ID: 384636
Cookbook: browseurl.jbs
Time: 15:12:58
Date: 09/04/2021
Version: 31.0.0 Emerald

Table of Contents

Copyright Joe Security LLC 2021

Copyright Joe Security LLC 2021

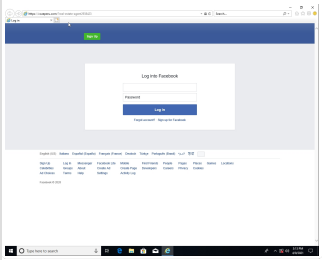
Analysis Report https://ccaeperu.com/?real-estate-agen…

Overview

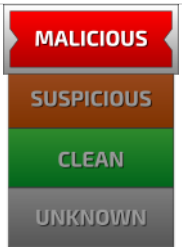
General Information

Sample URL:	http://https://ccaeperu.com/?real-estate-agent2938423
Analysis ID:	384636
Infos:	

Most interesting Screenshot:



Detection



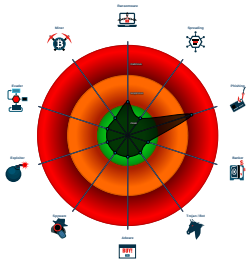
HTMLPhisher

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

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for URL or domain
- Yara detected HtmlPhish10
- HTML title does not match URL

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 4828 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 1576 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4828 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\VBLSBCBU.htm	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\B0LQ5SBH.htm	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\9HQ2AZB5.htm	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\6LTWT96P.htm	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\G1MK1W1S.htm	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	

Click to see the 10 entries

Sigma Overview

Copyright Joe Security LLC 2021

No Sigma rule has matched

Signature Overview

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

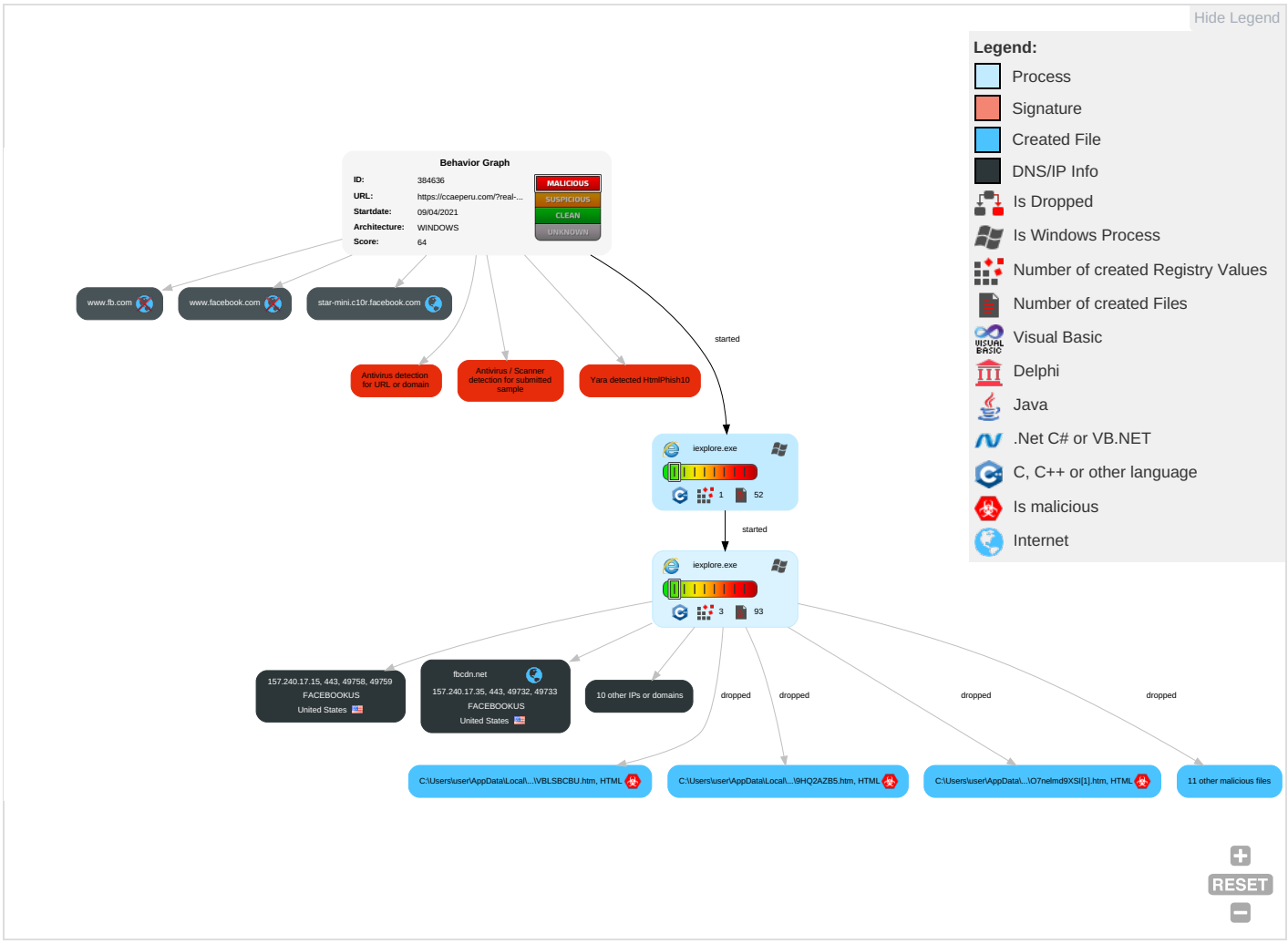
Phishing:

Yara detected HtmlPhish10

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	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delet Devic Data

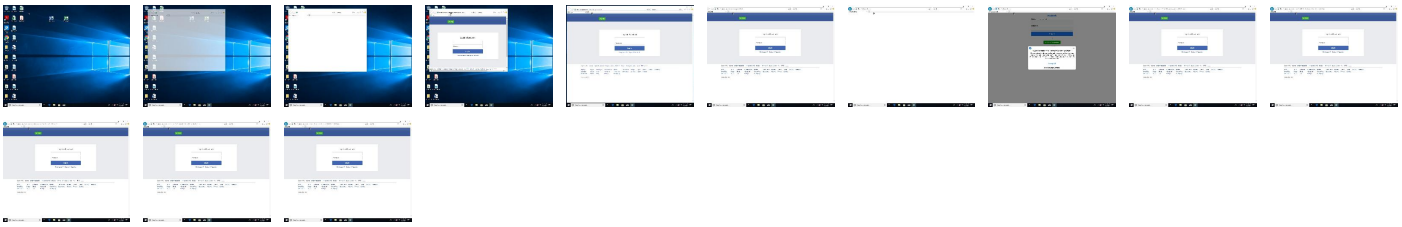
Behavior Graph

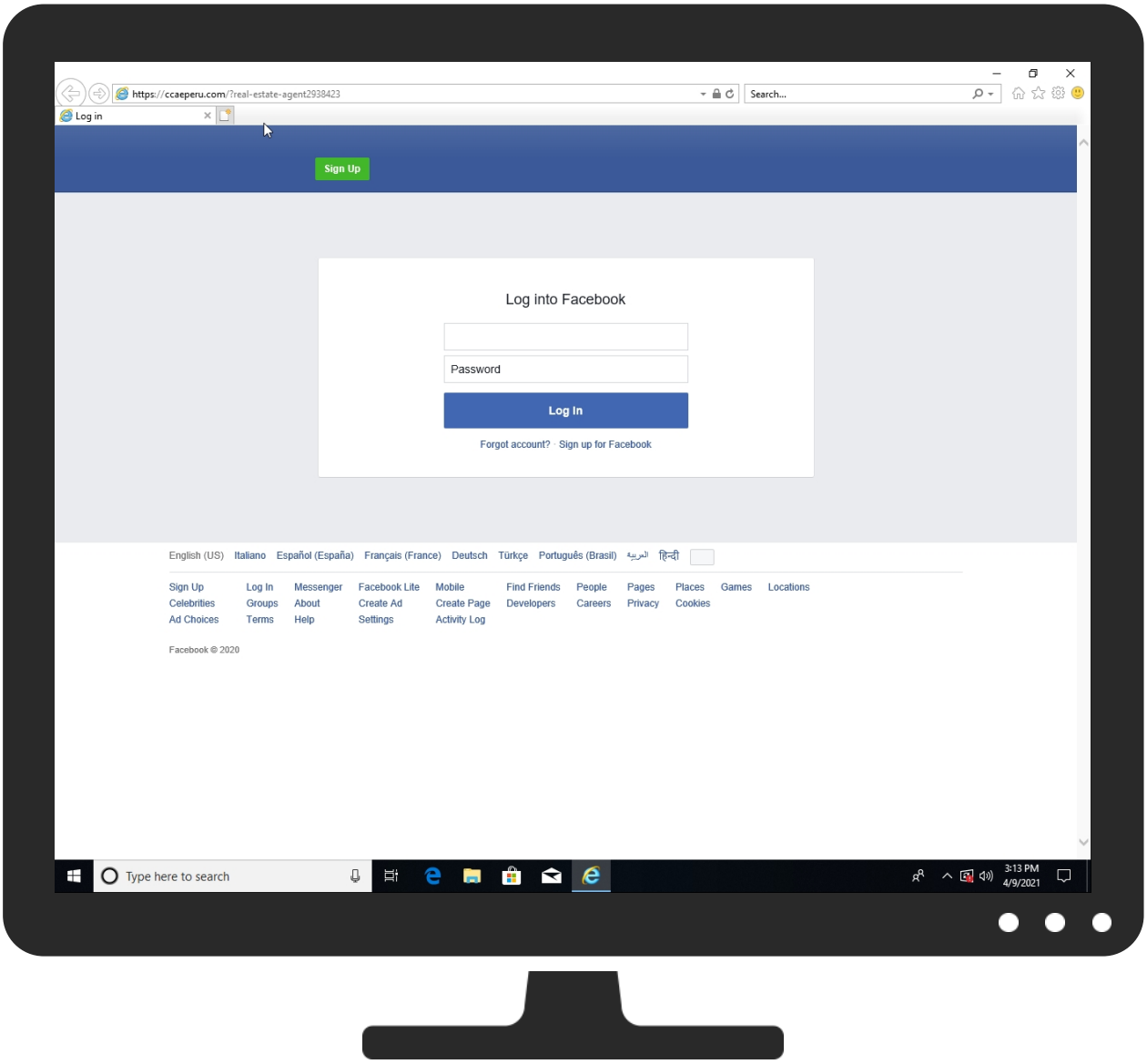


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://ccaeperu.com/?real-estate-agent2938423	0%	Avira URL Cloud	safe	
http://https://ccaeperu.com/?real-estate-agent2938423	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link

Copyright Joe Security LLC 2021

Source	Detection	Scanner	Label	Link
http://https://ccaeperu.com/?cmd=svnv9tsbx9tbsttsnxbtbnt.mynxy1vytby81nv1mb1v.b1ms9s	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://https://ccaeperu.com/r.php?locale=en_US	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://https://ccaeperu.com/?cmd=bnvtbtxmsbx1vy11snsm8nx8smbbmy8x8snns.8tm99yn88xtvv	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://https://ccaeperu.com/r.php?locale=en_US	100%	UrlScan	phishing brand: facebook	Browse
http://https://ccaeperu.com/?cmd=9tyym8t91xbt8b81mt81smbbm1s.9vtn8ytms1v9vvy8198118b	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://https://ccaeperu.com/?cmd=xbsmyynyy.8y18y8tvmsstm1ntysyxmx.ty.1xtxsm9bs8s88n8	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://https://ccaeperu.com/?cmd=xbsmyynyy.8y18y8tvmsstm1ntysyxmx.ty.1xtxsm9bs8s88n8	100%	UrlScan	phishing brand: facebook	Browse
http://https://ccaeperu.com/?cmd=m9xvsybnvn1sv.bsnmnsyx119yb8mx1yv88sst1s8sxsv11nt.t	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://https://ccaeperu.com/?cmd=vt9n.n11981t1t8b1t1xm1msm.s9tsxxssy9tstt1t8nsb.y1ms	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://https://ccaeperu.com/?cmd=9tyym8t91xbt8b81mt81smbbm1s.9vtn8ytms1v9vvy8198118b	100%	UrlScan	phishing brand: facebook	Browse
http://https://ccaeperu.com/?cmd=t8ntyxt9mnn.9.t9t1ns9tnb11.n9tttbstxsmt91bmnsb8xts1	100%	UrlScan	phishing brand: facebook	Browse
http://https://ccaeperu.com/?cmd=t8ntyxt9mnn.9.t9t1ns9tnb11.n9tttbstxsmt91bmnsb8xts1	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://https://ccaeperu.com/?cmd=stmn8bymn1v1.18svn81tv1ymtxtxy1ymns8y1vt81b.9nty9s8	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://https://ccaeperu.com/?cmd=m9xvsybnvn1sv.bsnmnsyx119yb8mx1yv88sst1s8sxsv11nt.t	100%	UrlScan	phishing brand: facebook	Browse
http://https://ccaeperu.com/?cmd=stmn8bymn1v1.18svn81tv1ymtxtxy1ymns8y1vt81b.9nty9s8	100%	UrlScan	phishing brand: facebook	Browse
http://https://ccaeperu.com/?cmd=snstmsbsvtx.s1.smysttx.sv11m9ss9xbtb1mvmmytn9t1tyny	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://https://ccaeperu.com/?cmd=snstmsbsvtx.s1.smysttx.sv11m9ss9xbtb1mvmmytn9t1tyny	100%	UrlScan	phishing brand: facebook	Browse
http://https://ccaeperu.com/?cmd=vt9n.n11981t1t8b1t1xm1msm.s9tsxxssy9tstt1t8nsb.y1ms	100%	UrlScan	phishing brand: facebook	Browse
http://https://ccaeperu.com/?real-estate-agent2938423//-estate-agent2938423Root	0%	Avira URL Cloud	safe	
http://https://ccaeperu.com/?real-estate-agent2938423om/-estate-agent2938423Root	0%	Avira URL Cloud	safe	
http://https://ccaeperu.com/?	0%	Avira URL Cloud	safe	
http://https://ccaeperu.com/?real-estate-agent2938423cmd=9tyym8t91xbt8b81mt81smbbm1s.	0%	Avira URL Cloud	safe	
http://https://ccaeperu.com/?real-estate-agent2938423cmd=bnvtbtxmsbx1vy11snsm8nx8smbb	0%	Avira URL Cloud	safe	
http://https://www.internalfb.com/intern/invariant/	0%	URL Reputation	safe	
http://https://www.internalfb.com/intern/invariant/	0%	URL Reputation	safe	
http://https://www.internalfb.com/intern/invariant/	0%	URL Reputation	safe	
http://https://ccaeperu.com/?real-estate-agent2938423cmd=m9xvsybnvn1sv.bsnmnsyx119yb8	0%	Avira URL Cloud	safe	
http://https://ccaeperu.com/?real-estate-agent2938423cmd=vt9n.n11981t1t8b1t1xm1msm.s9	0%	Avira URL Cloud	safe	
http://https://ccaeperu.com/?real-estate-agent2938423cmd=stmn8bymn1v1.18svn81tv1ymtxt	0%	Avira URL Cloud	safe	
http://https://ccaeperu.com/?real-estate-agent2938423~	0%	Avira URL Cloud	safe	
http://https://www.facebook.creal-estate-agent2938423~	0%	Avira URL Cloud	safe	
http://https://ccaeperu.com/r	0%	Avira URL Cloud	safe	
http://https://ccaeperu.com/?real-estate-agent2938423Root	0%	Avira URL Cloud	safe	
http://https://ccaeperu.com/?real-estate-agent2938423cmd=svnv9tsbx9tbsttsnxbtbnt.mynx	0%	Avira URL Cloud	safe	
http://https://ccaeperu.com/?real-estate-agent2938423cmd=t8ntyxt9mnn.9.t9t1ns9tnb11.n	0%	Avira URL Cloud	safe	
http://https://www.facebook.c	0%	URL Reputation	safe	
http://https://www.facebook.c	0%	URL Reputation	safe	
http://https://www.facebook.c	0%	URL Reputation	safe	
http://https://ccaeperu.com/?real-estate-agent2938423cmd=xbsmyynyy.8y18y8tvmsstm1ntys	0%	Avira URL Cloud	safe	
http://https://ccaeperu.com/?real-estate-agent2938423cmd=snstmsbsvtx.s1.smysttx.sv11m	0%	Avira URL Cloud	safe	

