF81A7E6FA37AE
SHA1:	77EDCDEDE5B3093C1D560876AE86099C43A56527
SHA-256:	FD73939D0D5E847411EB14FBF603C3A07A07AF1F55946A7C2E18FDD115412BC7
SHA-512:	0CA42F450DB43C6060BF5E006DCBAE9092A96E5AADCB43B7DF33C6E90A2B9626C5CEF39C4FB8D92EAF3B0DE6201D9F2635298083B88FA679A2E3FE3EAE02219
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0xfa0a7f3b,0x01d6bf72</date><accdate>0xfa0a7f3b,0x01d6bf72</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>0xfa0a7f3b,0x01d6bf72</date><accdate>0xfa0a7f3b,0x01d6bf72</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

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml	
Entropy (8bit):	5.081770144833602
Encrypted:	false
SSDEEP:	12:TMHdNMNx0n97JnWimI002EtM3MHdNMNx0n97JnWimI00ObxEtMb:2d6Nx097JSZHKd6Nx097JSZ7nb
MD5:	2CE25666A3F18C66E85A7470CC9FB711
SHA1:	451C57D3B0440F2138ADA7E12105F477E87EDC90
SHA-256:	2D50BADE6C790D8190155490C94E1ACDFC5E27A7FABE1E89505C2B8C87984C48
SHA-512:	12AB5218D978C2F933466AC9FC33DC5DD0D723FE7F18820CC1CCBDAC3A94393F2233CF6FDB542EA9D6FA120FFB77BACE7F146F621367787CDC523F7D1B2765 4
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0xfa081cf7,0x01d6bf72</date><accdate>0xfa081cf7,0x01d6bf72</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>0xfa081cf7,0x01d6bf72</date><accdate>0xfa081cf7,0x01d6bf72</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):	5.139096559262096
Encrypted:	false
SSDEEP:	12:TMHdNMNxx93BS3BmnWimI002EtM3MHdNMNxx93BS3BmnWimI00Ob6Kq5EtMb:2d6NxHxSxmSZHKd6NxHxSxmSZ7ob
MD5:	F7487ECD5E4BFB0D64D9268FC329C5FC
SHA1:	2AD73573C44DD198047FA2CC3E9CC0BF1BF39FA3
SHA-256:	53D55DC18104DD6489616B797E1CE011E629977C4DB90BF0ABE4E2292E8387FD
SHA-512:	6C462084704FBACB973142EED7C3B57F2DEFC39FD8CAA742B4A1E94BC2DA91BB17A589B09216427836B5BDA99E3FFE5B9E58501B3900FBA483C194776B75B1D 4
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0xfa05ba88,0x01d6bf72</date><accdate>0xfa05ba88,0x01d6bf72</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>0xfa05ba88,0x01d6bf72</date><accdate>0xfa05ba88,0x01d6bf72</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):	5.1270089425174445
Encrypted:	false
SSDEEP:	12:TMHdNMNxc9V3VdnWimI002EtM3MHdNMNxc9V3VdnWimI00ObVEtMb:2d6Nx6RHSZHKd6Nx6RHSZ7Db
MD5:	431547C0ED45DA7E6D24E78EE7AB4317
SHA1:	AB4F991CF8FF7C13788A66F344BB5157DF71687F
SHA-256:	3F08F470A0153E8C2CA090F5533E5D523B8BB075659E00481E5E132B49D004ED
SHA-512:	843A2E48565FB645D095038884DA037EBCDCB83F7B9CA5331A55954AF1E90201D0B5615BDEB5EC2EAAFFD4667BF2F214CEF74C3732DC71167140045CEE8D417 E
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0xfa035836,0x01d6bf72</date><accdate>0xfa035836,0x01d6bf72</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>0xfa035836,0x01d6bf72</date><accdate>0xfa035836,0x01d6bf72</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):	5.113724603773544
Encrypted:	false
SSDEEP:	12:TMHdNMNxfn9V3VdnWimI002EtM3MHdNMNxfn9V3VdnWimI00Obe5EtMb:2d6Nx1RHSZHKd6Nx1RHSZ7ijb

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml	
MD5:	51B6D7B1861FA1FB9A2D172373665239
SHA1:	2190E2A3D214E52699BE6D30D8E3417BBE35EF55
SHA-256:	2249CF281AF3BF23CD6BADD854D33740B0C2D08CB022E0331626FCC8CF3D2D92
SHA-512:	B509CAA9797EB3F07C274A2B65B1A9678CC16DBF47E25AC812DD0A7D0818ACE901932CDEB64CC30C0D41B5BD2DBC086441C71F7CFB6F520096EF7CD76AF6ADFA
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0xfa035836,0x01d6bf72</date><accdate>0xfa035836,0x01d6bf72</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>0xfa035836,0x01d6bf72</date><accdate>0xfa035836,0x01d6bf72</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\0W10PBUV\initLoginPage.pack.34c59a55bb3a42c88a91a86c33d95ad4[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with LF, NEL line terminators
Category:	downloaded
Size (bytes):	1302343
Entropy (8bit):	5.3567221795887185
Encrypted:	false
SSDEEP:	12288:5od204HulThBScpfs0Dbr1YMn6WuELCw+43Z1mufX/4D:5odYOThUc9uEywVv4D
MD5:	34C59A55BB3A42C88A91A86C33D95AD4
SHA1:	4088F167420BAC4998CCB587D457E5C7FF2449A2
SHA-256:	B726C44EA8FADDDDE110ED14D066683B04AC08A783BC5222A61FD19C7E17F731
SHA-512:	5D91DA819E260BD3C7876B708CFEFC6F0BBAFD1634AABA4AF68B6211983E6072B2ACAD267574542DD62BCED694BF015DC079509E2A6743DF83FEAC14F55722AF
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://atcocorp.okta.com/assets/js/mvc/loginpage/initLoginPage.pack.34c59a55bb3a42c88a91a86c33d95ad4.js
Preview:	var OktaLogin=OktaLogin||{};OktaLogin.initLoginPage=function(modules){function __webpack_require__(moduleId){if(installedModules[moduleId])return installedModules[moduleId].exports;var module=installedModules[moduleId]={i:moduleId,l:!1,exports:{}};return modules[moduleId].call(module.exports,module,module.exports,__webpack_require__),module.l=!0,module.exports}var installedModules={};return __webpack_require__.m=modules,__webpack_require__.c=installedModules,__webpack_require__.d=function(exports,name,getter){__webpack_require__.o(exports,name)||Object.defineProperty(exports,name,{configurable:!1,enumerable:!0,get:getter})},__webpack_require__.n=function(module){var getter=module&&module.__esModule?function(){return module["default"]}:function(){return module};return __webpack_require__.d(getter,"a",getter),getter},__webpack_require__.o=function(object,property){return Object.prototype.hasOwnProperty.call(object,property)},__webpack_require__.p="",__webpack_require__(__webpack_require_

