ID: 385346
Sample Name:
mfalomirm@gentalia.eu.HTM
Cookbook: default.jbs
Time: 11:04:57
Date: 12/04/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2
Analysis Report mfalomirm@gentalia.eu.HTM 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
Data Obfuscation: 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 8
Public 9
Private 9
General Information 9
Simulations 10
Behavior and APIs 10
Joe Sandbox View / Context 10
IPs 10
Domains 11
ASN 11
JA3 Fingerprints 11
Dropped Files 12
Created / dropped Files 12
Static File Info 18
General 18
File Icon 18
Network Behavior 19
Network Port Distribution 19
TCP Packets 19
UDP Packets 20
DNS Queries 22
DNS Answers 22
HTTPS Packets 22
Code Manipulations 23
Statistics 23
Behavior 23

System Behavior 24
Analysis Process: iexplore.exe PID: 5280 Parent PID: 792 24
General 24
File Activities 24
Registry Activities 24
Analysis Process: iexplore.exe PID: 3892 Parent PID: 5280 24
General 25
File Activities 25
Registry Activities 25
Disassembly 25

Analysis Report mfalomirm@gentalia.eu.HTM

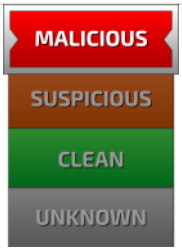
Overview

General Information

Sample Name:	mfalomirm@gentalia.eu.HTM
Analysis ID:	385346
MD5:	ebe2a44409febe2.
SHA1:	6cc7a3f83e3dbf6..
SHA256:	8d4ef43acbf962d..
Infos:	

Most interesting Screenshot:

Detection



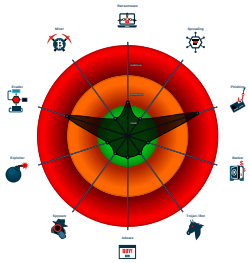
HTMLPhisher

Score:	60
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected HtmlPhish6
- Yara detected obfuscated html page
- Obfuscated HTML file found
- HTML body contains low number of …
- HTML title does not match URL
- IP address seen in connection with o…
- JA3 SSL client fingerprint seen in co…
- None HTTPS page querying sensitiv…
- Suspicious form URL found

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 5280 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 3892 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5280 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

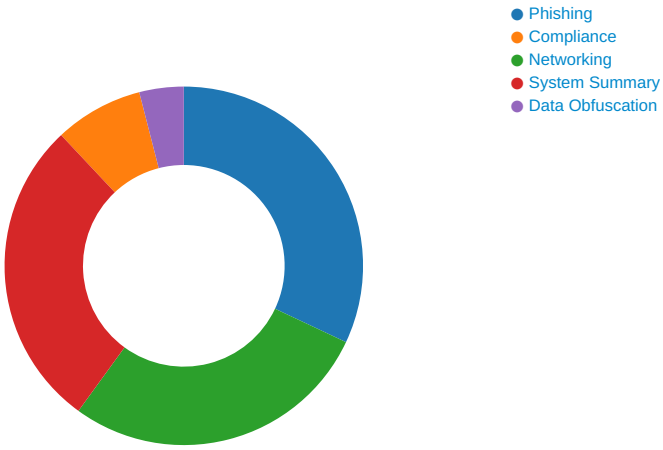
Initial Sample

Source	Rule	Description	Author	Strings
mfalomirm@gentalia.eu.HTM	JoeSecurity_Obshtml	Yara detected obfuscated html page	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

Phishing:

Yara detected HtmlPhish6

Yara detected obfuscated html page

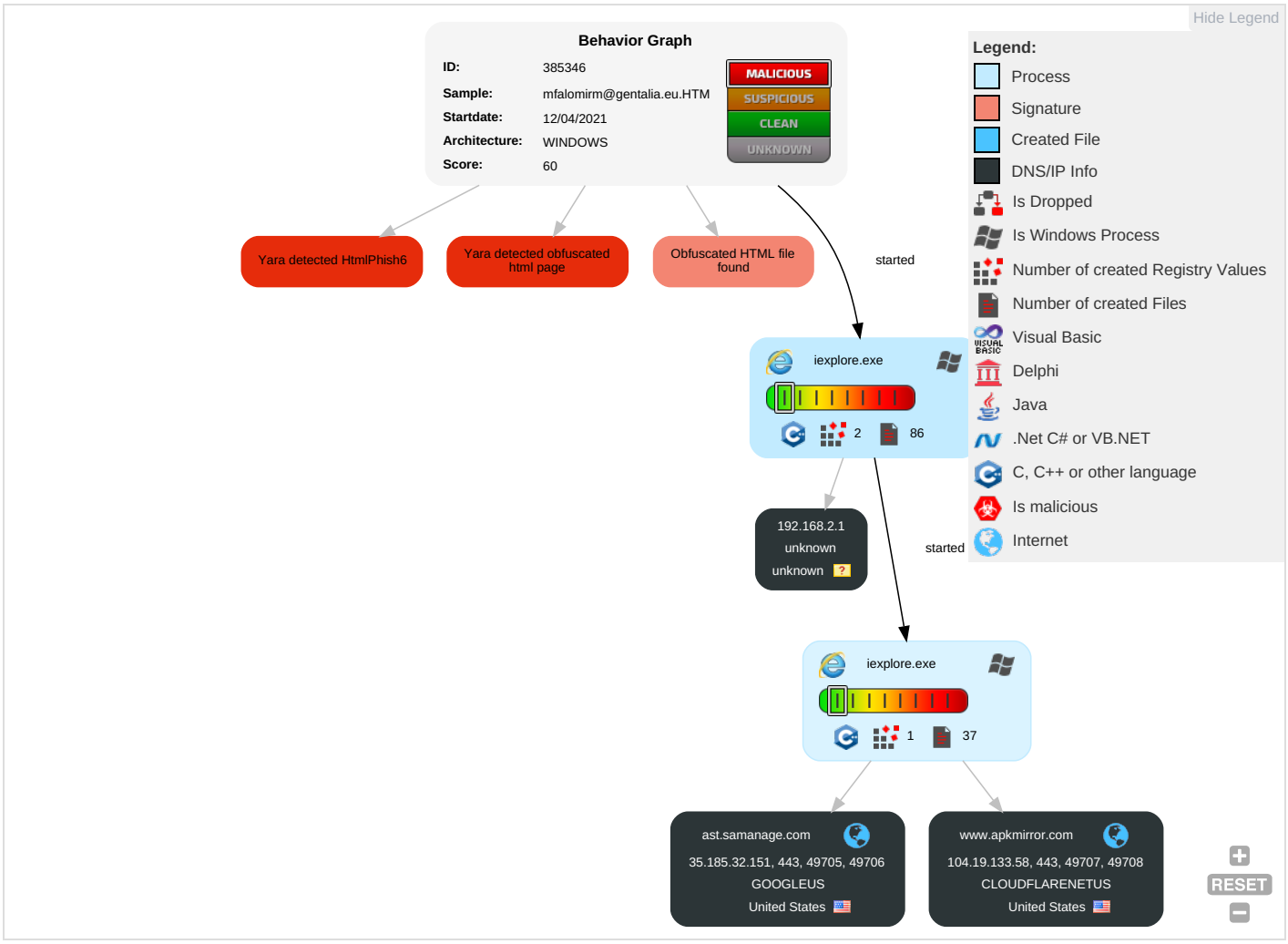
Data Obfuscation:

Obfuscated HTML file found

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impac
Valid Accounts	Scripting 1	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify Syster Partiti
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockou
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Scripting 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrie Billing Fraud