Copyright Joe Security LLC 2021

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
star-mini.c10r.facebook.com	157.240.17.35	true	false		high
fbsbx.com	157.240.17.35	true	false		high
scontent.xx.fbcdn.net	157.240.219.13	true	false		high
fb.com	157.240.17.35	true	false		high
facebook.com	157.240.17.35	true	false		high
fbcdn.net	157.240.17.35	true	false		high
ccaeperu.com	68.66.226.79	true	false		unknown
www.fb.com	unknown	unknown	false		high
www.facebook.com	unknown	unknown	false		high
m.facebook.com	unknown	unknown	false		high
static.xx.fbcdn.net	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://ccaeperu.com/?cmd=svnv9tsbx9tbsttsnxbtbnt.mynxy1vytby81nv1mb1v.b1ms9s	true	• SlashNext: Fake Login Page type: Phishing & Social Engineering	unknown
http://https://ccaeperu.com/?cmd=m9xvsybnvn1sv.bsnmnsyx119yb8mx1yv88sst1s8sxsv11nt.t	true	• 100%, UrlScan, Browse • SlashNext: Fake Login Page type: Phishing & Social Engineering	unknown
http://https://ccaeperu.com/?cmd=t8ntyxt9mnn.9.t9t1ns9tnb11.n9tttbstxsmt91bmnsb8xts1	true	• 100%, UrlScan, Browse • SlashNext: Fake Login Page type: Phishing & Social Engineering	unknown
http://https://ccaeperu.com/?cmd=vt9n.n11981t1t8b1t1xm1msm.s9tsxxssy9tstt1t8nsb.y1ms	true	• 100%, UrlScan, Browse • SlashNext: Fake Login Page type: Phishing & Social Engineering	unknown
http://https://ccaeperu.com/?cmd=xbsmyynyy.8y18y8tvmsstm1ntysyxmx.ty.1xtxsm9bs8s88n8	true	• 100%, UrlScan, Browse • SlashNext: Fake Login Page type: Phishing & Social Engineering	unknown
http://https://ccaeperu.com/?cmd=9tyym8t91xbt8b81mt81smbbm1s.9vtn8ytms1v9vvy8198118b	true	• 100%, UrlScan, Browse • SlashNext: Fake Login Page type: Phishing & Social Engineering	unknown
http://https://ccaeperu.com/?cmd=snstmsbsvtx.s1.smysttx.sv11m9ss9xbtb1mvmmytn9t1tyny	true	• 100%, UrlScan, Browse • SlashNext: Fake Login Page type: Phishing & Social Engineering	unknown
http://https://ccaeperu.com/?cmd=stmn8bymn1v1.18svn81tv1ymtxtxy1ymns8y1vt81b.9nty9s8	true	• 100%, UrlScan, Browse • SlashNext: Fake Login Page type: Phishing & Social Engineering	unknown
http://https://m.facebook.com/	false		high
http://https://ccaeperu.com/?cmd=bnvtbtxmsbx1vy11snsm8nx8smbbmy8x8snns.8tm99yn88xtvv	true	• SlashNext: Fake Login Page type: Phishing & Social Engineering	unknown
http://https://ccaeperu.com/?real-estate-agent2938423	true		unknown

URLs from Memory and Binaries

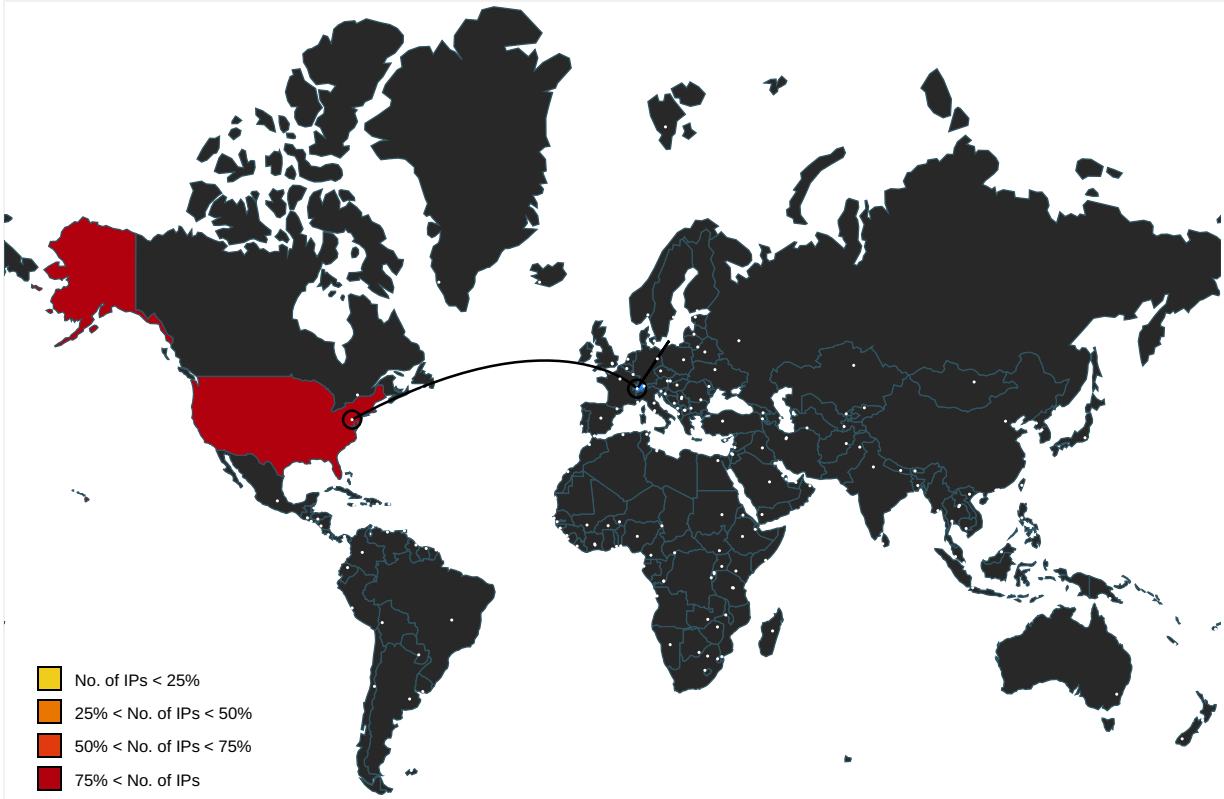
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://ccaeperu.com/?real-estate-agent2938423	{6767ACEF-9935-11EB-90EB-ECF4BBEA1588}.dat.1.dr	true		unknown
http://https://static.xx.fbcdn.net/rsrc.php/v3/yR/r/kPkP7qOaPwj.js?_nc_x=Ij3Wp8lg5Kz	B9RXHZ5I.htm.2.dr	false		high
http://https://ccaeperu.com/?real-estate-agent2938423//-estate-agent2938423Root	{6767ACEF-9935-11EB-90EB-ECF4BBEA1588}.dat.1.dr	true	• Avira URL Cloud: safe	unknown
http://https://static.xx.fbcdn.net/rsrc.php/v3/yT/l/0	B9RXHZ5I.htm.2.dr	false		high
http://https://ccaeperu.com/?cmd=svnv9tsbx9tbsttsnxbtbnt.mynxy1vytby81nv1mb1v.b1ms9s	{6767ACEF-9935-11EB-90EB-ECF4BBEA1588}.dat.1.dr, ~DF77662EBE27437295.TMP.1.dr	true	• SlashNext: Fake Login Page type: Phishing & Social Engineering	unknown
http://https://ccaeperu.com/?real-estate-agent2938423om/-estate-agent2938423Root	{6767ACEF-9935-11EB-90EB-ECF4BBEA1588}.dat.1.dr	true	• Avira URL Cloud: safe	unknown
http://https://ccaeperu.com/?	{6767ACEF-9935-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.fb.com/rsrc.php/yl/r/H3nktOa7ZMg.ico	9HQ2AZB5.htm.2.dr	false		high
http://https://ccaeperu.com/?real-estate-agent2938423cmd=9tyym8t91xbt8b81mt81smbbm1s.	{6767ACEF-9935-11EB-90EB-ECF4BBEA1588}.dat.1.dr	true	• Avira URL Cloud: safe	unknown
http://https://ccaeperu.com/?cmd=snstmsbsvtx.s1.smysttx.sv11m9ss9xbtb1mvmmytn9t1tyny	{6767ACEF-9935-11EB-90EB-ECF4BBEA1588}.dat.1.dr, ~DF77662EBE27437295.TMP.1.dr	true	• 100%, UrlScan, Browse • SlashNext: Fake Login Page type: Phishing & Social Engineering	unknown