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\okta-login-page.min.0f4b9922bfa70975cc884fea7cbd71fa[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	186201
Entropy (8bit):	5.098866906305462
Encrypted:	false
SSDEEP:	1536:Qy4Hkt7MuW5ZBoZ5Yylrx8KfNhB0kLoFZxrrA0qWo:L4Et7MhBAVZBDLoF3q
MD5:	0F4B9922BFA70975CC884FEA7CBD71FA
SHA1:	7CBA770F43B261873D62ADCC13BDB54593D4962D
SHA-256:	911311420D6C570FBF9F376D1104B6F9153F20413348D78262BDA9D18E80E7F6
SHA-512:	6CCD726D62CCCFB4D517690D68413D6BDA69DF1C107E59942245E75359982D8168AD79749326782AF432E24A9956D7B73883DAB554576E3CA420CD74A2C0D48
Malicious:	false
IE Cache URL:	http://https://atcocorp.okta.com/assets/loginpage/css/okta-login-page.min.0f4b9922bfa70975cc884fea7cbd71fa.css
Preview:	.qtip{position:absolute;left:-28000px;top:-28000px;display:none;max-width:280px;min-width:50px;font-size:10.5px;line-height:12px;direction:ltr;box-shadow:none;padding:0}.qtip-content{padding:5px 9px;text-align:left;word-wrap:break-word}.qtip-content,.qtip-titlebar{position:relative;overflow:hidden}.qtip-titlebar{padding:5px 35px 5px 10px;border-width:0 0 1px;font-weight:700}.qtip-titlebar+.qtip-content{border-top-width:0!important}.qtip-close{position:absolute;right:-9px;top:-9px;z-index:11;cursor:pointer;outline:medium none;border:1px solid transparent}.qtip-titlebar .qtip-close{right:4px;top:50%;margin-top:-9px}* html .qtip-titlebar .qtip-close{top:16px}.qtip-icon .ui-icon,.qtip-titlebar .ui-icon{display:block;text-indent:-1000em;direction:ltr}.qtip-icon,.qtip-icon .ui-icon{border-radius:3px;text-decoration:none}.qtip-icon .ui-icon{width:18px;height:14px;line-height:14px;text-align:center;text-indent:0;font:normal 700 10px/13px Tahoma,sans-serif;color:inherit;background:transparent n

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\okticon.fe8b3f5e8c2e13114d5bfb04e4731fb9[1].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), okticon family
Category:	downloaded
Size (bytes):	38908
Entropy (8bit):	6.244851443695859
Encrypted:	false
SSDEEP:	768:eWlBkwOA1B5rvXpC99lbP80DLbffHoZiWzEmkMFqTw2QFrIzm:Mo1zrvZC/l7zLDfaiWzEm5qTwbJ
MD5:	FE8B3F5E8C2E13114D5BFB04E4731FB9