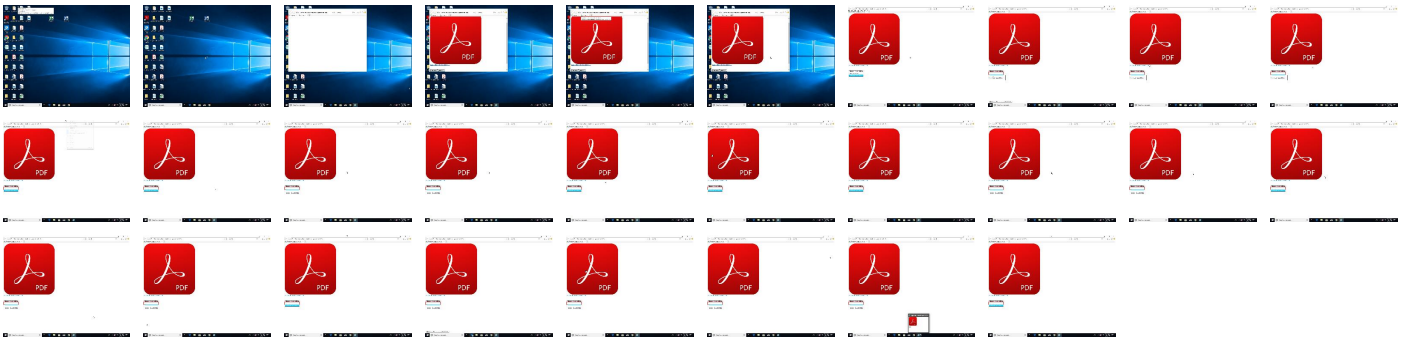
Behavior Graph

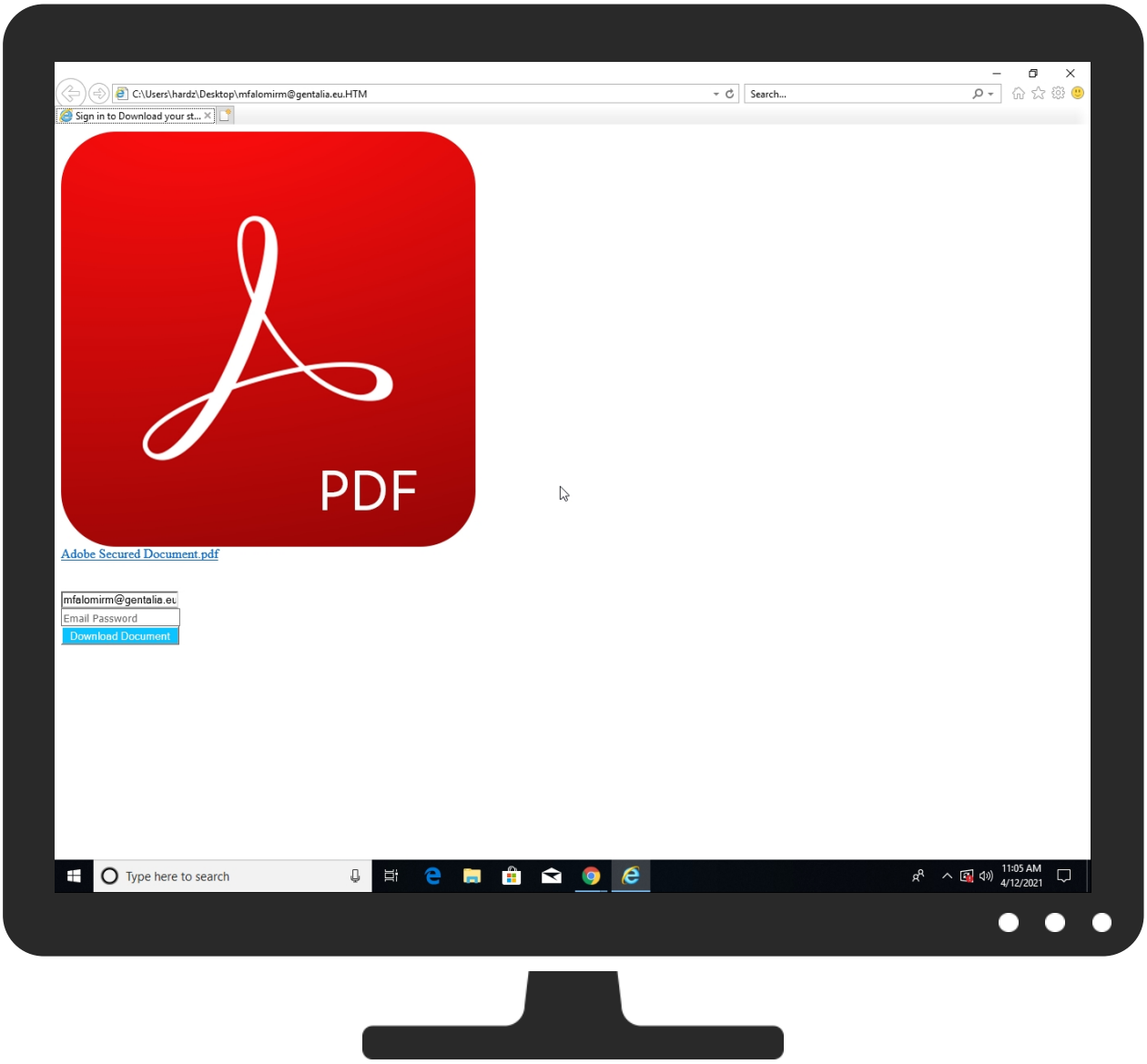


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.wikipedia.com/	0%	URL Reputation	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
www.apkmirror.com	104.19.133.58	true	false		high
ast.samanage.com	35.185.32.151	true	false		high

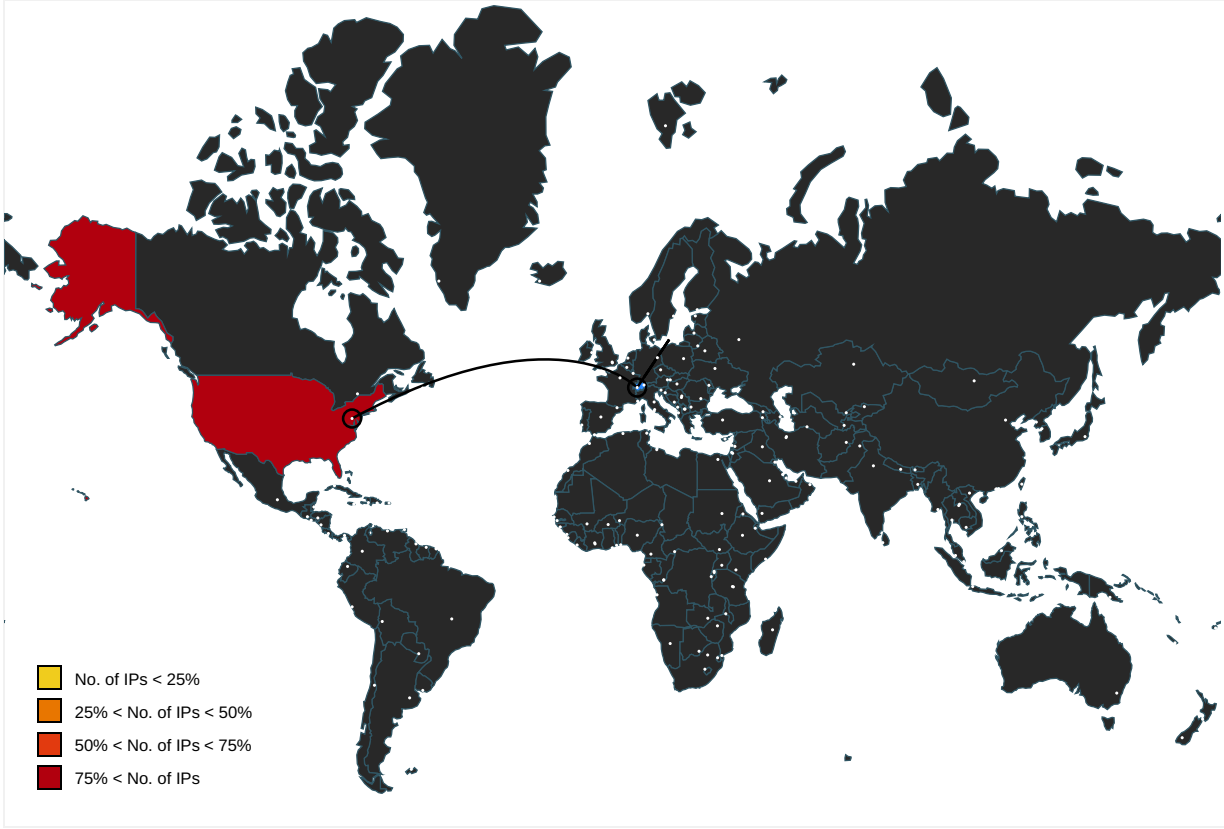
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
file:///C:/Users/user/Desktop/mfalomirm@gentalia.eu.HTM	true		low