Copyright Joe Security LLC 2021

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://ccaeperu.com/?real-estate-agent2938423cmd=bnvtbtxmsbx1vy11snsm8nx8smbb	{6767ACEF-9935-11EB-90EB-ECF4BBEA1588}.dat.1.dr	true	• Avira URL Cloud: safe	unknown
http://https://ccaeperu.com/?cmd=bnvtbtxmsbx1vy11snsm8nx8smbbmy8x8snns.8tm99yn88xtvv	{6767ACEF-9935-11EB-90EB-ECF4BBEA1588}.dat.1.dr, ~DF77662EBE27437295.TMP.1.dr	true	• SlashNext: Fake Login Page type: Phishing & Social Engineering	unknown
http://https://www.internalfb.com/intern/invariant/	VEs5hzVWt5B[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://static.xx.fbcdn.net/rsrc.php/v3/yj/l/0	B9RXHZ5I.htm.2.dr	false		high
http://https://ccaeperu.com/?cmd=t8ntyxt9mnn.9.t9t1ns9tnb11.n9tttbstxsmt91bmnsb8xts1	{6767ACEF-9935-11EB-90EB-ECF4BBEA1588}.dat.1.dr, ~DF77662EBE27437295.TMP.1.dr	true	• 100%, UrlScan, Browse • SlashNext: Fake Login Page type: Phishing & Social Engineering	unknown
http://https://static.xx.fbcdn.net/rsrc.php/v3/y5/l/0	B9RXHZ5I.htm.2.dr	false		high
http://https://static.xx.fbcdn.net/rsrc.php/v3/yU/r/fzkbB_w4sxK.js?_nc_x=Ij3Wp8lg5Kz	B9RXHZ5I.htm.2.dr	false		high
http://https://ccaeperu.com/?real-estate-agent2938423cmd=m9xvsybnvn1sv.bsnmnsyx119yb8	{6767ACEF-9935-11EB-90EB-ECF4BBEA1588}.dat.1.dr	true	• Avira URL Cloud: safe	unknown
http://https://static.xx.fbcdn.net/rsrc.php/v3/y6/l/0	B9RXHZ5I.htm.2.dr	false		high
http://https://fb.com/	9HQ2AZB5.htm.2.dr	false		high
http://https://static.xx.fbcdn.net/rsrc.php/v3/y7/r/qMrE4RFJBoQ.js?_nc_x=Ij3Wp8lg5Kz	B9RXHZ5I.htm.2.dr	false		high
http://https://developers.fb.com/?ref=pf	9HQ2AZB5.htm.2.dr, VBLSBCBU.htm.2.dr, O7nelmd9XSl[1].htm.2.dr, RUFPPAMX.htm.2.dr, r[1].htm.2.dr, RqQo1U5NOq1[1].htm.2.dr, B0LQ5SBH.htm.2.dr, 6LTWT96P.htm.2.dr, G1MK1W1S.htm.2.dr, favicon[1].htm.2.dr, 3GXKZCM3.htm.2.dr, HTQSVEM0.htm.2.dr, favicon[1].htm0.2.dr, A5FVZRWT.htm.2.dr, Z4A97TMF.htm.2.dr	false		high
http://https://static.xx.fbcdn.net/rsrc.php/v3iK-b4/yR/l/en_US/W5StuHxENhR.js?_nc_x=Ij3Wp8lg5Kz	B9RXHZ5I.htm.2.dr	false		high
http://https://ccaeperu.com/?real-estate-agent2938423cmd=vt9n.n11981t1t8b1t1xm1msm.s9	{6767ACEF-9935-11EB-90EB-ECF4BBEA1588}.dat.1.dr	true	• Avira URL Cloud: safe	unknown
http://https://static.xx.fbcdn.net/rsrc.php/v3/yP/l/0	B9RXHZ5I.htm.2.dr	false		high
http://https://ccaeperu.com/?real-estate-agent2938423cmd=stmn8bymn1v1.18svn81tv1ymtxt	{6767ACEF-9935-11EB-90EB-ECF4BBEA1588}.dat.1.dr	true	• Avira URL Cloud: safe	unknown
http://https://ccaeperu.com/?real-estate-agent2938423~	{6767ACEF-9935-11EB-90EB-ECF4BBEA1588}.dat.1.dr	true	• Avira URL Cloud: safe	unknown
http://https://www.facebook.creal-estate-agent2938423~	{6767ACEF-9935-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false	• Avira URL Cloud: safe	low
http://https://ccaeperu.com/r	{6767ACEF-9935-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://ccaeperu.com/?real-estate-agent2938423Root	{6767ACEF-9935-11EB-90EB-ECF4BBEA1588}.dat.1.dr	true	• Avira URL Cloud: safe	unknown
http://https://ccaeperu.com/?real-estate-agent2938423cmd=svnv9tsbx9tbsttsnxbtbnt.mynx	{6767ACEF-9935-11EB-90EB-ECF4BBEA1588}.dat.1.dr	true	• Avira URL Cloud: safe	unknown
http://https://static.xx.fbcdn.net/rsrc.php/v3/yb/l/0	B9RXHZ5I.htm.2.dr	false		high
http://https://ccaeperu.com/?cmd=xbsmyynyy.8y18y8tvmsstm1ntysyxmx.ty.1xtxsm9bs8s88n8	{6767ACEF-9935-11EB-90EB-ECF4BBEA1588}.dat.1.dr, ~DF77662EBE27437295.TMP.1.dr	true	• 100%, UrlScan, Browse • SlashNext: Fake Login Page type: Phishing & Social Engineering	unknown
http://https://ccaeperu.com/?real-estate-agent2938423cmd=t8ntyxt9mnn.9.t9t1ns9tnb11.n	{6767ACEF-9935-11EB-90EB-ECF4BBEA1588}.dat.1.dr	true	• Avira URL Cloud: safe	unknown
http://https://www.facebook.c	{6767ACEF-9935-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ccaeperu.com/?real-estate-agent2938423cmd=xbsmyynyy.8y18y8tvmsstm1ntys	{6767ACEF-9935-11EB-90EB-ECF4BBEA1588}.dat.1.dr	true	• Avira URL Cloud: safe	unknown
http://https://ccaeperu.com/?real-estate-agent2938423cmd=snstmsbsvtx.s1.smysttx.sv11m	{6767ACEF-9935-11EB-90EB-ECF4BBEA1588}.dat.1.dr	true	• Avira URL Cloud: safe	unknown
http://https://scontent.xx.fbcdn.net/hads-ak-prn2/1487645_6012475414660_1439393861_n.png	RpTFjVvO4D0[1].js.2.dr	false		high
http://https://ccaeperu.com/?cmd=vt9n.n11981t1t8b1t1xm1msm.s9tsxxssy9tstt1t8nsb.y1ms	{6767ACEF-9935-11EB-90EB-ECF4BBEA1588}.dat.1.dr, ~DF77662EBE27437295.TMP.1.dr	true	• 100%, UrlScan, Browse • SlashNext: Fake Login Page type: Phishing & Social Engineering	unknown
http://https://ccaeperu.com/?cmd=9tyym8t91xbt8b81mt81smbbm1s.9vtn8ytms1v9vvy8198118b	{6767ACEF-9935-11EB-90EB-ECF4BBEA1588}.dat.1.dr, ~DF77662EBE27437295.TMP.1.dr	true	• 100%, UrlScan, Browse • SlashNext: Fake Login Page type: Phishing & Social Engineering	unknown
http://https://ccaeperu.com/?cmd=stmn8bymn1v1.18svn81tv1ymtxtxy1ymns8y1vt81b.9nty9s8	{6767ACEF-9935-11EB-90EB-ECF4BBEA1588}.dat.1.dr, ~DF77662EBE27437295.TMP.1.dr	true	• 100%, UrlScan, Browse • SlashNext: Fake Login Page type: Phishing & Social Engineering	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://static.xx.fbcdn.net/rsrc.php/v3/yr/r/vdzjXL4eT5D.js?_nc_x=Ij3Wp8lg5Kz	B9RXHZ5I.htm.2.dr	false		high
http://https://ccaeperu.com/?cmd=m9xvsybnvn1sv.bsnmnsyx119yb8mx1yv88sst1s8sxsv11nt.t	{6767ACEF-9935-11EB-90EB-ECF4BBEA1588}.dat.1.dr, ~DF77662EBE27437295.TMP.1.dr	true	• 100%, UrlScan, Browse • SlashNext: Fake Login Page type: Phishing & Social Engineering	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
157.240.17.15	unknown	United States		32934	FACEBOOKUS	false
68.66.226.79	ccaeperu.com	United States		55293	A2HOSTINGUS	false
157.240.219.13	scontent.xx.fbcdn.net	United States		32934	FACEBOOKUS	false
157.240.17.35	star-mini.c10r.facebook.com	United States		32934	FACEBOOKUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	384636
Start date:	09.04.2021
Start time:	15:12:58
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 28s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://ccaeperu.com/?real-estate-agent2938423
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:	7

Copyright Joe Security LLC 2021

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 • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal64.phis.win@3/61@12/4
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browsing link: https://fb.com/ • Browsing link: https://ccaeperu.com/r.php?locale=en_US • Browsing link: https://ccaeperu.com/?cmd=stmn8bymn1v1.18svn81tv1ymtxtxy1ymns8y1vt81b.9nty9s8 • Browsing link: https://ccaeperu.com/?cmd=t8ntyxt9mnn.9.t9t1ns9tnb11.n9tttbstxsmt91bmnsb8xts1 • Browsing link: https://ccaeperu.com/?cmd=vt9n.n11981t1t8b1t1xm1msm.s9tsxxssy9tstt1t8nsb.y1ms • Browsing link: https://ccaeperu.com/?cmd=9tyym8t91xbt8b81mt81smbbm1s.9vtn8ytms1v9vvy8198118b • Browsing link: https://ccaeperu.com/?cmd=m9xvsybnvn1sv.bsnmnsyx119yb8mx1yv88sst1s8sxsv11nt.t • Browsing link: https://ccaeperu.com/?cmd=bnvtbtxmsbx1vy11snsm8nx8smbbmy8x8snns.8tm99yn88xtvv • Browsing link: https://ccaeperu.com/?cmd=xbsmyynyy.8y18y8tvmsstm1ntysyxmx.ty.1xtxsm9bs8s88n8 • Browsing link: https://ccaeperu.com/?cmd=svnv9tsbx9tbsttsnxbtbnt.mynxy1vytby81nv1mb1v.b1ms9s • Browsing link: https://ccaeperu.com/?cmd=snstmsbsvtx.s1.smysttx.sv11m9ss9xbtb1mvmmytn9t1tyny
Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 104.42.151.234, 13.88.21.125, 52.147.198.201, 2.18.101.230, 104.43.139.144, 20.50.102.62, 23.10.249.26, 23.10.249.43, 152.199.19.161 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, ie9comview.vo.msecnd.net, skypedataprdcolcus16.cloudapp.net, a1449.dscg2.akamai.net, arc.msn.com, skypedataprdcoleus16.cloudapp.net, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, go.microsoft.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, skypedataprdcolwus16.cloudapp.net, skypedataprdcolwus15.cloudapp.net, cs9.wpc.v0cdn.net • Report size getting too big, too many NtCreateFile calls found. • Report size getting too big, too many NtDeviceIoControlFile calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\E5F0NRSV\m.facebook[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	13
Entropy (8bit):	2.469670487371862
Encrypted:	false
SSDEEP:	3:D90aKb:JFKb
MD5:	C1DDEA3EF6BBEF3E7060A1A9AD89E4C5
SHA1:	35E3224FCBD3E1AF306F2B6A2C6BBEA9B0867966
SHA-256:	B71E4D17274636B97179BA2D97C742735B6510EB54F22893D3A2DAFF2CEB28DB
SHA-512:	6BE8CEC7C862AFAE5B37AA32DC5BB45912881A3276606DA41BF808A4EF92C318B355E616BF45A257B995520D72B7C08752C0BE445DCEADE5CF79F73480910FE D
Malicious:	false
Reputation:	low
Preview:	<root></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{6767ACED-9935-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8499028416788235
Encrypted:	false
SSDEEP:	192:rZZeZz2jWntNifFRlbzMAzBzQZDKsf6lCjX:rPKKatS2QYZ3
MD5:	0072F634E27348C1ED32B25CF30C8A59
SHA1:	8C9127D6C8D20F9FCCB1B12CAD9CDCC2E5CDFFC4
SHA-256:	F0381FB3A528916666693066C76E78E6FF5AFEC8286E3FD082D0811F3D796C0A
SHA-512:	B9203BAB3D758171A74222A1628512FE34364A11F297070211100A0C33D3BA76713539CDA734AD270A7210345F262A824C9461310E55CF0200EC1F3D64657AA0
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\{6767ACEF-9935-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	186352
Entropy (8bit):	2.6488975297394957
Encrypted:	false
SSDEEP:	384:rqCAAXgcPQXgRdUS7e5VxBliMXYd1l2bVLOyacTPtOvVOKfFB35CiZcA2h8VCcQn:sdM1IWVLOGT9A335CimETPZiY0qJZaZ
MD5:	522FDB7AAB9213ED0C92C61A0A20ED02
SHA1:	1C0C9F33B4A2CD3F57CE0E298152777BD7C9F899
SHA-256:	1EEF4E71EFE467AB09996BC8094FBCAB2652BD2BF1B01175953264B5F3B49FE8
SHA-512:	9B6E738E2236B79C21040647E3F3EE428B15209211E666C466117FBFDD422A17B12BA474FB10A3C841C34B977E8933D6DED251863FE5DAB2A98814C43075B169
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\{6767ACF0-9935-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5646421266261221
Encrypted:	false
SSDEEP:	48:IwkGcpr5GwpavG4pQnGrapbShGQpKMG7HpRbcTGIpG:r4ZzQh67BSbAnTbIA
MD5:	7403594A64A8C0C933D26332B0DF38F7
SHA1:	6BFD9F5EAECCFEB51243142CC27F65FFBAEB81B0
SHA-256:	4CB098360BB76BB0CD5EE49E5EAE1E9DDAEE0E24E597E2ABC9C7558CCB5410A2
SHA-512:	5A5FABBE104C36A77B9A7524C8A6B71E8FA6FEB57F91E312600461B900C9B4B5C4C923B2398A5ADB315315E4A919B7E5644A76F027F7B4D1A9DA202F4594C22
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\gee00pr\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	6848
Entropy (8bit):	7.920804979967896
Encrypted:	false
SSDEEP:	96:0UGIjjQlCsaKgulmtF/Wh4X9805lvjnJ3NrN72pxB6sCjcXNGjD91+mPrTRB70n0:0bujQCKguMnNz5ZN7gB6sWjr+Iv1
MD5:	B45F114C08F7D3AC943080A577EEE859
SHA1:	F45802E218840F07C2319E3EBC3D4F6E61B9E09E
SHA-256:	DA10756673AF83C195C4B73C4B9AA54A90F82C4C9FA2295DBDBAB47304ACA2C7
SHA-512:	FC48AEFC22F2F7DD0B351D812BE99A04B180834559AE0C876BEC31635EC538FCA8D2423F2A9A034A5C966B8EB9D76961883F530001DCFF40C181F8F1C32D022
Malicious:	false
Reputation:	low
Preview:	<.h.t.t.p.s.:./.s.t.a.t.i.c...x.x...f.b.c.d.n...n.e.t./.r.s.r.c...p.h.p./.v.3./.y.j./.r./.g.B.7.6.k.J.X.P.Y.J.V...p.n.g."....PNG.....IHDR.....x~Y....PLTE.....g.....e.....i.....c..d..b.. .....f..l..s..q.....h..t.....m..n.....p.....y.....o.....u.....v.....r.....k..j.....w.....x.....c..f..~.....d.....m..h.....o.....x..}.. .....w..z..v.....|..z..{.....z..}..r.....|.....p..k.....~.....y..u..y..n.....k.....v....=.....w.....j.....].....x...._.q...a..t.....y.}..s..s.....e..o.....f..k..c.... ...q..r...q.....j.r...l.....p... ..F.....n.....1.....s. .....~.....c.....t.....x.i.....W..... ...|.....5.....z.8..2.....Q.....v..\..=.....g.....>.jB....I DATx..W{..ey~.....L...x....T.@..b.2PA.."l8..$<....j..6.Z..`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\3GXKZCM3.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with very long lines
Category:	downloaded
Size (bytes):	12440
Entropy (8bit):	5.316155290356013
Encrypted:	false
SSDEEP:	192:irfhzUQHFY/YwqPusfq9tPzzuVgP4E55lTgH1MSCdqxaxU8FB7goXBqU5Q7hFDlC:iFUxhqPusC9tPzzuVgKQFdUcUE

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\3GXKZCM3.htm	
MD5:	0FA61F48FCD95C41B86B0588F2413E0C
SHA1:	91154692B3D9E62E0BF8E5EE34364033AC293377
SHA-256:	5BD1094305CC24100F7A9AE7FC112E89B3301E5FD3FDB404F5D46A5258A95BCB
SHA-512:	8A7EC789FD8B66AC49E5224ECEAA8417F2413A20D1D89804EE588A64DC76631A8146386338453E825BC6ADC50C52C5E29C022457942A0F5066B9687DDF2455D
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_10, Description: Yara detected HtmlPhish_10, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\3GXKZCM3.htm, Author: Joe Security
Reputation:	low
IE Cache URL:	http://https://ccaeperu.com/?cmd=stmn8bymn1v1.18svn81tv1ymtxtxy1ymns8y1vt81b.9nty9s8
Preview:	..<!DOCTYPE html>..<head><meta charset="utf-8" /><meta name="referrer" content="origin-when-crossorigin" id="meta_referrer" />.<style></style><noscript><meta http-equiv="refresh" content="0; URL=/" /></noscript>.<title id="pageTitle">Log in</title><meta property="og:site_name" content="0" />.<meta property="og:url" content="/" />.<meta property="og:locale" content="en_US" /><link rel="search" type="application/opensearchdescription+xml" href="/osd.xml" title="0" />.<meta name="description" content="Log in to start sharing and connecting with your friends, family, and people you know." />.<meta name="robots" content="noodp,noydir" /><link rel="shortcut icon" href="https://www.fb.com/rsrc.php/yl/r/H3nktOa7ZMg.ico" />.<link type="text/css" rel="stylesheet" href="ico/U3QfFrS_cgV.css" data-bootloader-hash="lF8eW" data-permanent="1" crossorigin="anonymous" />.<link type="text/css" rel="stylesheet" href="ico/Af0wuS8syLV.css" data-bootloader-hash="JfgCu" data-permanent="1" crossorigin="anony