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\okticon.fe8b3f5e8c2e13114d5bfb04e4731fb9[1].eot	
SHA1:	1EF1599F613C58C4C76256895CB7F7254DFC8277
SHA-256:	DC03EE881DDF90986F148256F31CB2768EDE9AAFC884F9FC9CDAA72020439407
SHA-512:	64E90CC938AF7B250CE7306A0BBC55F8148FD9A58474F91A8560451E262A56F9F293D076148658F9653E0D1B6DF2F8A43DB45AB36CEDECF45762483AE30A4F1F
Malicious:	false
IE Cache URL:	http://https://atcocorp.okta.com/assets/loginpage/font/okticon.fe8b3f5e8c2e13114d5bfb04e4731fb9.eot?
Preview:	....X.....LP.....&0EZ.....o.k.t.i.c.o.n.....R.e.g.u.l.a.r.....V.e.r.s.i.o.n. .1...0.....o.k.t.i.c.o.n.....PFFTM{..0...<....GDEF..... OS /2/.MD...X...Vcmap.X.....`....gasp.....glyfC.....|.head..x.....6hhea.J.....$hmtx.w.....loca.G.Z...\....maxp.(.....8... name.t..... ....postA.!'.....o.....ZE0&_.<.....e30. ....e30.....@.....L.f...G.L.f.....PfEd.@..... . ..... .....@. .....2..... .....*.....!.....@...`.`.@. .....:.....]. ..... .p.@... ...@.@. . ..... . . . . .@. . . . . . . . .@. ...*.`. ... ...z.#. .....@. ...S...=. . .#. . . ... .%.%.....%.%.%..... .#.3...`.3...P..... . ...`.P..... ...-.D.....@.....].@. .`... . ...@.-.+...+. ... .3..... .@.`...@. . . . . .0... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\checkbox-sign-in-widget.7846b2f8c6d0a7ca69fdd3d3c294e92d[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 50 x 1155, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	3141
Entropy (8bit):	7.275615969527201
Encrypted:	false
SSDEEP:	48:9OeUaC6O7ChQy5GY7Pd32kzVtOUG34ie0r:9OlaC6O7ChQy99BqnDt
MD5:	7846B2F8C6D0A7CA69FDD3D3C294E92D
SHA1:	E0BB021FFDF93C68FEF44DE2A3B08F378B6FB50A
SHA-256:	40810B0318131F9BA52C83A17E633A0AC476ADE66EA8A914D6C4980571397665
SHA-512:	C08600B8B07D56BB502F9AED5CE2BAB59B33105C1CCF595413BC7158368FA06C73BC2D22C7CC99D1EFD10FD7C599CEE92163DEC3D2312BFD98DBF69457C59E7
Malicious:	false
IE Cache URL:	http://https://atcocorp.okta.com/assets/loginpage/img/ui/forms/checkbox-sign-in-widget.7846b2f8c6d0a7ca69fdd3d3c294e92d.png
Preview:	.PNG.....IHDR...2.....;.lr....IDATx..._l.....{..@.,.g.e.2...l$...p8...H.ndxS...7o.\..1.4\.z...%K.[.%U.0..8.0...S..c..=..p...-...ky$...1..;.s...#.....GQ.....mQ....z1.uq.W.$.c.?d}....z.(..[.l).J.T.....<B..z.T*.P(.....]i?.i.u.k..7..!..!n.q.9$.....h.....q5...2?4&I.c``.s?.g=.Z...I.$...2..I.F....7..!..!n.qC..B....7..!..!n.qC..B....7..!..!n.qC..B....7..!..!n.qC..B....7..!..!n.qC..B....7..!..!n.qC..B.\7!..+.o.-..r.VK5^....+<..(*.....S]744T.....j.....uww+.x5..o..7..!..!n.q.9$..W..<.....!..y.....,..A.A..7..!..!n.qC..B....7..!..!n.qC..B....7..!..!n.qC..B....7..!..!n.qC..B....7..!..!n.qC..B....7..!..!n.qC..B....7..+....EQT....+.8..A.Y...D.RI.T*I...D.....U.....+.JJ.)^..F..I=.....S'..{AC^8.Go...v.yM.....^..=#C.32.(.....5.=zAB>.pN/..#I.v.F.Y^.~F....0.$I._.S.6..e+.`..C.9#X.....~s./..M.....c.jQ..6..JM.....H.....}.==...ZRh.....$.....,n.u.,.B~..Mu-[...W.V...._..E7.b...+:.....S..yu...}....vl....--._..}..S.....k.-z.[?Vk.Y.X.}.-j.}.,..Z.....s.j.....d...:<<\,.f.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\com.adobe.reader_512x512[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 512 x 512, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	17087
Entropy (8bit):	7.772487297530517
Encrypted:	false
SSDEEP:	384:ibNB8CM90bp8VP20S2MwdoeCWs/EE/ucz0PFR:gBbQ0bp8VPgeoevs/EE2BtR
MD5:	E9FCE767A2C9639961C81D53B8E750E6
SHA1:	B0FEFF6AA36A8D744049AEEAC1CF81D4530F2AFF
SHA-256:	4894969469E1726DD161DC3C53D4064BC38696C31F77D8D5D961FA425F166A50
SHA-512:	2A56CFB616D30FD4FDECE3B9DCDC4019ECAB8BB606818F46DA358E26D70B4D31AB54F00240B9E1803459876D3EB3B81FFDCC5E1059B55C731B944E3FC873FCAB
Malicious:	false
IE Cache URL:	http://https://s.cafebazaar.ir/1/icons/com.adobe.reader_512x512.png
Preview:	.PNG.....IHDR.....x....B.IDATx...w\U....wH.Yd...VX..e...bE...W..*...k.j.....=..e.M.Av....d.....(;7...=.....p.....Q9.{f..H.....J=.....Q...p!.....D.....(.....B....\.....Q...p!.....D....(.....B....\.....Q...p!.....D....(.....B....\.....Q...p!.....D....(.....B....\.....Q...p!.....D....(.....B....\.....Q...p!.....D....(.....B....\.....Q...p!.....D....(.....B....\.....Q...p!.....D....(.....B....\.....Q...p!.....D....(.....B....\.....Q...p!.....D....(.....B....\.....Q...p!.....D....(.....B....\(.t..u.....P.....Z...U?>A...:..W.y.*..V...l..M.U..j.o.h::.....!..ZpD...{....XMF\....uZ.I.n.....OUQX`qR.....8\hL.Z.....:..Of..o....w.....(....._.....V.r.~...e.i.,..Q....k.L=..T.g....._|.....|6.....a.\4RCV.7..f.^.....t.(#.....p...`u|.I...K...?...8.....).....8.,.Q..9....{.