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://jqueryui.com/themeroller/	index-0242ce1e093b95352b7de17f4889d924aa964c6ed418fcb2f51a6850c69675ef[1].css.3.dr	false		high
http://api.jqueryui.com/datepicker/	index-a68f016bafb3011a49d6ef1c1a6d1f61da04b24015de7fda99497fbf4d1b8d3d[1].js.3.dr	false		high
http://docs.jquery.com/UI/Slider#theming	index-0242ce1e093b95352b7de17f4889d924aa964c6ed418fcb2f51a6850c69675ef[1].css.3.dr	false		high
http://www.nytimes.com/	msapplication.xml3.2.dr	false		high
http://jquery.org/license	index-b7458e62bace5aee761c61948f390a6633709afd2adb0643cb8d250734bd25a6[1].js.3.dr	false		high
http://docs.jquery.com/UI/Tabs#theming	index-0242ce1e093b95352b7de17f4889d924aa964c6ed418fcb2f51a6850c69675ef[1].css.3.dr	false		high
http://www.youtube.com/	msapplication.xml7.2.dr	false		high
http://docs.jquery.com/UI/Dialog#theming	index-0242ce1e093b95352b7de17f4889d924aa964c6ed418fcb2f51a6850c69675ef[1].css.3.dr	false		high
http://docs.jquery.com/UI/Theming/API	index-0242ce1e093b95352b7de17f4889d924aa964c6ed418fcb2f51a6850c69675ef[1].css.3.dr	false		high
http://sizzlejs.com/	index-b7458e62bace5aee761c61948f390a6633709afd2adb0643cb8d250734bd25a6[1].js.3.dr	false		high
http://api.jqueryui.com/category/ui-core/	index-a68f016bafb3011a49d6ef1c1a6d1f61da04b24015de7fda99497fbf4d1b8d3d[1].js.3.dr	false		high
http://jqueryui.com	index-0242ce1e093b95352b7de17f4889d924aa964c6ed418fcb2f51a6850c69675ef[1].css.3.dr	false		high
http://docs.jquery.com/UI/Button#theming	index-0242ce1e093b95352b7de17f4889d924aa964c6ed418fcb2f51a6850c69675ef[1].css.3.dr	false		high
http://www.wikipedia.com/	msapplication.xml6.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://docs.jquery.com/UI/Datepicker#theming	index-0242ce1e093b95352b7de17f4889d924aa964c6ed418fcb2f51a6850c69675ef[1].css.3.dr	false		high
http://www.amazon.com/	msapplication.xml.2.dr	false		high
http://www.live.com/	msapplication.xml2.2.dr	false		high
http://www.reddit.com/	msapplication.xml4.2.dr	false		high
http://www.twitter.com/	msapplication.xml5.2.dr	false		high
http://docs.jquery.com/UI/Resizable#theming	index-0242ce1e093b95352b7de17f4889d924aa964c6ed418fcb2f51a6850c69675ef[1].css.3.dr	false		high
http://jquery.com/	index-b7458e62bace5aee761c61948f390a6633709afd2adb0643cb8d250734bd25a6[1].js.3.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
35.185.32.151	ast.samanage.com	United States		15169	GOOGLEUS	false
104.19.133.58	www.apkmirror.com	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	385346
Start date:	12.04.2021
Start time:	11:04:57
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 51s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	mfalomirm@gentalia.eu.HTM
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	29
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:	mal60.phis.evad.winHTM@3/19@2/3
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .HTM
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 92.122.145.220, 88.221.62.148, 52.147.198.201, 184.30.24.134, 93.184.220.29, 20.82.210.154, 152.199.19.161, 184.30.24.56, 40.88.32.150, 13.64.90.137, 52.255.188.83, 92.122.213.194, 92.122.213.247, 205.185.216.42, 205.185.216.10, 20.54.26.129, 104.42.151.234 • Excluded domains from analysis (whitelisted): e4578.dscg.akamaiedge.net, cs9.wac.phicdn.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.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, e12564.dspb.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, go.microsoft.com, ocsp.digicert.com, ssl-delivery.adobe.com.edgekey.net, audownload.windowsupdate.nsatc.net, au.download.windowsupdate.com.hwcdn.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, skypedataprdcolwus17.cloudapp.net, acrobat.adobe.com, fs.microsoft.com, ie9comview.vo.msecnd.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, cds.d2s7q6s2.hwcdn.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, store-images.s-microsoft.com, go.microsoft.com.edgekey.net, blobcollector.events.data.trafficmanager.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
104.19.133.58	FGzfp11Eji.exe	Get hash	malicious	Browse	
	Q4OfyKlLsy.exe	Get hash	malicious	Browse	
	p7ZXKudJWx.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	5WUX3Id8Bf.exe	Get hash	malicious	Browse	
	o7YZ7bAZyL.exe	Get hash	malicious	Browse	
	vanessadec@taqania.com.hTmL	Get hash	malicious	Browse	
	Adobe Secured.hTm	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.apkmirror.com	a.exe	Get hash	malicious	Browse	• 104.19.135.58
	TJ3Z43yN2m.exe	Get hash	malicious	Browse	• 104.19.135.58
	Tu8O5QdOKb.exe	Get hash	malicious	Browse	• 104.19.132.58
	ZYsTo6YDs9.exe	Get hash	malicious	Browse	• 104.19.134.58
	FGzfp11Eji.exe	Get hash	malicious	Browse	• 104.19.133.58
	Q4OfyKlLsy.exe	Get hash	malicious	Browse	• 104.19.133.58
	I1ELzkKHHV.exe	Get hash	malicious	Browse	• 104.19.134.58
	KKerT1Jel3.exe	Get hash	malicious	Browse	• 104.19.132.58
	sr43539SKp.exe	Get hash	malicious	Browse	• 104.19.136.58
	5jdXr0PniA.exe	Get hash	malicious	Browse	• 104.19.132.58
	xaVDKpgbfl.exe	Get hash	malicious	Browse	• 104.19.136.58
	p7ZXKudJWx.exe	Get hash	malicious	Browse	• 104.19.135.58
	p7ZXKudJWx.exe	Get hash	malicious	Browse	• 104.19.133.58
	jBAaHtOYXq.exe	Get hash	malicious	Browse	• 104.19.136.58
	5WUX3Id8Bf.exe	Get hash	malicious	Browse	• 104.19.133.58
	o7YZ7bAZyL.exe	Get hash	malicious	Browse	• 104.19.133.58
	5WUX3Id8Bf.exe	Get hash	malicious	Browse	• 104.19.134.58
	nancy.alarie.chum@ssss.gouv.qc.ca.HTM	Get hash	malicious	Browse	• 104.19.132.58
	t7865p@lvmpd.com.HTM	Get hash	malicious	Browse	• 104.19.132.58
	fin_supportservices@txdot.gov.HTM	Get hash	malicious	Browse	• 104.19.132.58

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	KHAWATMI CO.IMPORT & EXPORT_PDF.exe	Get hash	malicious	Browse	• 104.21.17.57
	YNzE2QUkvaTK7kd.exe	Get hash	malicious	Browse	• 172.67.148.14
	NdBLyH2h5d.exe	Get hash	malicious	Browse	• 23.227.38.74
	s6G3ZtvHZg.exe	Get hash	malicious	Browse	• 172.67.130.43
	4oItdZkNOZ.exe	Get hash	malicious	Browse	• 23.227.38.74
	ieuHgdpuPo.exe	Get hash	malicious	Browse	• 104.21.17.57
	Cobro Juridico_0420198202_326828_4985792583130360_300690_8122300886764676459_5190713730838_pdf.exe	Get hash	malicious	Browse	• 172.67.222.176
	Payment Slip.doc	Get hash	malicious	Browse	• 104.21.17.57
	Cobro Juridico_0291662728_7023446_452487041454723_016698_5192136884256735776_2301761820735_pdf.exe	Get hash	malicious	Browse	• 104.21.17.57
	INQUIRY 1820521 pdf.exe	Get hash	malicious	Browse	• 104.21.82.58
	PaymentCopy.vbs	Get hash	malicious	Browse	• 172.67.222.131
	PAYMENT COPY.exe	Get hash	malicious	Browse	• 104.21.28.135
	PO NUMBER 3120386 3120393 SIGNED.exe	Get hash	malicious	Browse	• 1.2.3.4
	Cobro Juridico_07223243630_5643594_539661009070075_49874359_5059639084170590400_7272781644_pdf.exe	Get hash	malicious	Browse	• 172.67.222.176
	BL2659618800638119374.xls.exe	Get hash	malicious	Browse	• 172.67.222.176
	Purchase order and quote confirmation.exe	Get hash	malicious	Browse	• 172.67.222.176
	Confirm Order for SK TRIMS & INDUSTRIES_DK4571,pdf .exe	Get hash	malicious	Browse	• 172.67.188.154
	Re Confirm#U00ffthe invoice#U00ffthe payment slip.exe	Get hash	malicious	Browse	• 104.21.17.57
	SOA.exe	Get hash	malicious	Browse	• 104.21.19.200
	RFQ No A'4762GHTECHNICAL DETAILS.exe	Get hash	malicious	Browse	• 104.21.19.200

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
9e10692f1b7f78228b2d4e424db3a98c	RemitSwift119353 xlsx.htm	Get hash	malicious	Browse	• 35.185.32.151 • 104.19.133.58
	Miral-Purushotham.verra.htm	Get hash	malicious	Browse	• 35.185.32.151 • 104.19.133.58
	IJht2pqbVh.exe	Get hash	malicious	Browse	• 35.185.32.151 • 104.19.133.58

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	782kQ15aYm.dll	Get hash	malicious	Browse	• 35.185.32.151 • 104.19.133.58
	$108,459.00.html	Get hash	malicious	Browse	• 35.185.32.151 • 104.19.133.58
	Alexandra38.docx	Get hash	malicious	Browse	• 35.185.32.151 • 104.19.133.58
	Tmd7W7qwQw.dll	Get hash	malicious	Browse	• 35.185.32.151 • 104.19.133.58
	9R5WtLGEAy.dll	Get hash	malicious	Browse	• 35.185.32.151 • 104.19.133.58
	ghnrope2.dll	Get hash	malicious	Browse	• 35.185.32.151 • 104.19.133.58
	mail_6512365134_7863_202104108.html	Get hash	malicious	Browse	• 35.185.32.151 • 104.19.133.58
	mapdata.dll	Get hash	malicious	Browse	• 35.185.32.151 • 104.19.133.58
	#Ud83d#Udcde973.htm	Get hash	malicious	Browse	• 35.185.32.151 • 104.19.133.58
	#U266b SecuredMessage.htm	Get hash	malicious	Browse	• 35.185.32.151 • 104.19.133.58
	Offline_record_ON-035107.htm	Get hash	malicious	Browse	• 35.185.32.151 • 104.19.133.58
	Fax-Message-4564259.html	Get hash	malicious	Browse	• 35.185.32.151 • 104.19.133.58
	Enclosed Updated Project Proposal From Robert Nilsson robert@lindstromundertak.se.html	Get hash	malicious	Browse	• 35.185.32.151 • 104.19.133.58
	nicoleta.fagaras-DHL_TRACKING_1394942.html	Get hash	malicious	Browse	• 35.185.32.151 • 104.19.133.58
	Signed pages of agreement copy.html	Get hash	malicious	Browse	• 35.185.32.151 • 104.19.133.58
	ensono8639844766FAXMESSAGE.HTM	Get hash	malicious	Browse	• 35.185.32.151 • 104.19.133.58
	Payment Report.html	Get hash	malicious	Browse	• 35.185.32.151 • 104.19.133.58