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\G1MK1W1S.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with very long lines
Category:	downloaded
Size (bytes):	12440
Entropy (8bit):	5.311987145178721
Encrypted:	false
SSDEEP:	192:irfhzUQHFY/YwqelAsYqTK9T3TQpgP4WBxgTH17/nnxP6x9lFB7goXB1xMtTDwnz:iFUxhqelAsPTK9TjQpgybOFd78E
MD5:	EF28B9AF4F55651692A7CEAE181CEE66
SHA1:	CCA27393E23A51424031BFA1F1A98868E0AB03FB
SHA-256:	8E4A0DC19A03D5A9A9783E1DD9776DABDA062DA7A80AA1672845D6905592BCEF
SHA-512:	8160FB3EEC52DB2C1298518E0934075C47FC8C56B1B70E87D1E7333283A2B65F9E33C010E3019F3D65243C1716006702D3611154E05E3E6660532F2D1D2FFF0B
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_10, Description: Yara detected HtmlPhish_10, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\G1MK1W1S.htm, Author: Joe Security
Reputation:	low
IE Cache URL:	http://https://ccaeperu.com/?cmd=9tyym8t91xbt8b81mt81smbbm1s.9vtn8ytms1v9vvy8198118b
Preview:	..<!DOCTYPE html>..<head><meta charset="utf-8" /><meta name="referrer" content="origin-when-crossorigin" id="meta_referrer" />.<style></style><noscript><meta http-equiv="refresh" content="0; URL=/" /></noscript>.<title id="pageTitle">Log in</title><meta property="og:site_name" content="0" />.<meta property="og:url" content="/" />.<meta property="og:locale" content="en_US" /><link rel="search" type="application/opensearchdescription+xml" href="/osd.xml" title="0" />.<meta name="description" content="Log in to start sharing and connecting with your friends, family, and people you know." />.<meta name="robots" content="noodp,noydir" /><link rel="shortcut icon" href="https://www.fb.com/rsrc.php/yl/r/H3nktOa7ZMg.ico" />.<link type="text/css" rel="stylesheet" href="ico/U3QfFrS_cgV.css" data-bootloader-hash="lF8eW" data-permanent="1" crossorigin="anonymous" />.<link type="text/css" rel="stylesheet" href="ico/Af0wuS8syLV.css" data-bootloader-hash="JfgCu" data-permanent="1" crossorigin="anony

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\GonuXiY4BzC[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	109735
Entropy (8bit):	5.695358139977212
Encrypted:	false
SSDEEP:	1536:G5qAUw5hvigC1EUXiT2y54w4f2sZ4wV1hBjc7OpC3JfbhsXiFKXoAfo3s9:GUAUIYWoC2y54w4klHs4S
MD5:	F6BE46592D787A4E2D6B8F47470A92D9
SHA1:	3E4CC97625D2B22D34A097DDE0646A203B1A4333
SHA-256:	5320C68A11331DCE100F37C976E9149E91DDAD5B4FC8A4F2B4415D8372A85247
SHA-512:	2A7384C6AC304C3ABBF95FC92313AE67A2BBEA73F0B9BEC46A57CFECDDBB4A7C88CC1D4F54FAAE065A2CF90FDEB136E29C4A4AEB5AFBEB340835270EF4A1C2F9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.xx.fbcdn.net/rsrc.php/v3ih-D4/yJ/l/en_US/GonuXiY4BzC.js?_nc_x=Ij3Wp8lg5Kz
Preview:	if (self.CavalryLogger) { CavalryLogger.start_js(["c1jQsCE"]); }..__d("MSeoDirectoryLinks",["cx","CSS","MVisibilityToggle"],(function(a,b,c,d,e,f,g){"use strict";f.initLinks=a;function a(a){var c=a.visible,d=a.toggleButton;b("MVisibilityToggle").setupOnClick({visible:c,toggleButton:d,toggledElement:a.linksContainer,onToggle:function(a){a?b("CSS").addClass(d,"_97hz"):b("CSS").removeClass(d,"_97hz")}})}}),null);.__d("LoggedOutLocaleEventsClientLogger",["Banzai","BanzaiLogger"],(function(a,b,c,d,e,f){"use strict";a=function(){function a(a,b){this.regInstance=b}var c=a.prototype;c.logLocaleEvent=function(a,c,d){a=a.getNode("change_language");if(a instanceof HTMLElement){a=a.dataset.locale;b("BanzaiLogger").create(b("Banzai").VITAL).log("LoggedOutLocaleEventsLoggerConfig",{event:"change_language_acquired",reg_instance:this.regInstance,surface:d,switch_info:{endLocale:a,step:c}})}};c.logMoreLanguage=function(a,c){b("BanzaiLogger").create(b("Banzai").VITAL).log("LoggedOutLocaleEventsLoggerCon

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\HTQSVEM0.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\HTQSVEM0.htm	
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with very long lines
Category:	downloaded
Size (bytes):	12440
Entropy (8bit):	5.315918310354368
Encrypted:	false
SSDEEP:	192:irfhzUQHFY/YwqzMsj8q0FlDOmzOYgP4Tl6moH1idYA5WIQxIpFB7goXBYTur6DI:iFUxhqzMsjr0FNOmzTgR4TFdhyRE
MD5:	6286B4F1462506B5F00A31FB92825163
SHA1:	4133D5403B0968AF3CAA9BCE6736497F995B64DC
SHA-256:	3249F1C5A088AB929405754A6A63F88A5F892572D24B338FB6FBD48AF2C33B81
SHA-512:	303DAB88B9E12BD4A28CA006CC097F6B905719829A17E3B989C8C9B165B027BF8F8613D8C514DB2487399322F8690B19C37BE45C66D4DC22A20185F3E31F866C
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_10, Description: Yara detected HtmlPhish_10, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\HTQSVEM0.htm, Author: Joe Security
Reputation:	low
IE Cache URL:	http://https://ccaeperu.com/?real-estate-agent2938423
Preview:	..<!DOCTYPE html>..<head><meta charset="utf-8" /><meta name="referrer" content="origin-when-crossorigin" id="meta_referrer" />.<style></style><noscript><meta http-equiv="refresh" content="0; URL=/" /></noscript>.<title id="pageTitle">Log in</title><meta property="og:site_name" content="0" />.<meta property="og:url" content="/" />.<meta property="og:locale" content="en_US" /><link rel="search" type="application/opensearchdescription+xml" href="/osd.xml" title="0" />.<meta name="description" content="Log in to start sharing and connecting with your friends, family, and people you know." />.<meta name="robots" content="noodp,noydir" /><link rel="shortcut icon" href="https://www.fb.com/rsrc.php/yl/r/H3nktOa7ZMg.ico" />.<link type="text/css" rel="stylesheet" href="ico/U3QfFrS_cgV.css" data-bootloader-hash="lF8eW" data-permanent="1" crossorigin="anonymous" />.<link type="text/css" rel="stylesheet" href="ico/Af0wuS8syLV.css" data-bootloader-hash="JfgCu" data-permanent="1" crossorigin="anony

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\MNiY97WzXPw[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):	13160
Entropy (8bit):	5.3070910755237035
Encrypted:	false
SSDEEP:	384:Y4wu7KaL5boqM38Y5Gyf28Ykwg7ZAsBhv:Y07PL5boqM38Y5Gyf28Wg7ZFBhv
MD5:	327255731425257 86F658FBEEB46EE50
SHA1:	27535B2678FE89C958AAB3D4B3E21739615712D8
SHA-256:	5C81B60060ADAE5945A11F94D02AC2FF7C7CE4DBC8CD69000C359CA08F1CAA57
SHA-512:	4364EABD97A0A08D0A98C01DD0400F5AD30E3EFAB4096B4E60BA7806946BEF540F81A181ACC909C2DF165A1636C3B8CBC341EEA203FFB330282C9FC2951F64 2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.xx.fbcdn.net/rsrc.php/v3/yB/r/MNiY97WzXPw.js?_nc_x=Ij3Wp8lg5Kz
Preview:	if (self.CavalryLogger) { CavalryLogger.start_js(["zTlK8ig"]); }..__d("CometLruCache",["recoverableViolation"],(function(a,b,c,d,e,f){"use strict";f.create=a;var g=function(){function a(a){this.$1=a,a<=0&&b("recoverableViolation")("CometLruCache: Unable to create instance of cache with zero or negative capacity.","CometLruCache"),this.$2=new Map()}var c=a.prototype;c.set=function(a,b){this.$2["delete"](a);this.$2.set(a,b);if(this.$2.size>this.$1){a=this.$2.keys().next();a.done||this.$2["delete"](a.value)}};c.get=function(a){var b=this.$2.get(a);b!=null&&(this.$2["delete"](a),this.$2.set(a,b));return b};c.has=function(a){return this.$2.has(a)};c["delete"]=function(a){this.$2["delete"](a)};c.size=function(){return this.$2.size};c.capacity=function(){return this.$1-this.$2.size};c.clear=function(){this.$2.clear()};return a}();function a(a){return new g(a)}),null);.__d("ConstUriUtils",["CometLruCache","FBLogger","PHPQuerySerializer","PHPQuerySerializerNoEncoding","URIRFC3986","URISchemes"

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\RqQo1U5NOq1[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with very long lines
Category:	downloaded
Size (bytes):	12440
Entropy (8bit):	5.311589921665687
Encrypted:	false
SSDEEP:	192:irfhzUQHFY/YwqBN6s3GqeBPNzIse7gP4e8MOm2IH1TC0PY0uxmF3FB7goXBWeLg:iFUxhqBMsteBVzIse7gRESBFdxqqzLE
MD5:	19ECE2E22F1A74AF578795E2CE42889B
SHA1:	A86644AB62A4D727442FC479F04A8D7C34F21F90
SHA-256:	978C6DAFEE34473356E240B4367FEB9D19CB008175DAE8240154C6A924E2B9C0
SHA-512:	CB7A1E5EF9F128E77CD72D552D3DB1A8F5164C2D874DA3D459766D04CFAB4C7C9267778563F953DE10BBBC6A18B9678FAC140652D53AACD5B5F2893CE7CDF 3E
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_10, Description: Yara detected HtmlPhish_10, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\RqQo1U5NOq1[1].htm, Author: Joe Security
Reputation:	low
IE Cache URL:	http://https://ccaeperu.com/rsrc.php/v3/yb/r/RqQo1U5NOq1.png

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\RqQo1U5NOq1[1].htm	
Preview:	..<!DOCTYPE html>..<head><meta charset="utf-8" /><meta name="referrer" content="origin-when-crossorigin" id="meta_referrer" />.<style></style><noscript><meta http-equiv="refresh" content="0; URL=/" /></noscript>.<title id="pageTitle">Log in</title><meta property="og:site_name" content="0" />.<meta property="og:url" content="/" />.<meta property="og:locale" content="en_US" /><link rel="search" type="application/opensearchdescription+xml" href="/osd.xml" title="0" />.<meta name="description" content="Log in to start sharing and connecting with your friends, family, and people you know." />.<meta name="robots" content="noodp,noydir" /><link rel="shortcut icon" href="https://www.fb.com/rsrc.php/yl/r/H3nktOa7ZMg.ico" />.<link type="text/css" rel="stylesheet" href="ico/U3QfFrS_cgV.css" data-bootloader-hash="lF8eW" data-permanent="1" crossorigin="anonymous" />.<link type="text/css" rel="stylesheet" href="ico/Af0wuS8syLV.css" data-bootloader-hash="JfgCu" data-permanent="1" crossorigin="anony

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\SWQSh8s8jr2[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	6642
Entropy (8bit):	5.320922344122721
Encrypted:	false
SSDEEP:	96:BOP5JedAUYk5JY5J0505JO5J0Anmq5J0a5J0xk1SnB7w/nA7nWG+kueqoetKDZ+z:BQernWAC0zDxSpIo+Ks
MD5:	56F1012F9038610D4323E60F0336AC92
SHA1:	0B88B14D347366B714CD6555D437E2E6FB4ED9A7
SHA-256:	9B49292E18BA707E5B84526E5F35CADF7A7246AA847087B7C20137B21BF6B4A2
SHA-512:	06F74E6524499A0201F00943F6E412910398BF41CBC0919A915426CB1BE9BDAE9F70EC2019FFB5CB520D29FC699F0249BA03CD51D41C89B81F7DF82E2FC68BA
Malicious:	false
Reputation:	low
Preview:	@media not print{._9ngh._9ngi{height:0;overflow:hidden;padding-bottom:0}}._9ngh{padding-bottom:16px}@media print{._9ngh._9ngi{width:100%}._9ngh{overflow:visible}._9ngj{display:block !important}}._9ngk{cursor:pointer;height:44px;padding:0;text-align:left}._9ngl{background-color:transparent;border:none;width:100%}._9ngl:focus{outline:none}._9ngj{display:flex}._9ngk ._9ngm{margin:0 0 0 0;width:100%}._9ngn{float:right;transform:rotate(90deg)}.._9fyr ._5m_s::after{border-image:none}._9fyr ._5m_u{margin:0 60px}._9fyr ._5m_s{border-radius:12px}._9fys{padding:10px 0 0 0}._9fyt{font-size:large;line-height:normal;padding:2px 30px;text-align:center}._9fyu{padding:5px 15px 20px 15px;text-align:center}._9fyv{border-color:#ccc;border-top-style:solid;border-width:.5px;padding:10px 0;text-align:center}.touch a._9gt6{color:#1c1e21;font-weight:bold}._9fyx{font-family:SFProDisplay-Regular, Helvetica, Arial, sans-serif;font-size:16px;letter-spacing:-0.32px;line-height:20px;width:100%}#accept-cookie-banner