C:\Users\user\AppData\Local\Temp\~DF21C372744A71BF0C.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	36289
Entropy (8bit):	0.6340104213837845
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+Ks2/sTwzjkNzvMKM/MEA:kBqoxKAuqR+Ks2/sTw3kN7MKM/M
MD5:	C92B77A77F8C2CA4D99A69C138A0EFDF
SHA1:	9050CAB87A091009702BB38809A3B539B7AE698E
SHA-256:	894684A11C0344E8FEF79ADEA9742B5FC24E69BC73BE90D29F21D8E9BF9EF13F
SHA-512:	2BAC3EA3CF002402BD74AA3AED68AA8982669DB3D56BF2CB2D0D4D1113B79421D5D413037929A44315A6BD6C2706688BC2803BF1FE0FCF8B5B9FCB3E2F6213A

C:\Users\user\AppData\Local\Temp\~DF21C372744A71BF0C.TMP	
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF4287DA41F4BBBE37.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.47646882167839216
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loGrF9loGR9lWGoGSe+piSe+tAS+tqvive:kBqoIJfXJd3d6s
MD5:	C6258003DE1F0CDA75B07DCA21FC15E5
SHA1:	D9EF5245FB9DEACE7346297B814FFBA996648D8A
SHA-256:	2348A1B3DAADC23232AA545E4C17299B532D056AF16AFCD02C4C5208DCFAB4F3
SHA-512:	7FD05610A967423A60C8C0A5FC4C5CD61B9E19EC830885EB74C81A48C5FE1CF5CA687F8655BF378199127C827CA9A905D47D61FAF96463688CBAC912CD2C4A
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFD3AF8564A5B2005B.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.32141681506881803
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laAtbi:kBqoxxJhHWSVSEabtbi
MD5:	7CA5128708F5C068CF5A5DFDF0AADF59
SHA1:	00A75257A4EBAC9F54E2C1662CD79C288F5D56AB
SHA-256:	6CC9737E92127F9879581D10F115AF85102D3C7831A621C441999CB9299DF1EA
SHA-512:	84BA366015A6BCD8F82D931B6DBEDF07512A9F82F1F8B5B72E2013853B2E608B9C4EAAF9D825A676DD45FF1B70609C988D59B7BE8EA22B1898AB8A9F8A574DD 8
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

Static File Info

General

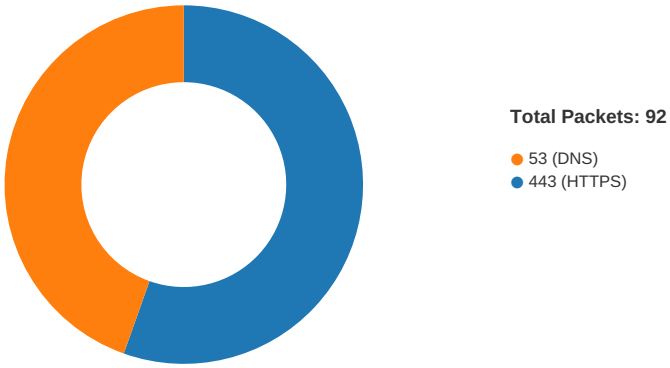
File type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Entropy (8bit):	4.944107906244486
TrID:	• HyperText Markup Language (12001/1) 18.75% • HyperText Markup Language (12001/1) 18.75% • HyperText Markup Language (11501/1) 17.97% • HyperText Markup Language (11501/1) 17.97% • HyperText Markup Language (11001/1) 17.19%
File name:	AccountStatements.html
File size:	8241
MD5:	c7f8f17bcf5d2656dd7f818969736342
SHA1:	4e2bf200592a5803b81eca7416ca514aae86188b
SHA256:	9df63134e160a49558a811b07b551c828dd733be30d970 ee5f4656a8e7006ff
SHA512:	1e5f18ad40d9b8626eb5301d5bdfe2852bc3fee4c750b3c 62eced4d26a142beab676ae27aff07303ca2bcead0f521a a3104d0011e8d565b5611cdf3ec82c4f16

General

SSDEEP:	192:Jr4Gmpts1IJlkTbJ2VrXxEKw3LibmY/7W:JsPzGr7hY/7W
File Content Preview:	<html> <![endif]--><head>.... <script>if (typeof module === 'object') {window.module = module; module = undefined;}</script>.... <title>Accounting - Invoicing System </title>.. <meta charset="UTF-8">.. <meta name="viewport" content="wid