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{B18D9DF7-9BB9-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	45656
Entropy (8bit):	1.9479523856430947
Encrypted:	false
SSDEEP:	192:rlZOZs2HWwtJfVxMdrdEdPfd9crd9dsded8d2X:rrab2U5YFGFq/OoSl
MD5:	D79589800B057503F7BF747C54AD4D11
SHA1:	155FAF4EC962CD94815690AAF5331886915E5A76
SHA-256:	05D5052D1A57BF969D893E544D3D14891E97D62D52FDC4BA457B5013690BCCDF
SHA-512:	4FFD4A5D93665F33563AF07164C8505E4983D2E5E512913199EAA3B5A34F3960129032B04020F1BD4C8323240034CC28B57D5F7EFEA828F6303E7E469A7BA018
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\{B18D9DF9-9BB9-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28524
Entropy (8bit):	1.948133682674411
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{B18D9DF9-9BB9-11EB-90E4-ECF4BB862DED}.dat	
SSDEEP:	48:IwtGcprYGwpa50G4pQ/mGrapbSxGQpBd0GHHpcKxTGUp8doGzYpmL6Gop1VKomGW:rzZAQa6ABSLjdr2mWdsM+7IgOR/qMdr
MD5:	F8F3532EA5AE62C67225C567ED21090A
SHA1:	D9A5CD1057890FD6413DC828D043F81358FCC4D5
SHA-256:	D7A9F0C711C2B9D045D778A796EA428D30773F501C711102940183BD557C3E43
SHA-512:	2B7E7EAFD506021879CC5EE92D8B3B558C530C813879725F86C2B0856BC837EBFD23883C6BF506503B1EF7A25EFB02B3D6A5A208961ED8E76A7CBC99FB2C69 5
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\{B18D9DFA-9BB9-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5646846458329198
Encrypted:	false
SSDEEP:	48:IwDGcprCGwpawG4pQQGrapbS5GQpKLG7HpRpTGIpG:r5ZqQw6uBSTAKTPA
MD5:	8C48B8A1C1BDC73DB7B3A7DACC0E0543
SHA1:	06ACFF656DB496C7084A513DE898920EB7B5A2A4
SHA-256:	35E7209D3D11A452E4D7EE50B06FDB808D4590B48B17166C2E384A4244CC98A2
SHA-512:	B89B8685C915171BC67BA88A431BAD49C5B300A15BF78F4B0F832FEFF45523EF798172CC76B41BFD56FA8DE98BF382AD21EABF76E5283E097D57DC2046F0448
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):	5.089611646328552
Encrypted:	false
SSDEEP:	12:TMHdNMNxOEEAdVjAdVAnWimI002EtM3MHdNMNxOEEAdVjAdVAnWimI00ObVbkEty:2d6NxOBAdhAd2SZHKd6NxOBAdhAd2SZ4
MD5:	657E0443F408C869722707FC08FBB34F
SHA1:	3666D7F39CB0A7BF4E8BE1A09D28D316F7519786
SHA-256:	7F4B77548B2FAA8D36E1B740C5618D78C5D995AF1B1B91FEC196AA31D061AF3E
SHA-512:	9AF9901EC264ED16A7912F4CB4CCD60A13D1D48AC7A0D2C1BA37F87B45235A6263610641CF17198142A19DFE21A2EDA57C61061BE970B8214C6FA1C05BABB9 9
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x885be1ed,0x01d72fc6</date> accdate>0x885be1ed,0x01d72fc6</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>0x885be1ed,0x01d72fc6</date><accdate>0 x885be1ed,0x01d72fc6</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):	5.143339855085945
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kEC+VjC+VAnWimI002EtM3MHdNMNxe2kEC+VjjEdVAnWimI00Obkan:2d6Nxrhjhj2SZHKd6Nxrhjhj+2SZ7Aan
MD5:	732BFD03E54368F625DB7FA9823FAC7A
SHA1:	0E9E1BC2E2263A86030D31F98C5D07EBA4B2EED4
SHA-256:	7CEFC09C66CE1DEA5D7FA9EB8B25FFF4CC034ED1436594818839281FD7E922B6
SHA-512:	A804A38D802EA05B0BEB2531E64EE24FE73F73FD623FF7859522F2DA1B22C58B38B531DE2A6884856BDFE3DA3B67C8762D36EB139649CA11ED99736ECAEC7B B

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x8852588c,0x01d72fc6</date><accdate>0x8852588c,0x01d72fc6</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>0x8852588c,0x01d72fc6</date><accdate>0x8854baf6,0x01d72fc6</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):	5.108377036894623
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLEAdVjAdVAnWimI002EtM3MHdNMNxvLEAdVjAdVAnWimI00ObmZEtMb:2d6NxvIAdhAd2SZHKd6NxvIAdhAd2SZM
MD5:	2C50CE2A478051D3E09CACDF77847F91
SHA1:	CFF0D4CE8E1A8ACCA3D94AD74686895BA3067CD7
SHA-256:	87029B8E63408EA767EC5C17D6B8783CB1564FFC138DF3B937E2DD1915C7BDD9
SHA-512:	7A68CD5F2FCC32F291011E282D60D8BF05DB01E0FB3CF7BF75A4EEDE1ECA738AA69AF870628EFAF5517D0A12C8CF7BD8941326BCFF4850F8328C39E7FD51C167
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x885be1ed,0x01d72fc6</date><accdate>0x885be1ed,0x01d72fc6</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>0x885be1ed,0x01d72fc6</date><accdate>0x885be1ed,0x01d72fc6</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):	5.151463660963136
Encrypted:	false
SSDEEP:	12:TMHdNMNxiEUeVjUeVAnWimI002EtM3MHdNMNxiEUeVjUeVAnWimI00Obd5EtMb:2d6NxfUehUe2SZHKd6NxfUehUe2SZ7J/
MD5:	7914236B46BCF321CB55D6C6E6A7AF44
SHA1:	E421E8F129F5D267C4FA9A9CD32EB6433E985900
SHA-256:	5FE94DE5441E37383C539CCED7A616FE5C668B81BAE84251586EC147B474E8BF
SHA-512:	2EE299DBD9730C313DAE6BDAAA3EC37F48A53906BE94E3B4AA829A29ED8B6DCEE8028138757542A22D9F3C04F1DA26A9C6EFF1F4479735FFCB67F19F110F587
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x88597fbb,0x01d72fc6</date><accdate>0x88597fbb,0x01d72fc6</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>0x88597fbb,0x01d72fc6</date><accdate>0x88597fbb,0x01d72fc6</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):	5.155635533140932
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwEfVjfVAnWimI002EtM3MHdNMNxhGwEfVjfVAnWimI00Ob8K075Ety:2d6NxQtfhf2SZHKd6NxQtfhf2SZ7YKa/
MD5:	9E640962FB5CA6B84E43EA4019C21BD0
SHA1:	B45DBC9BD61B112D1C630E7DC1A3854F9B3D6DD4
SHA-256:	55E0C236D1293673FC5BA49783EA8C5F75C9FFF77F336EABA70BE0174FEBFC8F
SHA-512:	B3B432EE8C80F2B5836C3F216B6911FE433950B225838A104C22BF6F98B740BCB6CD07500809D50A6E5C3139814C270EAD4765F89F4F0A22282DF2063642E4E9
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x885e446e,0x01d72fc6</date><accdate>0x885e446e,0x01d72fc6</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>0x885e446e,0x01d72fc6</date><accdate>0x885e446e,0x01d72fc6</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):	5.1299004997884845
Encrypted:	false
SSDEEP:	12:TMHdNMNx0nEUeVjUeVAnWimI002EtM3MHdNMNx0nEUeVjAdVAnWimI00ObxEtMb:2d6Nx0EUehUe2SZHKd6Nx0EUehAd2SZX
MD5:	AB1B82BA6A3EE54943B04C67251066DB
SHA1:	CAD391DA8BF48118E67563F74EB242E7107CB9DC
SHA-256:	8C1564AB9F56AC6E44D3AAB49719E3CB2DCC06CE60E1B2E51F049E99078EE052
SHA-512:	B156A223B9465A282D1D2E93C36F1F90E1B1FB66D7F06D858954BC79A9DEFB37685EC6F22F3FA79E30565C4C48D51CF10582076FB5D81CF26BF8151925CB38F7
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x88597fbb,0x01d72fc6</date><accdate>0x88597fbb,0x01d72fc6</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>0x88597fbb,0x01d72fc6</date><accdate>0x885be1ed,0x01d72fc6</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):	5.175560820175227
Encrypted:	false
SSDEEP:	12:TMHdNMNxxEUeVjUeVAnWimI002EtM3MHdNMNxxEUeVjUeVAnWimI00Ob6Kq5EtMb:2d6Nx2UehUe2SZHKd6Nx2UehUe2SZ7ob
MD5:	8931E3193076EE2B4456B30DD2CC47AB
SHA1:	962F8F449B4E6A5EF189CF07EC602C2E0D0CFB1C
SHA-256:	BB42A6799B1D83CE89FED971C025CC65D308DA18E85CAB473184A231A73D5194
SHA-512:	EEDDE3C1269F277EBF9B18A6245869D7A2A772D6EE10ABE8A2C73BE057CFF5EBDC5975D16973D120E58D7DE48FF41BD09218646F48CC7A4F5E5DD3F3D70085 3E
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x88597fbb,0x01d72fc6</date><accdate>0x88597fbb,0x01d72fc6</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>0x88597fbb,0x01d72fc6</date><accdate>0x88597fbb,0x01d72fc6</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):	5.1374008492174505
Encrypted:	false
SSDEEP:	12:TMHdNMNxcELdVjLdVAnWimI002EtM3MHdNMNxcELdVjLdVAnWimI00ObVEtMb:2d6NxJLdhLd2SZHKd6NxJLdhLd2SZ7Db
MD5:	24A51636BC816BD40C787050322D1D6E
SHA1:	FFA33BAC4B62B7DC69DCF7EA2BD5558F87AE4EFC
SHA-256:	3E7B154056986BAB8F025C2210921D753A5DF0AA91C6D60A93B384E02CFA8668
SHA-512:	12DAA5CC6305663AB8D2B2343D3C8F859FFB53B8BF2F23252AD318DA4C010C555D3F7AD47944A237B6F51BC7AEB54FF534C50E1108166E99165EF4CDAF6AEB 2
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x88571d4d,0x01d72fc6</date><accdate>0x88571d4d,0x01d72fc6</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>0x88571d4d,0x01d72fc6</date><accdate>0x88571d4d,0x01d72fc6</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):	5.11954614957584
Encrypted:	false
SSDEEP:	12:TMHdNMNxfnELdVjLdVAnWimI002EtM3MHdNMNxfnELdVjLdVAnWimI00Obe5EtMb:2d6NxsLdhLd2SZHKd6NxsLdhLd2SZ7i/
MD5:	39EDFEB3FC28F878334B279CB7A222C3
SHA1:	BB96164E815C8704192252F155AB5B258B3A125D
SHA-256:	E056168B274BCB47DC2B7B88DF9D4F88B2D7AF615617EC575466D54865493A41
SHA-512:	1A7F8E9CD85F04989636563E74E9ED8A7CC2E3CBDC207546C6450FCD7D622F7106BD39E8B6C44B4448B3A357E0B70B2A23290D56072B7EBBD4B62FBF7949F6D 2
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x88571d4d,0x01d72fc6</date><a ccdate>0x88571d4d,0x01d72fc6</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>0x88571d4d,0x01d72fc6</date><accdate>0x8 8571d4d,0x01d72fc6</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\index-a68f016bafb3011a49d6ef1c1a6d1f61da04b24015de7fda99497fbf4d1b8d3d[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	C source, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	56985
Entropy (8bit):	5.297221026695686
Encrypted:	false
SSDEEP:	1536:Y+Q6quSuVRWCf7v84BfVSrmgCUQ4Cf6OpRP9RAvhYbF+:XXRWoLgvB
MD5:	ECAA098D91C2F0B2B4F7F7436F1B5995
SHA1:	91E8D2773323CBC144D6A029746A0CAD355BE7B2
SHA-256:	A68F016BAFB3011A49D6EF1C1A6D1F61DA04B24015DE7FDA99497FBF4D1B8D3D
SHA-512:	56241991CAD39490EAB8F9C86181A4F2967429492542AE10568DBE76EA668B53CFC714BA84578626EAD2E480CFD058B29EA3A710FC287CF7BE7AA066ED5B060
Malicious:	false
Reputation:	moderate, very likely benign file
IE Cache URL:	http://https://ast.samanage.com/assets/guest/index-a68f016bafb3011a49d6ef1c1a6d1f61da04b24015de7fda99497fbf4d1b8d3d.js
Preview:	!function(t,e){"use strict";var a;t.rails!==e&&t.error("jquery-ujs has already been loaded!");var i=t(document);t.rails=a={linkClickSelector:"a[data-confirm], a[data-method], a[data-remote]:not([disabled]), a[data-disable-with], a[data-disable]",buttonClickSelector:"button[data-remote]:not([form]):not(form button), button[data-confirm]:not([form]):not(form button)",inputChangeSelector:"select[data-remote], input[data-remote], textarea[data-remote]",formSubmitSelector:"form",formInputClickSelector:"form input[type=submit], form input[type=image], form button[type=submit], form button:not([type]), input[type=submit][form], input[type=image][form], button[type=submit][form], button[form]:not([type])",disableSelector:"input[data-disable-with]:enabled, button[data-disable-with]:enabled, textarea[data-disable-with]:enabled, input[data-disable]:enabled, button[data-disable]:enabled, textarea[data-disable]:enabled",enableSelector:"input[data-disable-with]:disabled, button[data-disable-with]:di