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\VEs5hzVWt5B[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	241335
Entropy (8bit):	5.402172305621012
Encrypted:	false
SSDEEP:	3072:I0IqCFsrR9hHPlNhNLRxdx3JV/Cuvw4Im+gSUQBQAP2Td+/OaG7d:vIFsABQAPGd+WZJ
MD5:	346028FD22C2848201627CACD87E7E44
SHA1:	13C2B4E0E4C4423F0D3FF62C4BAA75E6C338499F
SHA-256:	C91668125CE2BF6CF670222B82CCEED766B58341111704D5026C739A0902F0CF
SHA-512:	B276B2E35273546B6CBDAC67446A5AC3CB20EDD4121E6CA1AB8E2597DD8E1DF91B0FC515C3B85811C1548CEB2316435A6379D27128FE6171029032B395F2E8DB
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.xx.fbcdn.net/rsrc.php/v3/y2/r/VEs5hzVWt5B.js?_nc_x=Ij3Wp8lg5Kz
Preview:	if (self.CavalryLogger) { CavalryLogger.start_js(["WrA3agz"]); }..Array.from||(Array.from=function(a){if(a==null)throw new TypeError("Object is null or undefined");var b=arguments[1],c=arguments[2],d=this,e=Object(a),f=typeof Symbol==="function"?typeof Symbol==="function"?Symbol.iterator:"@@iterator":"@@iterator",g=typeof b==="function",h=typeof e[f]==="function",i=0,j,k;if(h){j=typeof d==="function"?new d():[];var l=e[f](),m;while(!(m=l.next()).done)k=m.value,g&&(k=b.call(c,k,i)),j[i]=k,i+=1;j.length=i;return j}var n=e.length;(isNaN(n)||n<0)&&(n=0);j=typeof d==="function"?new d(n):new Array(n);while(i<n)k=e[i],g&&(k=b.call(c,k,i)),j[i]=k,i+=1;j.length=i;return j});.Array.isArray||(Array.isArray=function(a){return Object.prototype.toString.call(a)=="[object Array]"});.(function(){var a=Object.prototype.toString,b=Object("a"),c=b[0]!="a";function d(a){a=+a;a!==a?a=0:a!==0&&a!==1/0&&a!==-(1/0)&&(a=(a>0||-1)*Math.floor(Math.abs(a)));return a}Array.prototype.map||(Array.prototype.map=funct

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\Z4A97TMF.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with very long lines
Category:	downloaded
Size (bytes):	12440
Entropy (8bit):	5.312329126904888
Encrypted:	false
SSDEEP:	384:iFUxhq3yqsvx7OuvbJxXgXu5MFdG3TzoE:zxhq3yuqfjT
MD5:	89EA7E50F3FFFA5B61C5748E9365F028
SHA1:	182A4DDFB7A04717D564808C8729EB96C8D56320
SHA-256:	90C799C4F26600200AB43D1F68C4CF85B127264E102FA32C529A9A44C8F70C54
SHA-512:	677A4A6F80F8224D9962BC012ED87D3BC7C087ACA9F5E3E3E1DCD6F8C80B0DC0F272EBF2E823D2B28D01A7B779A88DBC43B2925F09E8DFCFFE6648A885CEAC2C
Malicious:	**true**

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\Z4A97TMF.htm	
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_10, Description: Yara detected HtmlPhish_10, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\Z4A97TMF.htm, Author: Joe Security
Reputation:	low
IE Cache URL:	http://https://ccaeperu.com/?cmd=xbsmyynyy.8y18y8tvmsstm1ntysyxmx.ty.1xtxsm9bs8s88n8
Preview:	..<!DOCTYPE html>..<head><meta charset="utf-8" /><meta name="referrer" content="origin-when-crossorigin" id="meta_referrer" />.<style></style><noscript><meta http-equiv="refresh" content="0; URL=/" /></noscript>.<title id="pageTitle">Log in</title><meta property="og:site_name" content="0" />.<meta property="og:url" content="/" />.<meta property="og:locale" content="en_US" /><link rel="search" type="application/opensearchdescription+xml" href="/osd.xml" title="0" />.<meta name="description" content="Log in to start sharing and connecting with your friends, family, and people you know." />.<meta name="robots" content="noodp,noydir" /><link rel="shortcut icon" href="https://www.fb.com/rsrc.php/yl/r/H3nktOa7ZMg.ico" />.<link type="text/css" rel="stylesheet" href="ico/U3QfFrS_cgV.css" data-bootloader-hash="lF8eW" data-permanent="1" crossorigin="anonymous" />.<link type="text/css" rel="stylesheet" href="ico/Af0wuS8syLV.css" data-bootloader-hash="JfgCu" data-permanent="1" crossorigin="anony

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\favicon[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with very long lines
Category:	dropped
Size (bytes):	12440
Entropy (8bit):	5.320371041658793
Encrypted:	false
SSDEEP:	192:irfhzUQHFY/YwqmLsMqsO66nAPjegP4atAhxvpvH1PoGI1o9xH5FB7goXB4dzqAM:iFUxhqmLs7sr6nAPjegSPN4+Fd0f33E
MD5:	94DE0293BBF1D6835E4DCC5DC4347CF2
SHA1:	8595B0AEF14CB94E06417ACD87076AC48007B978
SHA-256:	A4DAF526FDF6517104DFA2529621A75FE6D06D69999F59B198235DC062A11C75
SHA-512:	D42EBB879668742A39E6947DE92D4381B6464EE06524106B175101E659E03410A264ADEE412A4B92F2DD92E8CC98EFFC4073277A74CE7E7323D3B380D96C37D4
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_10, Description: Yara detected HtmlPhish_10, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\favicon[1].htm, Author: Joe Security • Rule: JoeSecurity_HtmlPhish_10, Description: Yara detected HtmlPhish_10, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\favicon[1].htm, Author: Joe Security
Reputation:	low
Preview:	..<!DOCTYPE html>..<head><meta charset="utf-8" /><meta name="referrer" content="origin-when-crossorigin" id="meta_referrer" />.<style></style><noscript><meta http-equiv="refresh" content="0; URL=/" /></noscript>.<title id="pageTitle">Log in</title><meta property="og:site_name" content="0" />.<meta property="og:url" content="/" />.<meta property="og:locale" content="en_US" /><link rel="search" type="application/opensearchdescription+xml" href="/osd.xml" title="0" />.<meta name="description" content="Log in to start sharing and connecting with your friends, family, and people you know." />.<meta name="robots" content="noodp,noydir" /><link rel="shortcut icon" href="https://www.fb.com/rsrc.php/yl/r/H3nktOa7ZMg.ico" />.<link type="text/css" rel="stylesheet" href="ico/U3QfFrS_cgV.css" data-bootloader-hash="lF8eW" data-permanent="1" crossorigin="anonymous" />.<link type="text/css" rel="stylesheet" href="ico/Af0wuS8syLV.css" data-bootloader-hash="JfgCu" data-permanent="1" crossorigin="anony

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\gB76kJXPYJV[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 196 x 196, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	6690
Entropy (8bit):	7.942833893486368
Encrypted:	false
SSDEEP:	96:iGIjjQlCsaKgulmtF/Wh4X9805lvjnJ3NrN72pxB6sCjcXNGjD91+mPrTRB70nL:BujQCKguMnNz5ZN7gB6sWjr+IvO
MD5:	389DFA18BE34D8CF767E06FD5CDE4EC6
SHA1:	47B751CFFAB47D076816C63CE08D3E84600376EE
SHA-256:	3C45CE612F41B1E7936E7CF5B235047344FD3146D1630E342F186D1D1E8E00D5
SHA-512:	C4DB18F636AD85E87F93A208FB4B02B528659BA367E51CFA6D7826AC1159F445A85FBCA8D12AC67556E8FB5208DAE24AE309E783D50FEB088EF0E9F47AC1943 0
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.xx.fbcdn.net/rsrc.php/v3/yj/r/gB76kJXPYJV.png
Preview:	.PNG.....IHDR.....x~Y....PLTE.....g.....e.....i.....c..d..b.....f..l..s..q.....h..t.....m..n.....p.....y.....o.....u.....v.....r.....k..j.....w.....x. .....c..f..~.....d.....m..h.....o.....x..}.....w..z..v.....|..z..{.....z..}..r.....|.....p..k.....~.....y..u..y..n.....k.....v....=.....w.....j..... .....].....x...._.q...a..t.....y.}..s..s.....e..o.....f..k..c.....q..r...q.....j.r...l.....p... ..F.....n.....1.....s. .....~.....c.....t.....x.i.....W..... ...|..... .....5.....z.8..2.....Q.....v..\..=.....g.....>.jB....IDATx..W{..ey~.....L...x....T.@..b.2PA.."I8..$<....j..6.Z..`.BAS...Y9.|.....}.\.|x.....>...}.....C....;.....T.Y.u..L ....TJ._..j*U.....#.,..9.....2C.VL...4.{Ie(?7.B/...>I&F.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\r[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with very long lines
Category:	downloaded
Size (bytes):	12440
Entropy (8bit):	5.317306675735031
Encrypted:	false
SSDEEP:	192:irfhzUQHFY/Ywqf9AsMqHcxCo2OrgP4oToyOJ1H1SlhUcwr7hnuYxF3FB7goXBnn:iFUxhqf9As7HcxB2Orgynz7EmFdePZ3E

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\r[1].htm	
MD5:	5F765609AE5CA78BB8AB72D384A6B249
SHA1:	056B5237448F26AB246BCF3F1ADDC98BA976C565
SHA-256:	ECB55D76491AF70B3A48A983E1EABD71A4D0F7CB1A13B9D2450BEDAFB3B6D0D3
SHA-512:	73AB629DD30A50832CED92F195A9CBADD3030C5F5978AAD1301A38A16C6089890DE0327B26090B44E2081B1320CB49AB51A59E3CA9B564229B45CA75F6529D9
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_10, Description: Yara detected HtmlPhish_10, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\r[1].htm, Author: Joe Security
Reputation:	low
IE Cache URL:	http://https://ccaeperu.com/r.php?locale=en_US
Preview:	..<!DOCTYPE html>..<head><meta charset="utf-8" /><meta name="referrer" content="origin-when-crossorigin" id="meta_referrer" />.<style></style><noscript><meta http-equiv="refresh" content="0; URL=/" /></noscript>.<title id="pageTitle">Log in</title><meta property="og:site_name" content="0" />.<meta property="og:url" content="/" />.<meta property="og:locale" content="en_US" /><link rel="search" type="application/opensearchdescription+xml" href="/osd.xml" title="0" />.<meta name="description" content="Log in to start sharing and connecting with your friends, family, and people you know." />.<meta name="robots" content="noodp,noydir" /><link rel="shortcut icon" href="https://www.fb.com/rsrc.php/yl/r/H3nktOa7ZMg.ico" />.<link type="text/css" rel="stylesheet" href="ico/U3QfFrS_cgV.css" data-bootloader-hash="lF8eW" data-permanent="1" crossorigin="anonymous" />.<link type="text/css" rel="stylesheet" href="ico/Af0wuS8syLV.css" data-bootloader-hash="JfgCu" data-permanent="1" crossorigin="anony

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\sO8pFbm5AdZ[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 124 x 279, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	8601
Entropy (8bit):	7.955860235104234
Encrypted:	false
SSDEEP:	192:NgauVCBV1rtpIBLs7FMOPNMcfbTPj11pQwbWF/1j4nCfUep:NiCZrtpHBMOPLPKwyrE4bp
MD5:	C0ACD687DA43DABDE2DE3B7C72C5D0F6
SHA1:	140C33E1836ABCAD4142608A7E77A9A099820EB6
SHA-256:	E91CBEE69B8C4EBEE53B0DB95AB385E9F6EA4BEA7FBC1B08B3961F5B87101221
SHA-512:	3078AFA29DDAD51A94B2CABC22028959FC1A654FC1C62804C3654DEAC7F4515F6B516A43CD372E2AF0D64152F5835B124BBB2CE234B7DEC3BD62FC3AA309B391
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.xx.fbcdn.net/rsrc.php/v3/y_/r/sO8pFbm5AdZ.png
Preview:	.PNG.....IHDR...|.....X.....PLTELiq.....Yo.....w.....KOV...V\e.....KOV.GV..4.....KOVTX_.....dOSZ...TX^ahu..:.... #=.b....%...N.....cho.:RWZcJMR...X..V[ePVbp..W....N...`fp..P..^..P.....:..._....__eoKOV.....m.....Ia.N:..KA.....Gb...`gqW...u.....V...2!.....+'...l..C_....n.;.....X.. D}..q...]P..V....<.s.....p...8.....)A.....3"...(....X.B_***.....a....9.l...Wm.....;.o.+...a.K|.....#m..O...=*.....X..KOV....B^jq...[..T...`fq..bXWV..j.....h..G.....@...bixO. .q.....p./...o....gn}._..}...Ge-.+.....OQ%... .9..V.Md.....l..../.Aa.....)UZk.lO...a.....v%.+A.....HBC.LQ....cX2..3..<.h*:?_...yqT.Jsl!.5..a..C..W.U..R.G3...8..N<.....tRNS... .....[.....l3..{J=....:.!.....H.;p..*.Q.*...._...B.....aw..+....Tk..N...{.h..:....*...L&.....k.Y.QE.1.....T..j.....n+.U.....~7q....IDATx^.... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\22KpFFJQuZn[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	46629
Entropy (8bit):	5.362213181152228
Encrypted:	false
SSDEEP:	384:P30RuIuXY1uGL6R3iFdz04VenDvXGecCOUlwAdmkqoYAWqNfBJx6NhFL:P0RuIuo1uGa3iFdOfJwOY9qNfBJx6NhF
MD5:	A62D62FD8007344163F69A268E7E918A
SHA1:	8C0A433D5E0BB8AE23C6AE5B302D51E77B0D195B
SHA-256:	D05D03A47182FD8C95735DAF2F65F2B80B8A8545DD6C0E271CFE3FDCCBF81246
SHA-512:	CAE9940226753129348F40D3D46D08519DA2F73F74EB36592D4B6BFBCF56BAD339BA71466B5D24B6E8F0A63B673B7926CFCDB193B2645C72E5F19386E80C45E
Malicious:	false
Reputation:	low
Preview:	._2g0e{margin-left:10px}._1-gi{display:inline-block;line-height:16px;margin-right:4px}._1-gi.invisible_elem{visibility:hidden}._1e_c{border-radius:2px;vertical-align:middle}._jvo._jvo{vertical-align:middle}._ru1{padding:12px 0;text-align:center}._ru0:first-child{border-top:none}._ru0{border-top:1px solid #e5e5e5;line-height:32px;padding:8px}._3nv2{float:right;padding:12px;padding-left:4px}..fbEmuTracking{position:absolute;visibility:hidden}.._513c #viewport{margin:0 auto;max-width:600px}.._7hj_{visibility:hidden}._6ykc{padding-left:5px}._6ykd{padding-right:5px}._7gvg{font-weight:bold;margin-left:-50px}._6-xu{height:30px;width:100%}.._3eqx{text-align:center}._ov_{margin:0 10px 15px}._6_f8{background:#fff;height:121px;margin:9px 0;position:relative}._6_f9{background:#ebedf0;border-radius:50%;height:48px;left:10px;position:absolute;top:14px;width:48px}._6_fa{background:#ebedf0;height:8px;left:70px;position:absolute;top:34px;width:150px}..touch ._b7l{margin:10px}.touch ._69aj{background:#f