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 11:25:28.649116039 CET	49713	443	192.168.2.3	185.166.104.3
Nov 20, 2020 11:25:28.651312113 CET	49714	443	192.168.2.3	185.166.104.3
Nov 20, 2020 11:25:28.652987957 CET	49715	443	192.168.2.3	18.209.113.162
Nov 20, 2020 11:25:28.653407097 CET	49716	443	192.168.2.3	18.209.113.162
Nov 20, 2020 11:25:28.672925949 CET	443	49713	185.166.104.3	192.168.2.3
Nov 20, 2020 11:25:28.673126936 CET	49713	443	192.168.2.3	185.166.104.3
Nov 20, 2020 11:25:28.675095081 CET	443	49714	185.166.104.3	192.168.2.3
Nov 20, 2020 11:25:28.675199032 CET	49714	443	192.168.2.3	185.166.104.3
Nov 20, 2020 11:25:28.680970907 CET	49713	443	192.168.2.3	185.166.104.3
Nov 20, 2020 11:25:28.681302071 CET	49714	443	192.168.2.3	185.166.104.3
Nov 20, 2020 11:25:28.704802036 CET	443	49713	185.166.104.3	192.168.2.3
Nov 20, 2020 11:25:28.704909086 CET	443	49714	185.166.104.3	192.168.2.3
Nov 20, 2020 11:25:28.705916882 CET	443	49713	185.166.104.3	192.168.2.3
Nov 20, 2020 11:25:28.705945015 CET	443	49713	185.166.104.3	192.168.2.3
Nov 20, 2020 11:25:28.705957890 CET	443	49713	185.166.104.3	192.168.2.3
Nov 20, 2020 11:25:28.706017017 CET	49713	443	192.168.2.3	185.166.104.3
Nov 20, 2020 11:25:28.706052065 CET	49713	443	192.168.2.3	185.166.104.3
Nov 20, 2020 11:25:28.706882954 CET	443	49714	185.166.104.3	192.168.2.3
Nov 20, 2020 11:25:28.706914902 CET	443	49714	185.166.104.3	192.168.2.3
Nov 20, 2020 11:25:28.706933975 CET	443	49714	185.166.104.3	192.168.2.3
Nov 20, 2020 11:25:28.706963062 CET	49714	443	192.168.2.3	185.166.104.3
Nov 20, 2020 11:25:28.706988096 CET	49714	443	192.168.2.3	185.166.104.3
Nov 20, 2020 11:25:28.741007090 CET	49713	443	192.168.2.3	185.166.104.3
Nov 20, 2020 11:25:28.741549969 CET	49714	443	192.168.2.3	185.166.104.3
Nov 20, 2020 11:25:28.747836113 CET	49713	443	192.168.2.3	185.166.104.3
Nov 20, 2020 11:25:28.747976065 CET	49714	443	192.168.2.3	185.166.104.3
Nov 20, 2020 11:25:28.748090029 CET	49713	443	192.168.2.3	185.166.104.3
Nov 20, 2020 11:25:28.756829977 CET	443	49716	18.209.113.162	192.168.2.3
Nov 20, 2020 11:25:28.757029057 CET	49716	443	192.168.2.3	18.209.113.162
Nov 20, 2020 11:25:28.757123947 CET	443	49715	18.209.113.162	192.168.2.3

Copyright null 2020

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 11:25:28.757198095 CET	49715	443	192.168.2.3	18.209.113.162
Nov 20, 2020 11:25:28.757739067 CET	49716	443	192.168.2.3	18.209.113.162
Nov 20, 2020 11:25:28.758019924 CET	49715	443	192.168.2.3	18.209.113.162
Nov 20, 2020 11:25:28.765116930 CET	443	49713	185.166.104.3	192.168.2.3
Nov 20, 2020 11:25:28.765160084 CET	443	49713	185.166.104.3	192.168.2.3
Nov 20, 2020 11:25:28.765266895 CET	49713	443	192.168.2.3	185.166.104.3
Nov 20, 2020 11:25:28.765299082 CET	49713	443	192.168.2.3	185.166.104.3
Nov 20, 2020 11:25:28.765469074 CET	443	49714	185.166.104.3	192.168.2.3
Nov 20, 2020 11:25:28.765484095 CET	443	49714	185.166.104.3	192.168.2.3
Nov 20, 2020 11:25:28.765624046 CET	49714	443	192.168.2.3	185.166.104.3
Nov 20, 2020 11:25:28.766083956 CET	49713	443	192.168.2.3	185.166.104.3
Nov 20, 2020 11:25:28.766383886 CET	49714	443	192.168.2.3	185.166.104.3
Nov 20, 2020 11:25:28.771645069 CET	443	49713	185.166.104.3	192.168.2.3
Nov 20, 2020 11:25:28.771673918 CET	443	49714	185.166.104.3	192.168.2.3
Nov 20, 2020 11:25:28.771778107 CET	49714	443	192.168.2.3	185.166.104.3
Nov 20, 2020 11:25:28.771780968 CET	49713	443	192.168.2.3	185.166.104.3