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\index-0242ce1e093b95352b7de17f4889d924aa964c6ed418fcb2f51a6850c69675ef[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	84127
Entropy (8bit):	5.125105600779134
Encrypted:	false
SSDEEP:	768:Zef7nBhCILzBeQgc+81XuOLzBNDwA/46gc5BhqF4:ZIBhCtvIxBhj
MD5:	FAE557E76288CB99AC3149E777D1DC71
SHA1:	774CAC341365714E6CBC202ABF64816437DBBB8F
SHA-256:	0242CE1E093B95352B7DE17F4889D924AA964C6ED418FCB2F51A6850C69675EF
SHA-512:	A662F8B527C4AD82739393F81985498A3A6C5BB3A155501086677ABEBA8D82680B7454DB69FE7C290C3B9552BE5B255856FD5564382CDDB32D387978C0842BA1
Malicious:	false
Reputation:	moderate, very likely benign file
IE Cache URL:	http://https://ast.samanage.com/assets/externals/index-0242ce1e093b95352b7de17f4889d924aa964c6ed418fcb2f51a6850c69675ef.css
Preview:	/*! fancyBox v2.1.5 fancyapps.com | fancyapps.com/fancybox/#license */.fancybox-wrap,.fancybox-skin,.fancybox-outer,.fancybox-inner,.fancybox-image,.fancybox-wrap iframe,.fancybox-wrap object,.fancybox-nav,.fancybox-nav span,.fancybox-tmp{padding:0;margin:0;border:0;outline:none;vertical-align:top}.fancybox-wrap{position:absolute;top:0;left:0;z-index:8020}.fancybox-skin{position:relative;background:#f9f9f9;color:#444;text-shadow:none;-webkit-border-radius:4px;-moz-border-radius:4px;border-radius:4px}.fancybox-opened{z-index:8030}.fancybox-opened .fancybox-skin{-webkit-box-shadow:0 10px 25px rgba(0,0,0,0.5);-moz-box-shadow:0 10px 25px rgba(0,0,0,0.5);box-shadow:0 10px 25px rgba(0,0,0,0.5)}.fancybox-outer,.fancybox-inner{position:relative}.fancybox-inner{overflow:hidden}.fancybox-type-iframe .fancybox-inner{-webkit-overflow-scrolling:touch}.fancybox-error{color:#444;font:14px/20px "Helvetica Neue",Helvetica,Arial,sans-serif;margin:0;padding:15px;white-space:nowrap}.fancybox-image,.fancyb

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\5e997a02e4382[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):	44471
Entropy (8bit):	7.964796763508138
Encrypted:	false
SSDEEP:	768:IUFUfr1n8snc2+zfPLAJCqaoogwqjXZ7fbG+m0pBxcitDTkjI9iqvW94Y:IUFu86cbzEJCiogwCp3jpBxDf4qvE
MD5:	EBDA810CBA658560CAA0C4D9BA945DC5
SHA1:	4AC4F2C81084193B3B1C315E44492E919BAA2E83
SHA-256:	0D2D4316F4EB523402C6EE72C3419EE7767BC818F969136568287728AA4FD4E2
SHA-512:	62A0C30CB1C6BD6D29C2CCCFDB6DCFCFDAA41E8C7F2361C5E716EB380711F0C4CBFAF59C73988207214832B0E0DC59D166E004D5E635BCD2E8DE425B601DC1
Malicious:	false
IE Cache URL:	http://https://www.apkmirror.com/wp-content/uploads/2020/04/5e997a02e4382.png
Preview:	.PNG.....IHDR.....x.... .IDATx.....u'~...{..[...H @.....1x.../.....$.o<..'.o.c.C<..;..cb.m..W.b...B..Zz.~K..s..yz.....}..Z.{.....6wvB3...d9N..XeY..e.n.,.....O..t4:.....;.lz./.....Jr..eQ.f..r..d..{..K.)]..;..L....0....^..r..9.....q.p,k..L3..-.....e..r..m.:>.8.,..cY...5.gPv....u...j_F#..2z..*...3Q..?..y...z-..a..s.\..d.0...t-...W..hw..=>0..8.....^u../.<..<.....(..m.x...p.mY.....m.a.>C.....<..&.p..=q....4z.....i...)s.....\.J.g=...56....+..J...x.....K.x=.a."....pt.q..e.m....<(.....Ll..@S.4....\.l[.k.. H...+.JPr..,..W..W.`.....M;..)..d...i..d.A5{.d.W....A.2....._..?..F..>.J.td.q>;.'....uE..hY?....KI.....pl...i.!....K.a.X....i5..T...ZG.@..k....5.of....9<wA.0..6.....`....?...^..;qh..Y.8..... ..P.-\..e..;_../.|...$3.U.S.o.v.e.5...D.+...,..S..o.....6..Z].r/...?..b.*_..H.o?.|:3...%.....~.....w.(.6..~.....d.C'...e}=.8....T.O8n.5.....R.u..T2N..t.....k...@..(.X.=..e.x.....A..K[..-....t..@.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\index-b7458e62bace5aee761c61948f390a6633709afd2adb0643cb8d250734bd25a6[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	86581
Entropy (8bit):	5.258146134922491
Encrypted:	false
SSDEEP:	1536:R7E8kjXHhHCiCLoZcaa8xL+Ltr7ZxdnVeUbTUvbP8IzjvIeOwBpQ2Ml6ivfG7M4D:cbSaav0kwjQey2s0jumv
MD5:	59AA3A9D6D5DF2F4CADDFF969BF6E340
SHA1:	F280E05A179E092D99FB68800A5493C40134C6CB
SHA-256:	B7458E62BACE5AEE761C61948F390A6633709AFD2ADB0643CB8D250734BD25A6
SHA-512:	A87932F1817A9403A3C668A7B0B2D397C46D5F2CC815030693B652EF5E68B8AD40B342768E4D73535A3F1D21BDC8658E0CAAD6E812242EDFD850176B56822655
Malicious:	false
IE Cache URL:	http://https://ast.samanage.com/assets/jquery_lib/index-b7458e62bace5aee761c61948f390a6633709afd2adb0643cb8d250734bd25a6.js
Preview:	/*!. * jQuery JavaScript Library v2.2.4. * http://jquery.com/. *. * Includes Sizzle.js. * http://sizzlejs.com/. *. * Copyright jQuery Foundation and other contributors. * Released under the MIT license. * http://jquery.org/license. *. * Date: 2016-05-20T17:23Z. */.!function(e,t){"object"==typeof module&&"object"==typeof module.exports?module.exports=e.document?t(e,!0):function(e){if(!e.document)throw new Error("jQuery requires a window with a document");return t(e)}:t(e)}("undefined"!=typeof window?window:this,function(e,t){function n(e){var t=!!e&&"length"in e&&e.length,n=oe.type(e);return"function"!==n&&!oe.isWindow(e)&&("array"===n||0===t||"number"==typeof t&&t>0&&t-1 in e)}function r(e,t,n){if(oe.isFunction(t))return oe.grep(e,function(e,r){return!!t.call(e,r,e)!==n});if(t.nodeType)return oe.grep(e,function(e){return e===t!==n});if("string"==typeof t){if(ge.test(t))return oe.filter(t,e,n);t=oe.filter(t,e)}return oe.grep(e,function(e){return Z.call(t,e)>-1!==n})}function i(e,t){for(