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\2b4ptAQoeCF[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	12443
Entropy (8bit):	5.312840203916209

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\2b4ptAQoeCF[1].js	
Encrypted:	false
SSDEEP:	96:7jPnFRWmLa+C4WtIR5vsXgxiOmf5eoqzICNJAATklEEk3A4slegOWWT2NdLzIsy0:ntgpNCmeoqjEkrs5IsOmSUDX89m
MD5:	BFEE33A16601268523152A0F32A72380
SHA1:	F87C42234BC8715AA6D6AEFE80D722E2B94F2221
SHA-256:	F7808EC7FF2FFE1C0F9D01EF87BDB7A9DB00DB99D65A2750FCD2AFE082ACC873
SHA-512:	C06B5D38138B755D0EE7200D70AA62497347EBDB762911FF9A6351D5DA6194BFAAE8E979443B591F54D3DAF762EAB28E27F637F3EC9D404841A2F0D1D9A3D96
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.xx.fbcdn.net/rsrc.php/v3ijfq4/y5/l/en_US/2b4ptAQoeCF.js?_nc_x=Ij3Wp8lg5Kz
Preview:	if (self.CavalryLogger) { CavalryLogger.start_js(["Br8yI3P"]); }..__d("MUFISocialSentence",["cx","fbt","Bootloader","CSS","DOM","MLiveData","Stratcom","SubscriptionsHandler"],(function(a,b,c,d,e,f,g,h){a=function(){"use strict";function a(a,c,d,e,f,g){if(!g&&!d)return;this.$1=a;this.$2=b("MLiveData").get(c);this.$3=e;this.$4=f;this.$5=g;this.$6=d;this.$7=new(b("SubscriptionsHandler"))();this.$7.addSubscriptions(this.$2.listen("change",this.onChange.bind(this)),b("Stratcom").listen("m:page:unload",null,this.onUnload.bind(this)))}var c=a.prototype;c.onChange=function(){var a=this.$2.getData();if(a.request_id===this.$4)return;b("CSS").removeClass(this.$1,"like_opt");var c=this.$5&&a.like_count?a[this.$3][0]:null,d=this.$6&&a.comment_count?a.comment_count:null;if(c&&c.text){this.$8={text:c,ftid:a.ft_ent_identifier};c=c.text;this.$6||b("Bootloader").loadModules(["MReactComponentRenderer","MUFISocialSentenceTextWithEntities.react"],function(a,b){a(b,this.$1,this.$8)}.bind(this),"MUFISocialSe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\BwjU4B_qfpp[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	10637
Entropy (8bit):	5.352070441529548
Encrypted:	false
SSDEEP:	96:Ue8ByumvNOJ6pVgqJTw08d54zAlKF/yAuR7RDghD:6ByumvYMH+4zAlVDR7RD6
MD5:	AA319BB3DC5CA571817088C857306945
SHA1:	D89ED924EE578B70C99317DA2AA480D95A6FCFE8
SHA-256:	9F737A9DDC6C4ED27D748F1571A6041EECDA3DFD7C391898CC35B01F0E6C435D
SHA-512:	E214D64F349C92D8BE67A2AC0F7E7662BCA8440C376DB1B3B55839D22B66FD90BD30AA67DB4A862DD402DD9CCF89A2CE38415CCF0A8C4764F809B36A424A51AB
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.xx.fbcdn.net/rsrc.php/v3/yC/r/BwjU4B_qfpp.js?_nc_x=Ij3Wp8lg5Kz
Preview:	if (self.CavalryLogger) { CavalryLogger.start_js(["KQ+loWk"]); }../**. * License: https://www.facebook.com/legal/license/HAC-_9WTKIm/. */.__d("flatbuffers",[],(function(a,b,c,d,e,f){var g={};g.Offset;g.Table;g.SIZEOF_SHORT=2;g.SIZEOF_INT=4;g.FILE_IDENTIFIER_LENGTH=4;g.Encoding={UTF8_BYTES:1,UTF16_STRING:2};g.int32=new Int32Array(2);g.float32=new Float32Array(g.int32.buffer);g.float64=new Float64Array(g.int32.buffer);g.isLittleEndian=new Uint16Array(new Uint8Array([1,0]).buffer)[0]===1;g.Long=function(a,b){this.low=a|0,this.high=b|0};g.Long.create=function(a,b){return a==0&&b==0?g.Long.ZERO:new g.Long(a,b)};g.Long.prototype.toFloat64=function(){return(this.low>>>0)+this.high*4294967296};g.Long.prototype.equals=function(a){return this.low==a.low&&this.high==a.high};g.Long.ZERO=new g.Long(0,0);g.Builder=function(a){if(!a)var b=1024;else var b=a;this.bb=g.ByteBuffer.allocate(b);this.space=b;this.minalign=1;this.vtable=null;this.vtable_in_use=0;this.isNested=!1;this.object_start=0;this.vtab

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\IxxDAbiZepi[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	5735
Entropy (8bit):	5.1317810811557365
Encrypted:	false
SSDEEP:	96:w1JMgRcPl4aWkSlLC+HDqebXHmpYXgrLzGm7tEDJsumLf1z6NBUEE7mWThQS47/X:Megql7WLqebXHmmXgrLz97tED+umL9+z
MD5:	3B0814188433956AF3D73648D0DB00B7
SHA1:	49BB4B80E746AA2296DDB987BA8D49F911D4E4B4
SHA-256:	28FC8DA452C6C21D1AEDA674F2F6B8864504FBE8A1823EEBB6CE1814836AF08E
SHA-512:	699B548F8381698783D9733E522755B1FA22DDD0B3BB651FF2433ED16D49AFDFEB89061FAE52BFF1B69D7F36DCA9A90F5D8B0C59003773C3BD9AE5C922B5C0
Malicious:	false
Reputation:	low
Preview:	.touch ._5m_x{height:0;position:absolute;width:100%;z-index:13}.touch ._3wo2 ._5m_x{z-index:25}._4sc_,._5m_v,._7teu{box-sizing:border-box;overflow:hidden;pointer-events:none;position:absolute;width:100%;z-index:0}._5m_v{padding-bottom:28px}._7teu{align-content:center;display:flex;height:100vh;justify-content:center}._5m_u{border-radius:3px;margin:auto 0;pointer-events:auto;position:relative;text-align:left}._7e0o ._5m_u{background:transparent;border-radius:2.7px;display:block;height:auto !important;margin:0 auto 0 auto;width:83vw}._5m_w{background:rgba(0, 0, 0, .5);bottom:0;left:0;pointer-events:auto;position:fixed;top:-600px;width:100%;z-index:-2}._7e0o ._5m_w{background:rgba(0, 0, 0, .6)}._7e0o ._5m_v{top:50vh;transform:translateY(-50%)}._5m_t>:first-child{border-top-left-radius:3px;border-top-right-radius:3px}._5m_t>:last-child{border-bottom-left-radius:3px;border-bottom-right-radius:3px}._5m_s{background:#fff;border-radius:3px;bottom:0;left:0;position:absolute;right:0;top:0;z-index

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\JopZtdti8dq[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	7272

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\JopZtdti8dq[1].js	
Entropy (8bit):	5.199912003117227
Encrypted:	false
SSDEEP:	192:YQ7ppcEf3k4TXlM49kfhTvp7J2X3eBCvqK:Yaf3kUM44vp70X3B
MD5:	3D275AC87B7225FAE26690F31A3110F1
SHA1:	D72083AD2A31CBC8BEA643676F2B214F2028A26A
SHA-256:	95D95840165EA5FC374A27F1CFFE88A1B3D033562916EF1071393C9C8ADBFE86
SHA-512:	DA97C4808DA40A3F564637CA26206477BB818EF9EA3B7361DF83D81DF146E46EA895E90D117FDF9F309447A5B0B2DE3618B9B08DA7882AAF0DF91383564FC1A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.xx.fbcdn.net/rsrc.php/v3/y_/r/JopZtdti8dq.js?_nc_x=Ij3Wp8lg5Kz
Preview:	if (self.CavalryLogger) { CavalryLogger.start_js(["FEt5GzN"]); }..__d("CavalryLoggerImpl",["Arbiter","Bootloader","ISB","ImageTimingHelper","KillabyteProfilerConfig","NavigationTimingHelper","PageEvents","PageletEventConstsJS","PageletEventsHelper","PerfXLogger","ResourceTimingBootloaderHelper","ScriptPath","performance","performanceAbsoluteNow"],(function(a,b,c,d,e,f){var g,h,i=b("KillabyteProfilerConfig").htmlProfilerModule,j=b("KillabyteProfilerConfig").profilerModule,k=["t_start","t_paint","t_cstart"],l=window.CavalryLogger;Object.assign(l.prototype,{initializeInstrumentation:function(){if(this.instrumentation_started)return;var a=this;b("Arbiter").subscribe("BigPipe/init",function(b,c){c.lid==a.lid&&c.arbiter&&(a._recordTTIEvent(c.arbiter,"tti_bigpipe"),a._recordDisplayedEvent(c.arbiter,"all_pagelets_displayed"),a._recordLoadedEvent(c.arbiter,"all_pagelets_loaded"),a._recordPageletEventsTime(c.arbiter)))});b("Arbiter").subscribe("MRenderingScheduler/init",function(b,c){c.lid==a.lid

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\NOmsNpPjqKN[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	10016
Entropy (8bit):	5.275912293066321
Encrypted:	false
SSDEEP:	192:kStlsoB9o6N7xAGy2SjAv+IZ7OAX5BVE1WOWnnF96ZKtttz/z7wovQZ4O39/lRRM:dcT0+lZ6DBkW
MD5:	BD36C07720E78ECA14E40F732B0DEA96
SHA1:	9400166538F6F65A89E1C102CCA07DAE82C4FF34
SHA-256:	404CBEFB1D9A3B2CD4F723C8553D714EA257E78B3691BC1BB37BF1F78A192AD6
SHA-512:	11D012B54B44880E3894DDB7D2E816AA6D39FA5F9CF0CA2DC371939D50B654CE3153FB59DB7894218AE9A57858747F2B561D29A062AB15C85C4FC3A2E86A140
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.xx.fbcdn.net/rsrc.php/v3/yJ/r/NOmsNpPjqKN.js?_nc_x=Ij3Wp8lg5Kz
Preview:	if (self.CavalryLogger) { CavalryLogger.start_js(["Xjm9V55"]); }..__d("BrowserPushMessageRedirectUtil",[],(function(a,b,c,d,e,f){e.exports=a;function a(a){return!0}}),null);.__d("BrowserPushCommands",[],(function(a,b,c,d,e,f){a="browser_push_ack";b="browser_push_redirect";c="browser_push_window_visible";d={ACK:a,REDIRECT:b,WINDOW_VISIBLE:c};e.exports=d}),null);.__d("BrowserPushMessageHandler",["BrowserPushCommands","BrowserPushMessageRedirectUtil","EventListener","URI","URISchemes","isFacebookURI"],(function(a,b,c,d,e,f){var g,h;function i(a){if(a.data.command&&a.data.command===b("BrowserPushCommands").REDIRECT){if(typeof window.onbeforeunload==="function"&&window.onbeforeunload()===void 0)a.ports[0].postMessage({command:b("BrowserPushCommands").ACK,success:!0});else{a.ports[0].postMessage({command:b("BrowserPushCommands").ACK,success:!1});return}a=a.data.uri;if(/^([^.:/?#]+):/.test(a)&&!(g||(g=b("URISchemes"))).isAllowed(/^([^.:/?#]+):/.exec(a)[1])||!b("isFacebookURI")(new(h||(h=b("UR

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\QrKwBeCiZyv[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	5747
Entropy (8bit):	5.116735868721678
Encrypted:	false
SSDEEP:	96:VRMNVDpweF7C/5YDJdM77IjgEdf9pQ9Qmz85Nt2o:VRU1w6740dacpQ9QX3
MD5:	B2FB748287798413178D4E1A1476E5C2
SHA1:	2517605D2727663377491224AACFA365209C6721
SHA-256:	9D427CB90E448F435ACBF1BD66AC37C7CEC6E8B8AFA5BF8D691FC80C51F62DE2
SHA-512:	6D8BE2E43EAABF10F713000EE04247F68B03DDF92B7CEC9ABBF99A71C3813DEEFDD1F02DF7542A70FDC79E196DB7DB963FF3B54A4BA52A63E22DD13626547644
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ccaeperu.com/ico/QrKwBeCiZyv.css
Preview:	html,body{border:0}body.booklet{margin:0;padding:0;overflow:visible}#booklet{margin:0;padding:0}#booklet #content{border:0 solid white;float:none;margin:0;padding:0;width:auto}#booklet #pageheader{background:#365899;color:#fff}#booklet #pageheader #homelink{background:url(/rsrc.php/v3/yR/r/teE39sffXW8.png) no-repeat 10px 50%;color:#fff;margin:0;padding:8px 10px 8px 30px}#booklet #fbpageheader{background-color:#365899;border-bottom:1px solid #1a3878;height:34px}#booklet #fbpageheader #logo{float:left;background-image:url(/rsrc.php/v3/yQ/r/Tx1-fA__anj.png);background-repeat:no-repeat;background-size:auto;background-position:4px -2px;height:34px;width:96px}#booklet #fbpageheader a{color:#fff;display:inline-block;float:right;font-weight:bold;margin-top:6px}#booklet #fbpageheader a:hover,#booklet #fbpageheader a:focus,#booklet #fbpageheader a:active{background-color:#4267b2;outline:none;text-decoration:none}#booklet #dialog_buttons{padding:8px 10px}#booklet #dialog_buttons input{margin:2px}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\RUFPPAMX.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with very long lines