Nov 20, 2020 11:25:28.771855116 CET	443	49713	185.166.104.3	192.168.2.3
Nov 20, 2020 11:25:28.771873951 CET	443	49713	185.166.104.3	192.168.2.3
Nov 20, 2020 11:25:28.771891117 CET	443	49713	185.166.104.3	192.168.2.3
Nov 20, 2020 11:25:28.771903038 CET	443	49713	185.166.104.3	192.168.2.3
Nov 20, 2020 11:25:28.771923065 CET	49713	443	192.168.2.3	185.166.104.3
Nov 20, 2020 11:25:28.771924973 CET	443	49713	185.166.104.3	192.168.2.3
Nov 20, 2020 11:25:28.771943092 CET	443	49713	185.166.104.3	192.168.2.3
Nov 20, 2020 11:25:28.771960974 CET	49713	443	192.168.2.3	185.166.104.3
Nov 20, 2020 11:25:28.771965981 CET	443	49713	185.166.104.3	192.168.2.3
Nov 20, 2020 11:25:28.772008896 CET	49713	443	192.168.2.3	185.166.104.3
Nov 20, 2020 11:25:28.788959980 CET	443	49713	185.166.104.3	192.168.2.3
Nov 20, 2020 11:25:28.788988113 CET	443	49713	185.166.104.3	192.168.2.3
Nov 20, 2020 11:25:28.789000988 CET	443	49713	185.166.104.3	192.168.2.3
Nov 20, 2020 11:25:28.789012909 CET	443	49713	185.166.104.3	192.168.2.3
Nov 20, 2020 11:25:28.789132118 CET	49713	443	192.168.2.3	185.166.104.3
Nov 20, 2020 11:25:28.795708895 CET	443	49713	185.166.104.3	192.168.2.3
Nov 20, 2020 11:25:28.795737028 CET	443	49713	185.166.104.3	192.168.2.3
Nov 20, 2020 11:25:28.795753002 CET	443	49713	185.166.104.3	192.168.2.3
Nov 20, 2020 11:25:28.795764923 CET	443	49713	185.166.104.3	192.168.2.3
Nov 20, 2020 11:25:28.795886993 CET	49713	443	192.168.2.3	185.166.104.3
Nov 20, 2020 11:25:28.795917034 CET	49713	443	192.168.2.3	185.166.104.3
Nov 20, 2020 11:25:28.833698034 CET	443	49714	185.166.104.3	192.168.2.3
Nov 20, 2020 11:25:28.860439062 CET	443	49716	18.209.113.162	192.168.2.3
Nov 20, 2020 11:25:28.861129999 CET	443	49716	18.209.113.162	192.168.2.3
Nov 20, 2020 11:25:28.861151934 CET	443	49716	18.209.113.162	192.168.2.3
Nov 20, 2020 11:25:28.861162901 CET	443	49716	18.209.113.162	192.168.2.3
Nov 20, 2020 11:25:28.861246109 CET	49716	443	192.168.2.3	18.209.113.162
Nov 20, 2020 11:25:28.861411095 CET	443	49715	18.209.113.162	192.168.2.3
Nov 20, 2020 11:25:28.862273932 CET	443	49715	18.209.113.162	192.168.2.3
Nov 20, 2020 11:25:28.862298965 CET	443	49715	18.209.113.162	192.168.2.3
Nov 20, 2020 11:25:28.862314939 CET	443	49715	18.209.113.162	192.168.2.3
Nov 20, 2020 11:25:28.862365961 CET	49715	443	192.168.2.3	18.209.113.162
Nov 20, 2020 11:25:28.862396002 CET	49715	443	192.168.2.3	18.209.113.162
Nov 20, 2020 11:25:28.874387980 CET	49716	443	192.168.2.3	18.209.113.162
Nov 20, 2020 11:25:28.874480963 CET	49715	443	192.168.2.3	18.209.113.162
Nov 20, 2020 11:25:28.874998093 CET	49715	443	192.168.2.3	18.209.113.162
Nov 20, 2020 11:25:28.875130892 CET	49715	443	192.168.2.3	18.209.113.162
Nov 20, 2020 11:25:28.875195026 CET	49715	443	192.168.2.3	18.209.113.162
Nov 20, 2020 11:25:28.875241041 CET	49716	443	192.168.2.3	18.209.113.162
Nov 20, 2020 11:25:28.977375031 CET	443	49716	18.209.113.162	192.168.2.3
Nov 20, 2020 11:25:28.977418900 CET	443	49716	18.209.113.162	192.168.2.3
Nov 20, 2020 11:25:28.977497101 CET	49716	443	192.168.2.3	18.209.113.162
Nov 20, 2020 11:25:28.977526903 CET	49716	443	192.168.2.3	18.209.113.162
Nov 20, 2020 11:25:28.977982044 CET	443	49716	18.209.113.162	192.168.2.3
Nov 20, 2020 11:25:28.978079081 CET	49716	443	192.168.2.3	18.209.113.162
Nov 20, 2020 11:25:28.978138924 CET	443	49715	18.209.113.162	192.168.2.3
Nov 20, 2020 11:25:28.978162050 CET	443	49715	18.209.113.162	192.168.2.3
Nov 20, 2020 11:25:28.978231907 CET	49715	443	192.168.2.3	18.209.113.162