C:\Users\user\AppData\Local\Temp\~DF1B7ED03EDF86E566.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	1.551027638273437
Encrypted:	false
SSDEEP:	96:kBqoxDhHWSVSE+FO/m8LwojM0Jp5I8hYPhJzWPY2Sw3wMlKgaK9Pok:kBqoxDhHjgE+W8ojM07JihCIUlXa+PL
MD5:	BA7A86006D12FA8C5CA956CCAA421C00
SHA1:	5826673C9536B1B5894890D58E39AAF118F1BCBA
SHA-256:	CB9555CA5D2EF49F515E309F47EAB8A9467DAE05FE559A483F7803ECF0122D5A
SHA-512:	211B291B6282FE0FA779D92DB0384FE2423B11253FCDDC955A2FC238D16F4C4824B19BF26A4C5FD808A3E711920B48AF8710C171E5CE36FC10C54A9E3337CAC
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF28746C75DF5CE9A2.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	36221
Entropy (8bit):	0.6282587553519693

C:\Users\user\AppData\Local\Temp\~DF28746C75DF5CE9A2.TMP	
Encrypted:	false
SSDEEP:	48:kBqoxKAuvScS+CkuHLILXVK5mwim+RqhW0:kBqoxKAuvScS+CkuH0zOR/
MD5:	2373D12694F06CF3440AC388A830B1D0
SHA1:	F7AB67E7DD87C588F7187FF6A702224229D3EFC1
SHA-256:	74CE9E2383B04F2C3F4313CAD9CB4E10D07DAF80810911FB903F3995E1144109
SHA-512:	72D6B61A407AAD385EB4F635CBC740D514F46FAF0E6B4E436F92924B7B3F187F2039D9EF5E11F1D5A9FFB02C28D7B8AB0197511EF324E095E12EE19A04CBB8E4
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF2E26229C26FB78DB.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13269
Entropy (8bit):	0.634966977599164
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lo+F9loC9lWnJZhNZJMJ55ZJNJxJbfJBFJv:kBqoIdbnJZhNZJMJ55ZJNJxJbfJzJv
MD5:	CA50CD71EBDCBF16B26A2474AFA8FC48
SHA1:	4D8B806767BD1B407BCFB60F2AF56F2A9AACE341
SHA-256:	C6F08CAADFEFFD015E33ABF950E29ADE00DACEEC81B9B1D54A042EE0AE0F37DF
SHA-512:	765FB23E9576D91348A68A010FA0B184B6A1C266044ED4763890C745DB307C9FC6B1C881046BA2D47DCD7FFD7842AC2E5E70058B8BC7D4D6F9E65745714255C
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

Static File Info

General

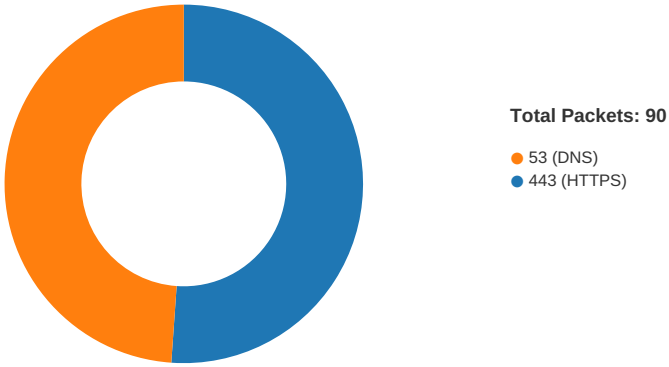
File type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Entropy (8bit):	3.294719207966508
TrID:	• HTML Application (8008/1) 100.00%
File name:	mfalomirm@gentalia.eu.HTM
File size:	8967
MD5:	ebe2a44409febe2a3347a115df136ae5
SHA1:	6cc7a3f83e3dbf63a537ffffc3ec2ef5ee8f2a66
SHA256:	8d4ef43acbf962dba319cacec0270b36df054e212d15f8de7e4eafd5dcda5d47
SHA512:	4643156b9c2f25f4f65b5894be9a293e4c7f06e6c4c7cfbbf4bc7b8a1ed24fde6bd9e1b073fa046634572b6ad8c74a7b03d1e462a2dc66b494e4f86d1c43a0c7
SSDEEP:	192:Lao8koMR6Kmb5a1xLu4wFu4C4UHxHBJF7IP000g:xNo49x1xLIAHxBJY
File Content Preview:	<script>document.write(unescape('%3C%21%44%4F%43%54%59%50%45%20%68%74%6D%6C%3E%0A%3C%68%74%6D%6C%20%6C%61%6E%67%3D%27%65%6E%2D%55%53%27%20%78%6D%6C%3A%6C%61%6E%67%3D%27%65%6E%2D%55%53%27%20%78%6D%6C%6E%73%3D%27%68%74%74%70%3A%2F%2F%77%77%77%2E%77%33%2E%6F