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\RUFPPAMX.htm	
Category:	downloaded
Size (bytes):	12440
Entropy (8bit):	5.318989777584086
Encrypted:	false
SSDEEP:	192:irfhzUQHFY/YwqE3dsAqgQ74ClnJdeW3gP4hFH8r6H1fh5z+XkYx/oh1FB7goXBv:iFUxhqEts3P7FlnTt3ggT1/Fd4BE
MD5:	AC309C3BBE172ED5CBC37060FCD0B5CC
SHA1:	BCDAA6B0997F4B82EF90C360950B2AB3B485D931
SHA-256:	24EFD34CFDA269AE64A495DEEFEADA684AB3F3CE990363FA869BAC8AF47B6B7F
SHA-512:	FC99B26B7989B25DB9F7122A97466356E0527652FA896A4AD630E21C5FE41755F7E961AE671CAF659B435DC18D0C3621CEEAE228F02E9A71B6A1F530CEF45981
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_10, Description: Yara detected HtmlPhish_10, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\RUFPPAMX.htm, Author: Joe Security
Reputation:	low
IE Cache URL:	http://https://ccaeperu.com/?cmd=snstmsbsvtx.s1.smysttx.sv11m9ss9xbtb1mvmmytn9t1tyny
Preview:	..<!DOCTYPE html>..<head><meta charset="utf-8" /><meta name="referrer" content="origin-when-crossorigin" id="meta_referrer" />.<style></style><noscript><meta http-equiv="refresh" content="0; URL=/" /></noscript>.<title id="pageTitle">Log in</title><meta property="og:site_name" content="0" />.<meta property="og:url" content="/" />.<meta property="og:locale" content="en_US" /><link rel="search" type="application/opensearchdescription+xml" href="/osd.xml" title="0" />.<meta name="description" content="Log in to start sharing and connecting with your friends, family, and people you know." />.<meta name="robots" content="noodp,noydir" /><link rel="shortcut icon" href="https://www.fb.com/rsrc.php/yl/r/H3nktOa7ZMg.ico" />.<link type="text/css" rel="stylesheet" href="ico/U3QfFrS_cgV.css" data-bootloader-hash="lF8eW" data-permanent="1" crossorigin="anonymous" />.<link type="text/css" rel="stylesheet" href="ico/Af0wuS8syLV.css" data-bootloader-hash="JfgCu" data-permanent="1" crossorigin="anony

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\RpTFjVvO4D0[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	3685
Entropy (8bit):	5.621453320033895
Encrypted:	false
SSDEEP:	96:1IjyBqrIeHQs1a6ZuM5J74DAPTTvbPr/0fJ:CWBqrIeH51RiA73rch
MD5:	5120667A686AB2528C050D156D27B811
SHA1:	C69B77AF43F14EFB4951367CF6A4EEEA661F6219
SHA-256:	5147F2B0C3A7E731F599FDB80503F7D445BFAFB8736B512166A166906E926759
SHA-512:	3AE4897A61B7DF751C85C1965659D2811CD716F5C3E93BC681D5EE2B94FBAE1A7BB6FE6B1C986F69A2E28FFEBD2A47F81388A8CDD1D98DCCFC9F062C20AA762
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.xx.fbcdn.net/rsrc.php/v3ikP64/yA/l/en_US/RpTFjVvO4D0.js?_nc_x=Ij3Wp8lg5Kz
Preview:	if (self.CavalryLogger) { CavalryLogger.start_js(["lo0QsWE"]); }..__d("MStoriesUIConstants",["fbt"],(function(a,b,c,d,e,f,g){"use strict";a={DEFAULT_TIMER_DURATION_IN_SEC:6,STORY_UPDATE_TICK_IN_SEC:.1};f.PROGRESS_BAR=a;b=20;f.REDIRECT_DELAY_IN_MS=b;c=10*60*1e3;f.REFRESH_TIMEOUT_IN_MS=c;d=1e3;f.SEC_TO_MS=d;e=80;f.SWIPE_DISTANCE=e;a=150;f.SWIPE_DOWN_DISTANCE=a;b=10*60*1e3;f.CACHE_EXPIRATION_IN_MS=b;c=["/stories/view_tray","/stories/preview/"];f.HIDE_HEADER_URLS=c;d=g._("Story Added");f.UPLOAD_SUCCESSFUL=d;e=g._("Unable to Add Story");f.UPLOAD_FAILED=e;a=g._("Unable to load effects");f.EFFECTS_LIST_FAILED=a;b=g._("Unable to apply effect");f.EFFECT_APPLY_FAILED=b}),null);.__d("GHLTestElement",["csx","invariant","ODS","Parent","URI","containsNode","getElementPosition","gkx"],(function(a,b,c,d,e,f,g,h){"use strict";var i;a=function(a,c){var d=Array.from(a.querySelectorAll("img"));if(b("gkx")("1059877")){var e=(i||(i=b("URI"))).getRequestURI();e=e!=null?e.getPath():"";var f="images"+c,g="leng

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\TAH3WlPZB8H[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	15872
Entropy (8bit):	5.277764274871931
Encrypted:	false
SSDEEP:	384:P8o1gULKLQcHcdVvdUaVkghPlYO8g9ZUR2kv:P8o1gULKLQc8dVvdUaVVhPlYvg9Ghv
MD5:	29EBFF3A7ACAB502296B5C2FD1283962
SHA1:	2C443237A07210D4FD5E1073D2AB1263F2AAE6FF
SHA-256:	7FCF2EA5DCBBE5ED06D0740A3E2A22C2B474C2ED4F6F7BA87EB8F9DDEE7EC0F3
SHA-512:	45C73651626B50249671B69CC6C5E31EDB67B9C0A85F778FC14E9D3F5C84D82EB9C9CF4BECA1308779AA2CCF2EF19CC3C7F15748ACE9BC639A02D604A9CAD96
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.xx.fbcdn.net/rsrc.php/v3/yd/r/TAH3WlPZB8H.js?_nc_x=Ij3Wp8lg5Kz
Preview:	if (self.CavalryLogger) { CavalryLogger.start_js(["FpeIRVs"]); }..__d("Animation",["BrowserSupport","CSS","DOM","DataStore","Style","clearInterval","clearTimeout","getVendorPrefixedName","requestAnimationFrame","setIntervalAcrossTransitions","setTimeoutAcrossTransitions","shield"],(function(a,b,c,d,e,f){var g=b("requestAnimationFrame"),h=[],i;function j(b){if(a==this)return new j(b);else this.obj=b,this._reset_state(),this.queue=[],this.last_attr=null,this.unit="px",this.behaviorOverrides={ignoreUserScroll:!1}}function k(a){if(b("BrowserSupport").hasCSS3DTransforms())return n(a);else return m(a)}function l(a){return a.toFixed(8)}function m(a){a=[a[0],a[4],a[1],a[5],a[12],a[13]];return"matrix("+a.map(l).join(",")+")"}function n(a){return"matrix3d("+a.map(l).join(",")+")"}function o(a,b){a||(a=[1,0,0,0,0,1,0,0,0,0,1,0,0,0,0,1]);var c=[];for(var d=0;d<4;d++)for(var e=0;e<4;e++){var f=0;for(var g=0;g<4;g++)f+=a[d*4+g]*b[g*4+e];c[d*4+e]=f}return c}var p=0;j.prototype._reset_state=function()

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\h3jijAStzKK[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	38475
Entropy (8bit):	5.497208573087439
Encrypted:	false
SSDEEP:	384:jywzIoAcMI6sIN+p2fNkvtTyZJWCkqogynHPEdav6EfolV25qhDTtUqgdobl1CpA:mwzxHMiIcWddxfEsLixxcwTig
MD5:	2546EA47AA7749C9BA01D2EDEF9C87F2
SHA1:	67E90018EDFD011A95692EF3549BD2C420A1126C
SHA-256:	17359A995DE7DEF07EA79A016F3506C1ED56B3C8C9AFC8F9A1C76F7ABB9636A4
SHA-512:	F31C7B75CF31031E9A1209EE2E22CC0D701C501AF74639D4ABD3B3E5C4FFE5E6A00052206B3A5C3647A4D5E5D26052F9267CA5BAF3559CA0A784605A8C40358
Malicious:	false
Reputation:	low
Preview:	.wp.touch._fzu .storyStream>.carded,.wp.touch._fzu .storyStream>article>.carded,.wp.touch._fzu .storyStream>div>.carded,.android.touch._fzu .storyStream>.carded ,.android.touch._fzu .storyStream>article>.carded,.android.touch._fzu .storyStream>div>.carded,.wp.touch._fzu .groupChromeView.feedRevamp .carded,.android.touch ._fzu .groupChromeView.feedRevamp .carded{border:1px solid #bdbebf;border-image:none}.touch._fzu .storyStream>.carded,.touch._fzu .storyStream>.carded:first-chi ld,.touch._fzu .storyStream>article>.carded,.touch._fzu .storyStream>div>.carded,.touch._fzu .groupChromeView.feedRevamp .carded{border-image:url(/rsrc.php/v3/y N/r/QmGuax92JQa.png) 4 4 6 repeat;border-width:4px 4px 6px;margin:0 8px 9px}.touch._fzu .storyStream>.carded._29d0{border:0 none;margin:0 0 8px;overflow:hidden; padding:16px}.touch._fzu .storyStream>.carded._29d0._122m{padding:10px 10px 0}.touch._fzu .groupChromeView.feedRevamp .carded.groupHeader{margin:10px 8px}.x2.touch._fzu .storyStream>.carded,.x2.touch.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\n4bGLjGRWrl[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	11208
Entropy (8bit):	5.394612582577508
Encrypted:	false
SSDEEP:	192:gTw8C7Ls5EBwb70Oc39dSWEfpIH0Wupmxm6VHTT:gTwbL3VoROgYVHTT
MD5:	4E068352658B4E168C79AA686F611FA8
SHA1:	EAF91AFAA2AB1F6C0D16A284B51284BC5158C42F
SHA-256:	5E75640FA4EAA50080551EE539B16841EC479343BB40891F91D7092B5C7FF901
SHA-512:	1A91F85F138583F4D9561A63765E91E26CB9317A037BA337A3B0CD745EA2F5A208C13EB982C6261EF6251434904E8D3892475D47229E890F3D239C65A9FFDE10
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.xx.fbcdn.net/rsrc.php/v3i8594/yf/l/en_US/n4bGLjGRWrl.js?_nc_x=Ij3Wp8lg5Kz
Preview:	if (self.CavalryLogger) { CavalryLogger.start_js(["iV49c5Q"]); }..__d("MSideNavMarauderLogger",["MLegacyDataStore","MTouchClick","MarauderLogger","Stratcom"],(function(a,b,c,d,e,f){var g="";function a(a){b("MarauderLogger").toggleModule("sidebar_menu",!0)}function c(a){b("MarauderLogger").toggleModule("sidebar_menu",! 1)}function d(a){var c=a.getNode("tag:a");a=a.getNode("tag:div");b("MarauderLogger").log("open_application","sidebar_menu",{application_link_type:"local_module" ,display_name:a?a.innerText:"unknown",url:c&&c.href});b("MarauderLogger").setNavigationModule("sidebar_menu")}function f(){j("session_start")}function h(a){a=a. getData();if(a.node.rel<=0)return;var c=0,d="",e=b("MLegacyDataStore").get(a.node);e&&(c=e.bootstrap?1:0,d=e.type);e=0;var f=null;for(var g=0;g<a.results.length;g++) {var h=a.results[g];if(h.rel>0){if(h.rel==a.node.rel){f=e;break}e++}}j("click",{query:a.query,is_bootstrapped:c,display_position:f},d,a.node.rel)}function i(a){g!==a&&j("searc h_keystroke",{prev_q

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\vjVEyrdqGK6[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	28268
Entropy (8bit):	5.373256065673994
Encrypted:	false
SSDEEP:	384:4WqvA9umvNBihfTGN8itN519iefQcft+Mi3MGJj6rvHHewvp2+j:Bsa11i3MXp2+j
MD5:	E431EF5BA54E86632644507C1625DBE0
SHA1:	368235C186B92B7ED6BED000CA718EB432F21864
SHA-256:	15DF2A9AEC645B1DC61F7688529859C0DC4C58DDF9DA3798E9951D9DAB185D36
SHA-512:	2D9E069D6887CD28999E3CD92DF742A1913E9EE5DFBD55BB3BFF6099A204AA3E6EEB97CABFC305132BA21C9A965C6FC5828F4448573257EF24E70EBF91391A 0
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ccaeperu.com/ico/vjVEyrdqGK6.css
Preview:	._4-{display:none}.child_was_focused ._4-{display:block}._55d0{background-color:#fff}._119 .textInput::-ms-clear{height:0;width:0}.._wbs a{color:#fff;text-decoration:unde rline}.._3quh{background:transparent;border:0;color:#0084ff;cursor:pointer;font-family:inherit;font-size:14px;line-height:inherit;margin:0;padding:0}._2t_{font-weight:500 }._2u0{font-weight:400}._3quh._3ay_{color:#f03d25}._3quh:active{opacity:.2}._4zab{cursor:default;opacity:.4}._4zab:active{opacity:.4}.._39r5{display:block;font-weight:nor mal}._39r6{color:#1d2129;font-size:14px}._39r7{color:rgba(0, 0, 0, .40);font-size:13px}._39r8{font-size:13px}.__0d{display:inline}.._4eby{-webkit-animation-duration:.15s;- webkit-animation-name:popIn;background:#fff;border:0;border-radius:6px;box-shadow:0 2px 8px 0 rgba(0, 0, 0, .20);box-sizing:border-box;-webkit-font-smoothing:a ntialiased;position:relative}._2c9g{padding:24px}._2c9g ._4ebz{font-size:16px;font-weight:500;margin-bottom:16px}._2c9i ._4ebz{border-bottom:1px solid rgba(0, 0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\1487645_6012475414660_1439393861_n[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 10 x 10, 8-bit/color RGB, non-interlaced
Category:	downloaded
Size (bytes):	79
Entropy (8bit):	4.71696959175789
Encrypted:	false
SSDEEP:	3:yionv//thPlH1tnt/tAhHGZscm1olkqCwbp:6v/lhP6hHDcZCYp
MD5:	8DC258A49B60FAE051E9A7CE11AD05CF
SHA1:	DAFEF280663F4205FC7F0E47799E9945E6A68D6D
SHA-256:	C8CAED93847AFFC154CB3D424E34FC146E7340BB29ABEBD5EBA7063E3DCA0604
SHA-512:	5F11ED60D79A80EF7CCEFFA907CD55F31D8DB19BD2A7F4C2650C62A355C5071C5FB61DA1EB0A2071CE22ECDC35C0D12F51E4D13AAC3B0FDB95ED4629815B AFB
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://scontent.xx.fbcdn.net/hads-ak-prn2/1487645_6012475414660_1439393861_n.png
Preview:	.PNG.....IHDR.....PX.....IDAT.Wc...0a.!..)....A,....Zl....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\6LTWT96P.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with very long lines
Category:	downloaded
Size (bytes):	12440
Entropy (8bit):	5.319604500502523
Encrypted:	false
SSDEEP:	192:irfhzUQHFY/Ywq7byzsMqMnVVn3G9gP4qv7cixHnH1Di/kgdxdG+FB7goXBhXJuM:iFUxhq78s7MnVVn3G9gFFv+FdiflE
MD5:	3EFD2F3A4034940DC005B22CF17C2A2C
SHA1:	C4204FE95E7C3189B65DD33AEC0438D941CF3935
SHA-256:	4121DB577DE5FAECEB0BB546C53CFF8A71642F56D7AF4B493EE6932F19EB126A
SHA-512:	0775DFA2238E2093D6AFFAF51A07B910E901D8D52EBD51770AC904FB8B4D92026CEF21E0A82F51783C1607586E7836F0E05B093F8511B9FB17C05DA2230476E2
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_10, Description: Yara detected HtmlPhish_10, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\6LTWT96P.htm, Author: Joe Security
Reputation:	low
IE Cache URL:	http://https://ccaeperu.com/?cmd=vt9n.n11981t1t8b1t1xm1msm.s9tsxxssy9tstt1t8nsb.y1ms
Preview:	..<!DOCTYPE html>..<head><meta charset="utf-8" /><meta name="referrer" content="origin-when-crossorigin" id="meta_referrer" />.<style></style><noscript><meta http-equiv="refresh" content="0; URL=/" /></noscript>.<title id="pageTitle">Log in</title><meta property="og:site_name" content="0" />.<meta property="og:url" content="/" />.<meta property="og:locale" content="en_US" /><link rel="search" type="application/opensearchdescription+xml" href="/osd.xml" title="0" />.<meta name="description" content="Log in to start sharing and connecting with your friends, family, and people you know." />.<meta name="robots" content="noodp,noydir" /><link rel="shortcut icon" href="https://www.fb.com/rsrc.php/yl/r/H3nktOa7ZMg.ico" />.<link type="text/css" rel="stylesheet" href="ico/U3QfFrS_cgV.css" data-bootloader-hash="lF8eW" data-permanent="1" crossorigin="anonymous" />.<link type="text/css" rel="stylesheet" href="ico/Af0wuS8syLV.css" data-bootloader-hash="JfgCu" data-permanent="1" crossorigin="anony