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 11:25:28.978260040 CET	49715	443	192.168.2.3	18.209.113.162
Nov 20, 2020 11:25:28.978400946 CET	443	49715	18.209.113.162	192.168.2.3
Nov 20, 2020 11:25:28.978483915 CET	49715	443	192.168.2.3	18.209.113.162
Nov 20, 2020 11:25:28.978560925 CET	443	49715	18.209.113.162	192.168.2.3
Nov 20, 2020 11:25:28.978765011 CET	49716	443	192.168.2.3	18.209.113.162
Nov 20, 2020 11:25:28.979296923 CET	49715	443	192.168.2.3	18.209.113.162

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 11:25:20.845921040 CET	60831	53	192.168.2.3	8.8.8.8
Nov 20, 2020 11:25:20.883887053 CET	53	60831	8.8.8.8	192.168.2.3
Nov 20, 2020 11:25:21.579787016 CET	60100	53	192.168.2.3	8.8.8.8
Nov 20, 2020 11:25:21.607012033 CET	53	60100	8.8.8.8	192.168.2.3
Nov 20, 2020 11:25:27.269762039 CET	53195	53	192.168.2.3	8.8.8.8
Nov 20, 2020 11:25:27.305557966 CET	53	53195	8.8.8.8	192.168.2.3
Nov 20, 2020 11:25:28.592164040 CET	50141	53	192.168.2.3	8.8.8.8
Nov 20, 2020 11:25:28.595928907 CET	53023	53	192.168.2.3	8.8.8.8
Nov 20, 2020 11:25:28.631537914 CET	53	53023	8.8.8.8	192.168.2.3
Nov 20, 2020 11:25:28.646873951 CET	53	50141	8.8.8.8	192.168.2.3
Nov 20, 2020 11:25:31.312299013 CET	49563	53	192.168.2.3	8.8.8.8
Nov 20, 2020 11:25:31.348078966 CET	53	49563	8.8.8.8	192.168.2.3
Nov 20, 2020 11:25:32.387758970 CET	51352	53	192.168.2.3	8.8.8.8
Nov 20, 2020 11:25:32.414787054 CET	53	51352	8.8.8.8	192.168.2.3
Nov 20, 2020 11:25:33.202666044 CET	59349	53	192.168.2.3	8.8.8.8
Nov 20, 2020 11:25:33.229741096 CET	53	59349	8.8.8.8	192.168.2.3
Nov 20, 2020 11:25:33.872510910 CET	57084	53	192.168.2.3	8.8.8.8
Nov 20, 2020 11:25:33.899594069 CET	53	57084	8.8.8.8	192.168.2.3
Nov 20, 2020 11:25:34.571896076 CET	58823	53	192.168.2.3	8.8.8.8
Nov 20, 2020 11:25:34.598961115 CET	53	58823	8.8.8.8	192.168.2.3
Nov 20, 2020 11:25:35.423058033 CET	57568	53	192.168.2.3	8.8.8.8
Nov 20, 2020 11:25:35.450545073 CET	53	57568	8.8.8.8	192.168.2.3
Nov 20, 2020 11:25:37.039868116 CET	50540	53	192.168.2.3	8.8.8.8
Nov 20, 2020 11:25:37.067079067 CET	53	50540	8.8.8.8	192.168.2.3
Nov 20, 2020 11:25:37.736941099 CET	54366	53	192.168.2.3	8.8.8.8
Nov 20, 2020 11:25:37.764038086 CET	53	54366	8.8.8.8	192.168.2.3
Nov 20, 2020 11:25:49.858526945 CET	53034	53	192.168.2.3	8.8.8.8
Nov 20, 2020 11:25:49.886069059 CET	53	53034	8.8.8.8	192.168.2.3
Nov 20, 2020 11:25:51.662534952 CET	57762	53	192.168.2.3	8.8.8.8
Nov 20, 2020 11:25:51.689765930 CET	53	57762	8.8.8.8	192.168.2.3
Nov 20, 2020 11:25:53.472920895 CET	55435	53	192.168.2.3	8.8.8.8
Nov 20, 2020 11:25:53.500020981 CET	53	55435	8.8.8.8	192.168.2.3
Nov 20, 2020 11:25:54.128175974 CET	50713	53	192.168.2.3	8.8.8.8
Nov 20, 2020 11:25:54.165997982 CET	53	50713	8.8.8.8	192.168.2.3
Nov 20, 2020 11:25:57.301301003 CET	56132	53	192.168.2.3	8.8.8.8
Nov 20, 2020 11:25:57.337027073 CET	53	56132	8.8.8.8	192.168.2.3
Nov 20, 2020 11:25:58.114677906 CET	58987	53	192.168.2.3	8.8.8.8
Nov 20, 2020 11:25:58.150515079 CET	53	58987	8.8.8.8	192.168.2.3
Nov 20, 2020 11:25:58.313416958 CET	56132	53	192.168.2.3	8.8.8.8
Nov 20, 2020 11:25:58.340447903 CET	53	56132	8.8.8.8	192.168.2.3
Nov 20, 2020 11:25:59.104906082 CET	58987	53	192.168.2.3	8.8.8.8
Nov 20, 2020 11:25:59.132030010 CET	53	58987	8.8.8.8	192.168.2.3
Nov 20, 2020 11:25:59.324069977 CET	56132	53	192.168.2.3	8.8.8.8
Nov 20, 2020 11:25:59.351089954 CET	53	56132	8.8.8.8	192.168.2.3
Nov 20, 2020 11:26:00.120460033 CET	58987	53	192.168.2.3	8.8.8.8
Nov 20, 2020 11:26:00.166840076 CET	53	58987	8.8.8.8	192.168.2.3
Nov 20, 2020 11:26:01.339915037 CET	56132	53	192.168.2.3	8.8.8.8
Nov 20, 2020 11:26:01.367182970 CET	53	56132	8.8.8.8	192.168.2.3
Nov 20, 2020 11:26:02.136172056 CET	58987	53	192.168.2.3	8.8.8.8
Nov 20, 2020 11:26:02.182342052 CET	53	58987	8.8.8.8	192.168.2.3
Nov 20, 2020 11:26:05.377055883 CET	56132	53	192.168.2.3	8.8.8.8
Nov 20, 2020 11:26:05.423424006 CET	53	56132	8.8.8.8	192.168.2.3
Nov 20, 2020 11:26:06.157399893 CET	58987	53	192.168.2.3	8.8.8.8
Nov 20, 2020 11:26:06.195194960 CET	53	58987	8.8.8.8	192.168.2.3