File Icon

Icon Hash:	f8c89c9a9a998cb8

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 11:05:44.895675898 CEST	49706	443	192.168.2.3	35.185.32.151
Apr 12, 2021 11:05:44.895828962 CEST	49705	443	192.168.2.3	35.185.32.151
Apr 12, 2021 11:05:45.029762983 CEST	443	49705	35.185.32.151	192.168.2.3
Apr 12, 2021 11:05:45.029863119 CEST	49705	443	192.168.2.3	35.185.32.151
Apr 12, 2021 11:05:45.029959917 CEST	443	49706	35.185.32.151	192.168.2.3
Apr 12, 2021 11:05:45.030050993 CEST	49706	443	192.168.2.3	35.185.32.151
Apr 12, 2021 11:05:45.035504103 CEST	49706	443	192.168.2.3	35.185.32.151
Apr 12, 2021 11:05:45.035684109 CEST	49705	443	192.168.2.3	35.185.32.151
Apr 12, 2021 11:05:45.169836044 CEST	443	49705	35.185.32.151	192.168.2.3
Apr 12, 2021 11:05:45.169886112 CEST	443	49706	35.185.32.151	192.168.2.3
Apr 12, 2021 11:05:45.171405077 CEST	443	49706	35.185.32.151	192.168.2.3
Apr 12, 2021 11:05:45.171432018 CEST	443	49706	35.185.32.151	192.168.2.3
Apr 12, 2021 11:05:45.171443939 CEST	443	49706	35.185.32.151	192.168.2.3
Apr 12, 2021 11:05:45.171510935 CEST	49706	443	192.168.2.3	35.185.32.151
Apr 12, 2021 11:05:45.171535969 CEST	49706	443	192.168.2.3	35.185.32.151
Apr 12, 2021 11:05:45.172306061 CEST	443	49705	35.185.32.151	192.168.2.3
Apr 12, 2021 11:05:45.172329903 CEST	443	49705	35.185.32.151	192.168.2.3
Apr 12, 2021 11:05:45.172343016 CEST	443	49705	35.185.32.151	192.168.2.3
Apr 12, 2021 11:05:45.172385931 CEST	49705	443	192.168.2.3	35.185.32.151
Apr 12, 2021 11:05:45.172426939 CEST	49705	443	192.168.2.3	35.185.32.151
Apr 12, 2021 11:05:45.208650112 CEST	49706	443	192.168.2.3	35.185.32.151
Apr 12, 2021 11:05:45.212487936 CEST	49705	443	192.168.2.3	35.185.32.151
Apr 12, 2021 11:05:45.214452028 CEST	49706	443	192.168.2.3	35.185.32.151
Apr 12, 2021 11:05:45.214580059 CEST	49705	443	192.168.2.3	35.185.32.151
Apr 12, 2021 11:05:45.214642048 CEST	49706	443	192.168.2.3	35.185.32.151
Apr 12, 2021 11:05:45.343369961 CEST	443	49706	35.185.32.151	192.168.2.3
Apr 12, 2021 11:05:45.343403101 CEST	443	49706	35.185.32.151	192.168.2.3
Apr 12, 2021 11:05:45.343571901 CEST	49706	443	192.168.2.3	35.185.32.151
Apr 12, 2021 11:05:45.344294071 CEST	49706	443	192.168.2.3	35.185.32.151
Apr 12, 2021 11:05:45.346874952 CEST	443	49705	35.185.32.151	192.168.2.3
Apr 12, 2021 11:05:45.346932888 CEST	443	49705	35.185.32.151	192.168.2.3
Apr 12, 2021 11:05:45.346982956 CEST	49705	443	192.168.2.3	35.185.32.151
Apr 12, 2021 11:05:45.347012997 CEST	49705	443	192.168.2.3	35.185.32.151
Apr 12, 2021 11:05:45.347609997 CEST	49705	443	192.168.2.3	35.185.32.151
Apr 12, 2021 11:05:45.348727942 CEST	443	49706	35.185.32.151	192.168.2.3
Apr 12, 2021 11:05:45.352408886 CEST	443	49706	35.185.32.151	192.168.2.3
Apr 12, 2021 11:05:45.352433920 CEST	443	49706	35.185.32.151	192.168.2.3
Apr 12, 2021 11:05:45.352448940 CEST	443	49705	35.185.32.151	192.168.2.3
Apr 12, 2021 11:05:45.352467060 CEST	443	49706	35.185.32.151	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 11:05:45.352483034 CEST	443	49706	35.185.32.151	192.168.2.3
Apr 12, 2021 11:05:45.352499962 CEST	443	49706	35.185.32.151	192.168.2.3
Apr 12, 2021 11:05:45.352504015 CEST	49706	443	192.168.2.3	35.185.32.151
Apr 12, 2021 11:05:45.352516890 CEST	443	49706	35.185.32.151	192.168.2.3
Apr 12, 2021 11:05:45.352526903 CEST	49706	443	192.168.2.3	35.185.32.151
Apr 12, 2021 11:05:45.352538109 CEST	443	49706	35.185.32.151	192.168.2.3
Apr 12, 2021 11:05:45.352551937 CEST	49705	443	192.168.2.3	35.185.32.151
Apr 12, 2021 11:05:45.352555990 CEST	443	49706	35.185.32.151	192.168.2.3
Apr 12, 2021 11:05:45.352564096 CEST	49706	443	192.168.2.3	35.185.32.151
Apr 12, 2021 11:05:45.352586031 CEST	49706	443	192.168.2.3	35.185.32.151
Apr 12, 2021 11:05:45.352605104 CEST	49706	443	192.168.2.3	35.185.32.151
Apr 12, 2021 11:05:45.477826118 CEST	443	49706	35.185.32.151	192.168.2.3
Apr 12, 2021 11:05:45.477880001 CEST	443	49706	35.185.32.151	192.168.2.3
Apr 12, 2021 11:05:45.477905035 CEST	443	49706	35.185.32.151	192.168.2.3
Apr 12, 2021 11:05:45.477931023 CEST	443	49706	35.185.32.151	192.168.2.3
Apr 12, 2021 11:05:45.478030920 CEST	49706	443	192.168.2.3	35.185.32.151
Apr 12, 2021 11:05:45.478074074 CEST	49706	443	192.168.2.3	35.185.32.151
Apr 12, 2021 11:05:45.486723900 CEST	443	49706	35.185.32.151	192.168.2.3
Apr 12, 2021 11:05:45.486831903 CEST	443	49706	35.185.32.151	192.168.2.3
Apr 12, 2021 11:05:45.486901999 CEST	443	49706	35.185.32.151	192.168.2.3
Apr 12, 2021 11:05:45.486913919 CEST	49706	443	192.168.2.3	35.185.32.151
Apr 12, 2021 11:05:45.486948967 CEST	49706	443	192.168.2.3	35.185.32.151
Apr 12, 2021 11:05:45.486963034 CEST	49706	443	192.168.2.3	35.185.32.151
Apr 12, 2021 11:05:45.486964941 CEST	443	49706	35.185.32.151	192.168.2.3
Apr 12, 2021 11:05:45.487019062 CEST	49706	443	192.168.2.3	35.185.32.151
Apr 12, 2021 11:05:45.487025023 CEST	443	49706	35.185.32.151	192.168.2.3
Apr 12, 2021 11:05:45.487073898 CEST	443	49706	35.185.32.151	192.168.2.3
Apr 12, 2021 11:05:45.487124920 CEST	443	49706	35.185.32.151	192.168.2.3
Apr 12, 2021 11:05:45.487162113 CEST	49706	443	192.168.2.3	35.185.32.151
Apr 12, 2021 11:05:45.487166882 CEST	443	49706	35.185.32.151	192.168.2.3
Apr 12, 2021 11:05:45.487171888 CEST	49706	443	192.168.2.3	35.185.32.151
Apr 12, 2021 11:05:45.487174988 CEST	49706	443	192.168.2.3	35.185.32.151
Apr 12, 2021 11:05:45.487205982 CEST	443	49706	35.185.32.151	192.168.2.3
Apr 12, 2021 11:05:45.487240076 CEST	49706	443	192.168.2.3	35.185.32.151
Apr 12, 2021 11:05:45.487246990 CEST	443	49706	35.185.32.151	192.168.2.3
Apr 12, 2021 11:05:45.487276077 CEST	49706	443	192.168.2.3	35.185.32.151
Apr 12, 2021 11:05:45.487286091 CEST	443	49706	35.185.32.151	192.168.2.3
Apr 12, 2021 11:05:45.487319946 CEST	49706	443	192.168.2.3	35.185.32.151
Apr 12, 2021 11:05:45.487323999 CEST	443	49706	35.185.32.151	192.168.2.3
Apr 12, 2021 11:05:45.487358093 CEST	49706	443	192.168.2.3	35.185.32.151
Apr 12, 2021 11:05:45.487363100 CEST	443	49706	35.185.32.151	192.168.2.3
Apr 12, 2021 11:05:45.487390995 CEST	49706	443	192.168.2.3	35.185.32.151
Apr 12, 2021 11:05:45.487402916 CEST	443	49706	35.185.32.151	192.168.2.3
Apr 12, 2021 11:05:45.487432003 CEST	49706	443	192.168.2.3	35.185.32.151
Apr 12, 2021 11:05:45.487447023 CEST	443	49706	35.185.32.151	192.168.2.3
Apr 12, 2021 11:05:45.487485886 CEST	49706	443	192.168.2.3	35.185.32.151
Apr 12, 2021 11:05:45.487536907 CEST	49706	443	192.168.2.3	35.185.32.151
Apr 12, 2021 11:05:45.524553061 CEST	443	49705	35.185.32.151	192.168.2.3
Apr 12, 2021 11:05:45.668494940 CEST	49706	443	192.168.2.3	35.185.32.151
Apr 12, 2021 11:05:45.831444025 CEST	443	49706	35.185.32.151	192.168.2.3
Apr 12, 2021 11:05:45.831598997 CEST	49706	443	192.168.2.3	35.185.32.151
Apr 12, 2021 11:05:45.834902048 CEST	49706	443	192.168.2.3	35.185.32.151
Apr 12, 2021 11:05:45.973773003 CEST	443	49706	35.185.32.151	192.168.2.3
Apr 12, 2021 11:05:45.973808050 CEST	443	49706	35.185.32.151	192.168.2.3
Apr 12, 2021 11:05:45.973820925 CEST	443	49706	35.185.32.151	192.168.2.3
Apr 12, 2021 11:05:45.973833084 CEST	443	49706	35.185.32.151	192.168.2.3
Apr 12, 2021 11:05:45.973854065 CEST	443	49706	35.185.32.151	192.168.2.3
Apr 12, 2021 11:05:45.973871946 CEST	443	49706	35.185.32.151	192.168.2.3
Apr 12, 2021 11:05:45.973887920 CEST	443	49706	35.185.32.151	192.168.2.3
Apr 12, 2021 11:05:45.973905087 CEST	443	49706	35.185.32.151	192.168.2.3
Apr 12, 2021 11:05:45.973921061 CEST	443	49706	35.185.32.151	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 11:05:36.164710999 CEST	57544	53	192.168.2.3	8.8.8.8
Apr 12, 2021 11:05:36.225663900 CEST	53	57544	8.8.8.8	192.168.2.3
Apr 12, 2021 11:05:43.005655050 CEST	55984	53	192.168.2.3	8.8.8.8
Apr 12, 2021 11:05:43.066235065 CEST	53	55984	8.8.8.8	192.168.2.3
Apr 12, 2021 11:05:44.824978113 CEST	64185	53	192.168.2.3	8.8.8.8
Apr 12, 2021 11:05:44.885303020 CEST	53	64185	8.8.8.8	192.168.2.3
Apr 12, 2021 11:05:46.408926010 CEST	65110	53	192.168.2.3	8.8.8.8
Apr 12, 2021 11:05:46.469491005 CEST	53	65110	8.8.8.8	192.168.2.3
Apr 12, 2021 11:05:47.027865887 CEST	58361	53	192.168.2.3	8.8.8.8
Apr 12, 2021 11:05:47.076697111 CEST	53	58361	8.8.8.8	192.168.2.3
Apr 12, 2021 11:05:48.026350021 CEST	63492	53	192.168.2.3	8.8.8.8
Apr 12, 2021 11:05:48.075149059 CEST	53	63492	8.8.8.8	192.168.2.3
Apr 12, 2021 11:06:01.217040062 CEST	60831	53	192.168.2.3	8.8.8.8
Apr 12, 2021 11:06:01.275831938 CEST	53	60831	8.8.8.8	192.168.2.3
Apr 12, 2021 11:06:12.140897989 CEST	60100	53	192.168.2.3	8.8.8.8
Apr 12, 2021 11:06:12.192866087 CEST	53	60100	8.8.8.8	192.168.2.3
Apr 12, 2021 11:06:12.576720953 CEST	53195	53	192.168.2.3	8.8.8.8
Apr 12, 2021 11:06:12.625663042 CEST	53	53195	8.8.8.8	192.168.2.3
Apr 12, 2021 11:06:13.024738073 CEST	50141	53	192.168.2.3	8.8.8.8
Apr 12, 2021 11:06:13.085149050 CEST	53	50141	8.8.8.8	192.168.2.3
Apr 12, 2021 11:06:14.018980980 CEST	50141	53	192.168.2.3	8.8.8.8
Apr 12, 2021 11:06:14.040183067 CEST	53023	53	192.168.2.3	8.8.8.8
Apr 12, 2021 11:06:14.079072952 CEST	53	50141	8.8.8.8	192.168.2.3
Apr 12, 2021 11:06:14.088865042 CEST	53	53023	8.8.8.8	192.168.2.3
Apr 12, 2021 11:06:14.659295082 CEST	49563	53	192.168.2.3	8.8.8.8
Apr 12, 2021 11:06:14.745630026 CEST	53	49563	8.8.8.8	192.168.2.3
Apr 12, 2021 11:06:15.062937975 CEST	53023	53	192.168.2.3	8.8.8.8
Apr 12, 2021 11:06:15.090401888 CEST	50141	53	192.168.2.3	8.8.8.8
Apr 12, 2021 11:06:15.119807005 CEST	53	53023	8.8.8.8	192.168.2.3
Apr 12, 2021 11:06:15.150537968 CEST	53	50141	8.8.8.8	192.168.2.3
Apr 12, 2021 11:06:16.065526962 CEST	53023	53	192.168.2.3	8.8.8.8
Apr 12, 2021 11:06:16.122757912 CEST	53	53023	8.8.8.8	192.168.2.3
Apr 12, 2021 11:06:17.117046118 CEST	50141	53	192.168.2.3	8.8.8.8
Apr 12, 2021 11:06:17.168587923 CEST	53	50141	8.8.8.8	192.168.2.3
Apr 12, 2021 11:06:18.081532955 CEST	53023	53	192.168.2.3	8.8.8.8
Apr 12, 2021 11:06:18.141105890 CEST	53	53023	8.8.8.8	192.168.2.3
Apr 12, 2021 11:06:18.707266092 CEST	51352	53	192.168.2.3	8.8.8.8
Apr 12, 2021 11:06:18.760081053 CEST	53	51352	8.8.8.8	192.168.2.3
Apr 12, 2021 11:06:19.967436075 CEST	59349	53	192.168.2.3	8.8.8.8
Apr 12, 2021 11:06:20.031102896 CEST	53	59349	8.8.8.8	192.168.2.3
Apr 12, 2021 11:06:21.128561974 CEST	50141	53	192.168.2.3	8.8.8.8
Apr 12, 2021 11:06:21.182214975 CEST	53	50141	8.8.8.8	192.168.2.3
Apr 12, 2021 11:06:21.186840057 CEST	57084	53	192.168.2.3	8.8.8.8
Apr 12, 2021 11:06:21.250566006 CEST	53	57084	8.8.8.8	192.168.2.3
Apr 12, 2021 11:06:22.097186089 CEST	53023	53	192.168.2.3	8.8.8.8
Apr 12, 2021 11:06:22.154308081 CEST	53	53023	8.8.8.8	192.168.2.3
Apr 12, 2021 11:06:22.456798077 CEST	58823	53	192.168.2.3	8.8.8.8
Apr 12, 2021 11:06:22.516343117 CEST	53	58823	8.8.8.8	192.168.2.3
Apr 12, 2021 11:06:23.282768965 CEST	57568	53	192.168.2.3	8.8.8.8
Apr 12, 2021 11:06:23.341373920 CEST	53	57568	8.8.8.8	192.168.2.3
Apr 12, 2021 11:06:29.805732965 CEST	50540	53	192.168.2.3	8.8.8.8
Apr 12, 2021 11:06:29.864653111 CEST	53	50540	8.8.8.8	192.168.2.3
Apr 12, 2021 11:06:30.829356909 CEST	54366	53	192.168.2.3	8.8.8.8
Apr 12, 2021 11:06:30.878025055 CEST	53	54366	8.8.8.8	192.168.2.3
Apr 12, 2021 11:06:38.378586054 CEST	53034	53	192.168.2.3	8.8.8.8
Apr 12, 2021 11:06:38.430288076 CEST	53	53034	8.8.8.8	192.168.2.3
Apr 12, 2021 11:06:39.184587002 CEST	57762	53	192.168.2.3	8.8.8.8
Apr 12, 2021 11:06:39.236407995 CEST	53	57762	8.8.8.8	192.168.2.3
Apr 12, 2021 11:06:39.992520094 CEST	55435	53	192.168.2.3	8.8.8.8
Apr 12, 2021 11:06:40.049843073 CEST	53	55435	8.8.8.8	192.168.2.3
Apr 12, 2021 11:06:40.794567108 CEST	50713	53	192.168.2.3	8.8.8.8
Apr 12, 2021 11:06:40.844032049 CEST	53	50713	8.8.8.8	192.168.2.3
Apr 12, 2021 11:06:42.090018034 CEST	56132	53	192.168.2.3	8.8.8.8
Apr 12, 2021 11:06:42.142421961 CEST	53	56132	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 11:06:46.088289976 CEST	58987	53	192.168.2.3	8.8.8.8
Apr 12, 2021 11:06:46.159375906 CEST	53	58987	8.8.8.8	192.168.2.3
Apr 12, 2021 11:06:47.519130945 CEST	56579	53	192.168.2.3	8.8.8.8
Apr 12, 2021 11:06:47.567908049 CEST	53	56579	8.8.8.8	192.168.2.3
Apr 12, 2021 11:06:53.950035095 CEST	60633	53	192.168.2.3	8.8.8.8
Apr 12, 2021 11:06:53.998878002 CEST	53	60633	8.8.8.8	192.168.2.3
Apr 12, 2021 11:06:57.763751030 CEST	61292	53	192.168.2.3	8.8.8.8
Apr 12, 2021 11:06:57.825226068 CEST	53	61292	8.8.8.8	192.168.2.3
Apr 12, 2021 11:07:06.212263107 CEST	63619	53	192.168.2.3	8.8.8.8
Apr 12, 2021 11:07:06.261131048 CEST	53	63619	8.8.8.8	192.168.2.3
Apr 12, 2021 11:07:08.141169071 CEST	64938	53	192.168.2.3	8.8.8.8
Apr 12, 2021 11:07:08.192800045 CEST	53	64938	8.8.8.8	192.168.2.3
Apr 12, 2021 11:07:09.514235020 CEST	61946	53	192.168.2.3	8.8.8.8
Apr 12, 2021 11:07:09.563199043 CEST	53	61946	8.8.8.8	192.168.2.3
Apr 12, 2021 11:07:10.599459887 CEST	64910	53	192.168.2.3	8.8.8.8
Apr 12, 2021 11:07:10.657047033 CEST	53	64910	8.8.8.8	192.168.2.3
Apr 12, 2021 11:07:11.770838022 CEST	52123	53	192.168.2.3	8.8.8.8
Apr 12, 2021 11:07:11.820852041 CEST	53	52123	8.8.8.8	192.168.2.3
Apr 12, 2021 11:07:12.622142076 CEST	56130	53	192.168.2.3	8.8.8.8
Apr 12, 2021 11:07:12.672322989 CEST	53	56130	8.8.8.8	192.168.2.3
Apr 12, 2021 11:07:28.858005047 CEST	56338	53	192.168.2.3	8.8.8.8
Apr 12, 2021 11:07:28.907083988 CEST	53	56338	8.8.8.8	192.168.2.3
Apr 12, 2021 11:07:30.523232937 CEST	59420	53	192.168.2.3	8.8.8.8
Apr 12, 2021 11:07:30.588737011 CEST	53	59420	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 12, 2021 11:05:44.824978113 CEST	192.168.2.3	8.8.8.8	0x7e39	Standard query (0)	ast.samanage.com	A (IP address)	IN (0x0001)
Apr 12, 2021 11:05:46.408926010 CEST	192.168.2.3	8.8.8.8	0xbfe	Standard query (0)	www.apkmirror.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 12, 2021 11:05:44.885303020 CEST	8.8.8.8	192.168.2.3	0x7e39	No error (0)	ast.samanage.com		35.185.32.151	A (IP address)	IN (0x0001)
Apr 12, 2021 11:05:46.469491005 CEST	8.8.8.8	192.168.2.3	0xbfe	No error (0)	www.apkmirror.com		104.19.133.58	A (IP address)	IN (0x0001)
Apr 12, 2021 11:05:46.469491005 CEST	8.8.8.8	192.168.2.3	0xbfe	No error (0)	www.apkmirror.com		104.19.132.58	A (IP address)	IN (0x0001)
Apr 12, 2021 11:05:46.469491005 CEST	8.8.8.8	192.168.2.3	0xbfe	No error (0)	www.apkmirror.com		104.19.136.58	A (IP address)	IN (0x0001)
Apr 12, 2021 11:05:46.469491005 CEST	8.8.8.8	192.168.2.3	0xbfe	No error (0)	www.apkmirror.com		104.19.134.58	A (IP address)	IN (0x0001)
Apr 12, 2021 11:05:46.469491005 CEST	8.8.8.8	192.168.2.3	0xbfe	No error (0)	www.apkmirror.com		104.19.135.58	A (IP address)	IN (0x0001)

HTTPS Packets

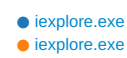
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 12, 2021 11:05:45.171432018 CEST	35.185.32.151	443	192.168.2.3	49706	CN=*.samanage.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sun Feb 07 14:01:27 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Sat May 08 15:01:27 CEST 2021 Wed Sep 29 21:21:40 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

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Apr 12, 2021 11:05:45.172329903 CEST	35.185.32.151	443	192.168.2.3	49705	CN=*.samanage.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sun Feb 07 14:01:27 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Sat May 08 15:01:27 CEST 2021 Wed Sep 29 21:21:40 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=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Apr 12, 2021 11:05:46.579402924 CEST	104.19.133.58	443	192.168.2.3	49707	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Thu Aug 06 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Fri Aug 06 14:00:00 CEST 2021 Wed Jan 01 00:59:59 CET 2025	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=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Apr 12, 2021 11:05:46.580859900 CEST	104.19.133.58	443	192.168.2.3	49708	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Thu Aug 06 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Fri Aug 06 14:00:00 CEST 2021 Wed Jan 01 00:59:59 CET 2025	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=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 5280 Parent PID: 792

General

Start time:	11:05:42
Start date:	12/04/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff617aa0000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: iexplore.exe PID: 3892 Parent PID: 5280

General

Start time:	11:05:42
Start date:	12/04/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5280 CREDAT:17410 /prefetch:2
Imagebase:	0x10000
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