Copyright null 2020

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 11:26:19.555505037 CET	56579	53	192.168.2.3	8.8.8.8
Nov 20, 2020 11:26:19.591114044 CET	53	56579	8.8.8.8	192.168.2.3
Nov 20, 2020 11:26:20.285681009 CET	60633	53	192.168.2.3	8.8.8.8
Nov 20, 2020 11:26:20.321077108 CET	53	60633	8.8.8.8	192.168.2.3
Nov 20, 2020 11:26:20.901051044 CET	61292	53	192.168.2.3	8.8.8.8
Nov 20, 2020 11:26:20.928047895 CET	53	61292	8.8.8.8	192.168.2.3
Nov 20, 2020 11:26:21.238286972 CET	63619	53	192.168.2.3	8.8.8.8
Nov 20, 2020 11:26:21.274694920 CET	53	63619	8.8.8.8	192.168.2.3
Nov 20, 2020 11:26:21.605727911 CET	64938	53	192.168.2.3	8.8.8.8
Nov 20, 2020 11:26:21.632769108 CET	53	64938	8.8.8.8	192.168.2.3
Nov 20, 2020 11:26:22.041721106 CET	61946	53	192.168.2.3	8.8.8.8
Nov 20, 2020 11:26:22.068978071 CET	53	61946	8.8.8.8	192.168.2.3
Nov 20, 2020 11:26:22.154016972 CET	64910	53	192.168.2.3	8.8.8.8
Nov 20, 2020 11:26:22.189713955 CET	53	64910	8.8.8.8	192.168.2.3
Nov 20, 2020 11:26:22.721561909 CET	52123	53	192.168.2.3	8.8.8.8
Nov 20, 2020 11:26:22.767801046 CET	53	52123	8.8.8.8	192.168.2.3
Nov 20, 2020 11:26:23.777124882 CET	56130	53	192.168.2.3	8.8.8.8
Nov 20, 2020 11:26:23.804310083 CET	53	56130	8.8.8.8	192.168.2.3
Nov 20, 2020 11:26:25.034368038 CET	56338	53	192.168.2.3	8.8.8.8
Nov 20, 2020 11:26:25.070208073 CET	53	56338	8.8.8.8	192.168.2.3
Nov 20, 2020 11:26:25.568754911 CET	59420	53	192.168.2.3	8.8.8.8
Nov 20, 2020 11:26:25.615036964 CET	53	59420	8.8.8.8	192.168.2.3
Nov 20, 2020 11:26:33.618117094 CET	58784	53	192.168.2.3	8.8.8.8
Nov 20, 2020 11:26:33.655600071 CET	53	58784	8.8.8.8	192.168.2.3
Nov 20, 2020 11:27:02.200150013 CET	63978	53	192.168.2.3	8.8.8.8
Nov 20, 2020 11:27:02.227191925 CET	53	63978	8.8.8.8	192.168.2.3
Nov 20, 2020 11:27:06.692781925 CET	62938	53	192.168.2.3	8.8.8.8
Nov 20, 2020 11:27:06.730767965 CET	53	62938	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 20, 2020 11:25:28.592164040 CET	192.168.2.3	8.8.8.8	0x89fe	Standard query (0)	atcocorp.okta.com	A (IP address)	IN (0x0001)
Nov 20, 2020 11:25:28.595928907 CET	192.168.2.3	8.8.8.8	0xa485	Standard query (0)	s.cafebazaar.ir	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 20, 2020 11:25:28.631537914 CET	8.8.8.8	192.168.2.3	0xa485	No error (0)	s.cafebazaar.ir	b5d75f750c811003839a64fb243bafc0.cdn.cafebazaar.cloud		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 11:25:28.631537914 CET	8.8.8.8	192.168.2.3	0xa485	No error (0)	b5d75f750c811003839a64fb243bafc0.cdn.cafebazaar.cloud		185.166.104.3	A (IP address)	IN (0x0001)
Nov 20, 2020 11:25:28.631537914 CET	8.8.8.8	192.168.2.3	0xa485	No error (0)	b5d75f750c811003839a64fb243bafc0.cdn.cafebazaar.cloud		185.166.104.4	A (IP address)	IN (0x0001)
Nov 20, 2020 11:25:28.646873951 CET	8.8.8.8	192.168.2.3	0x89fe	No error (0)	atcocorp.okta.com	ok4-crtrs.tng.okta.com		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 11:25:28.646873951 CET	8.8.8.8	192.168.2.3	0x89fe	No error (0)	ok4-crtrs.tng.okta.com	ok4-crtr-tls12-nlb-29367a8e4bb80716.elb.us-east-1.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 11:25:28.646873951 CET	8.8.8.8	192.168.2.3	0x89fe	No error (0)	ok4-crtr-tls12-nlb-29367a8e4bb80716.elb.us-east-1.amazonaws.com		18.209.113.162	A (IP address)	IN (0x0001)
Nov 20, 2020 11:25:28.646873951 CET	8.8.8.8	192.168.2.3	0x89fe	No error (0)	ok4-crtr-tls12-nlb-29367a8e4bb80716.elb.us-east-1.amazonaws.com		18.209.113.163	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 20, 2020 11:25:28.646873951 CET	8.8.8.8	192.168.2.3	0x89fe	No error (0)	ok4-crtr-tls12-nlb-2 9367a8e4bb 80716.elb.us-east-1. amazonaws.com		18.209.113.161	A (IP address)	IN (0x0001)

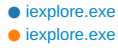
HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Nov 20, 2020 11:25:28.705945015 CET	185.166.104.3	443	192.168.2.3	49713	CN=s.cafebazaar.ir 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.	Sat Sep 26 19:53:54 CEST 2020	Fri Dec 25 18:53:54 CET 2020	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 20, 2020 11:25:28.706914902 CET	185.166.104.3	443	192.168.2.3	49714	CN=s.cafebazaar.ir 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.	Sat Sep 26 19:53:54 CEST 2020	Fri Dec 25 18:53:54 CET 2020	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 20, 2020 11:25:28.861162901 CET	18.209.113.162	443	192.168.2.3	49716	CN=*.okta.com, O="Okta, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue May 28 02:00:00 CEST 2019	Fri May 28 14:00:00 CEST 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=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		
Nov 20, 2020 11:25:28.862314939 CET	18.209.113.162	443	192.168.2.3	49715	CN=*.okta.com, O="Okta, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue May 28 02:00:00 CEST 2019	Fri May 28 14:00:00 CEST 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=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: 5276 Parent PID: 792

General

Start time:	11:25:26
Start date:	20/11/2020
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff75c010000
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

Copyright null 2020

Analysis Process: iexplore.exe PID: 5600 Parent PID: 5276

General

Start time:	11:25:26
Start date:	20/11/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5276 CREDAT:17410 /prefetch:2
Imagebase:	0xa20000
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