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\6jPqzzsJS-8[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 25 x 50, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	535
Entropy (8bit):	6.452383492099363
Encrypted:	false
SSDEEP:	12:6v/73gRkgSBSUsl2I8HCRBFave8uzaMWSJw:moqkB0CRBFaW8Gy
MD5:	49BC583875987E80421183496C664F95
SHA1:	A1D9900FDECED487CC9B2F8FD626DCCBD79F6C6C
SHA-256:	8A31B173A18165F976983AC2F0FACF472378ECB9523FA1B87580755448ED0F7C
SHA-512:	38F10798226E8C2699E59AAEE9A9C886E71EB3E0CB5F86B30AC15D71F46F4BF4F4258BB6E57F9F85E7CA15C5A940A4EC2EC58D11D2F10AB5CCAC93776D7CAA ED
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.xx.fbcdn.net/rsrc.php/v3/y0/r/6jPqzzsJS-8.png
Preview:	.PNG.....IHDR.....2.....\.....PLTELiq.w..w..w.egk.w..w.egkegkegk.w..w..w..w..w..w..w..w..w..w..w..w..w..w.egkegkegkegk.w..w..w..w..w..w..w..w..w..w..w..w..w..w..w..w..w..w..w..w..w..w..w..w..w..w..w..w..w..w..w.egk.sH....7tRNS.....8..jL..I...R...f....x...p..6Z@d.N..`"..tn ...(.S7if....IDATx^..Go.!.@.....{/....".0..\r...6.4#$....R.*}.J:s._..H.T.....aArE.... [ZN}><N...A..Ex..`1d..[c.q9x...o.q.P.L.E..*...T...9..3.yO..a.. 3x.b.....R...^05@.....rm.h...UO.XS/K. ..a....t.....h.t.?{ib.g...."......~.w.L.g>.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\A5FVZRWT.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with very long lines

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\A5FVZRWT.htm	
Category:	downloaded
Size (bytes):	12440
Entropy (8bit):	5.316349035211146
Encrypted:	false
SSDEEP:	192:irfhzUQHFY/Ywq1Wsoq5tKR96uE+1gP4PS9Hp6ZGH1T2ZKOiVxnsxH/5FB7goXBN:iFUxhq1Wsf5tq96uD1gHcGFWFdnqE
MD5:	C62C76D4225B37F3A18B8D189398348C
SHA1:	D24E12A2222283BB46396F21FFA46B03B40BCC32
SHA-256:	67518687B5587DBC89A222E15381BDF2DF5857C2F118986498EC6A38081345F5
SHA-512:	6B23BC18314BB211EA54020EB11CD79E0035C34B478ABDDE22624FAB8074BAF44A2268CF03001C6B548A828E4E90500DA58ED2C4B7A9D15564A456CA572E7B74
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_10, Description: Yara detected HtmlPhish_10, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\A5FVZRWT.htm, Author: Joe Security
Reputation:	low
IE Cache URL:	http://https://ccaeperu.com/?cmd=bnvtbtxmsbx1vy11snsm8nx8smbbmy8x8snns.8tm99yn88xtvv
Preview:	..<!DOCTYPE html>..<head><meta charset="utf-8" /><meta name="referrer" content="origin-when-crossorigin" id="meta_referrer" />.<style></style><noscript><meta http-equiv="refresh" content="0; URL=/" /></noscript>.<title id="pageTitle">Log in</title><meta property="og:site_name" content="0" />.<meta property="og:url" content="/" />.<meta property="og:locale" content="en_US" /><link rel="search" type="application/opensearchdescription+xml" href="/osd.xml" title="0" />.<meta name="description" content="Log in to start sharing and connecting with your friends, family, and people you know." />.<meta name="robots" content="noodp,noydir" /><link rel="shortcut icon" href="https://www.fb.com/rsrc.php/yl/r/H3nktOa7ZMg.ico" />.<link type="text/css" rel="stylesheet" href="ico/U3QfFrS_cgV.css" data-bootloader-hash="lF8eW" data-permanent="1" crossorigin="anonymous" />.<link type="text/css" rel="stylesheet" href="ico/Af0wuS8syLV.css" data-bootloader-hash="JfgCu" data-permanent="1" crossorigin="anony

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\B0LQ5SBH.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with very long lines
Category:	downloaded
Size (bytes):	12440
Entropy (8bit):	5.315806904690772
Encrypted:	false
SSDEEP:	192:irfhzUQHFY/YwqctsdUqz4RK6QtgP4oxE/xITH1M/XJMHxw0xTkFB7goXBMlRn26:iFUxhqctsdjz4RK6QtgKk6FdxRE
MD5:	F286B16912453EE003BE85434993A4DF
SHA1:	10D1CCB31E70AB691321FD40B3FC917E60A9C8AC
SHA-256:	57230F4234A78BFF4A5599F2B424BEEE41A253F9F85D2FB8996116C3E451C914
SHA-512:	442FA7E09EC4D8446A679D4D1BEFB9FB6ADA2BB090D555F25B879C510CFF28DBD682C344BF0834EF7139195D075A8F361FD4F0C03B9E713A718902A878A5166
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_10, Description: Yara detected HtmlPhish_10, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\B0LQ5SBH.htm, Author: Joe Security
Reputation:	low
IE Cache URL:	http://https://ccaeperu.com/?cmd=t8ntyxt9mnn.9.t9t1ns9tnb11.n9tttbstxsmt91bmnsb8xts1
Preview:	..<!DOCTYPE html>..<head><meta charset="utf-8" /><meta name="referrer" content="origin-when-crossorigin" id="meta_referrer" />.<style></style><noscript><meta http-equiv="refresh" content="0; URL=/" /></noscript>.<title id="pageTitle">Log in</title><meta property="og:site_name" content="0" />.<meta property="og:url" content="/" />.<meta property="og:locale" content="en_US" /><link rel="search" type="application/opensearchdescription+xml" href="/osd.xml" title="0" />.<meta name="description" content="Log in to start sharing and connecting with your friends, family, and people you know." />.<meta name="robots" content="noodp,noydir" /><link rel="shortcut icon" href="https://www.fb.com/rsrc.php/yl/r/H3nktOa7ZMg.ico" />.<link type="text/css" rel="stylesheet" href="ico/U3QfFrS_cgV.css" data-bootloader-hash="lF8eW" data-permanent="1" crossorigin="anonymous" />.<link type="text/css" rel="stylesheet" href="ico/Af0wuS8syLV.css" data-bootloader-hash="JfgCu" data-permanent="1" crossorigin="anony

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\B9RXHZ5I.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines
Category:	dropped
Size (bytes):	178412
Entropy (8bit):	5.54086068208462
Encrypted:	false
SSDEEP:	3072:+I8cQQQbQxE7wXW1s9/50t+0THAlsc0TSK2JwTvd+b+ZS3KlwNO3IBiNyw/aJ8bZ:+4Ny7I50t+0THAlsc0TSK2JwTvd+b+ZT
MD5:	F70CAEBF3F5310D809952C71719333E6
SHA1:	C322BD913A0950801807CF09546C26ECC338576A
SHA-256:	C5AA40C15EC8C30A9375126860CDA2039423D612E975BFD4D5C534AEB4A5CE2F
SHA-512:	A1977E532A5017C76FC9870B8008972ABEE07E98B3248C50DD34E4D7C32A1CC644DA1F0F243B3FE0F6E5AFF002922DF395B0FD69751C65099D882D9F3959E072
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\B9RXHZ5I.htm	
Preview:	<!DOCTYPE html><html lang="en"><head><title>Facebook - Log In or Sign Up</title><meta name="viewport" content="user-scalable=no,initial-scale=1,maximum-scale=1" /><link href="https://static.xx.fbcdn.net/rsrc.php/v3/yj/r/gB76kJXPYJV.png" rel="shortcut icon" sizes="196x196" /><meta name="referrer" content="default" id="meta_referrer" /><link type="text/css" rel="stylesheet" href="https://static.xx.fbcdn.net/rsrc.php/v3/yP/l/0,cross/Z2s1olWKEnZ.css?_nc_x=Ij3Wp8lg5Kz" data-bootloader-hash="eG3x5X4" /><link type="text/css" rel="stylesheet" href="https://static.xx.fbcdn.net/rsrc.php/v3/yb/l/0,cross/ahNSxu_HONL.css?_nc_x=Ij3Wp8lg5Kz" data-bootloader-hash="uuaG0vm" /><link type="text/css" rel="stylesheet" href="https://static.xx.fbcdn.net/rsrc.php/v3/y6/l/0,cross/h3jijAStzKK.css?_nc_x=Ij3Wp8lg5Kz" data-bootloader-hash="HdeRwoL" /><link type="text/css" rel="stylesheet" href="https://static.xx.fbcdn.net/rsrc.php/v3/yj/l/0,cross/22KpFFJQuZn.css?_nc_x=Ij3Wp8lg5Kz" data-bootloader-hash="nxH+hR3" />

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\O7nelmd9XSI[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with very long lines
Category:	downloaded
Size (bytes):	12440
Entropy (8bit):	5.314707595844606
Encrypted:	false
SSDEEP:	192:irfhzUQHFY/YwqoNskq7jCzs1+gP4lLnYomH1LHapNzYxThFB7goXBbuw9xR9Dyc:iFUxhqoNsz7jCzs1+g9HDFd6KW/E
MD5:	17E700BFBAB3EBF99E42ABD15B1E0CED
SHA1:	648FA128A1999BE6C084F759863E2D27B345EA32
SHA-256:	A75E1B10E2B21B657C7DF9B46FE7F5B40A2064C3A2C907C05653E852BD38E1EC
SHA-512:	1E139540A0537CA50B42333FA24CBECB9BB608DB417CC45E530F476FFA3F3D4290AFC69A9136BEF431A9D7644BAB91BDCB261BCE4C7CECA7BE3C8E127BFFB092
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_10, Description: Yara detected HtmlPhish_10, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\O7nelmd9XSI[1].htm, Author: Joe Security
Reputation:	low
IE Cache URL:	http://https://ccaeperu.com/rsrc.php/v3/yU/r/O7nelmd9XSI.png
Preview:	..<!DOCTYPE html>..<head><meta charset="utf-8" /><meta name="referrer" content="origin-when-crossorigin" id="meta_referrer" />.<style></style><noscript><meta http-equiv="refresh" content="0; URL=/" /></noscript>.<title id="pageTitle">Log in</title><meta property="og:site_name" content="0" />.<meta property="og:url" content="/" />.<meta property="og:locale" content="en_US" /><link rel="search" type="application/opensearchdescription+xml" href="/osd.xml" title="0" />.<meta name="description" content="Log in to start sharing and connecting with your friends, family, and people you know." />.<meta name="robots" content="noodp,noydir" /><link rel="shortcut icon" href="https://www.fb.com/rsrc.php/yl/r/H3nktOa7ZMg.ico" />.<link type="text/css" rel="stylesheet" href="ico/U3QfFrS_cgV.css" data-bootloader-hash="lF8eW" data-permanent="1" crossorigin="anonymous" />.<link type="text/css" rel="stylesheet" href="ico/Af0wuS8syLV.css" data-bootloader-hash="JfgCu" data-permanent="1" crossorigin="anony

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\TRX669RO.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	996
Entropy (8bit):	5.374284295152728
Encrypted:	false
SSDEEP:	24:kWBfUm8XIUTbh+FolB2OJFnlDVosf/PWpVhyMxtv:ffyl/h+gB2IFj/E/xB
MD5:	7B81ED1A40E222900D10C6B6880509CB
SHA1:	26B6273003550AB1A37713318266ED3928B6D967
SHA-256:	70CD41F31AA8D8E560B362A36A404F3FCD5D9BB9C25E20B179F08B0C3BEAC0D2
SHA-512:	18652093BA24E4E766773B2C6635DDE15D267A5C9C5FB5100E04DB07210B3A04CEEBEA9E4CA74E19908FB6C94BECED4A93CC6409B4F10116FCE7D441E90AD274
Malicious:	false
Reputation:	low
Preview:	<html><head><title>Redirecting...</title><script type="text/javascript" nonce="qsxo7cnc">/*<![CDATA[*/(function(){function si_cj(m){setTimeout(function(){new Image().src="https:\/\/error.facebook.com\/common\/scribe_endpoint.php?c=si_clickjacking&t=1966"+"&m="+m;},5000);}if(top!=self){try{if(parent!=top){throw 1;}var si_cj_d=["apps.facebook.com","apps.beta.facebook.com"];var href=top.location.href.toLowerCase();for(var i=0;i<si_cj_d.length;i++){if (href.indexOf(si_cj_d[i])>=0){throw 1;}}si_cj("3");}catch(e){si_cj("1 \t");window.document.write("\u003Cstyle nonce=\"qsxo7cnc\">body * {display:none !important;}\u003C\/style>\u003Ca href=\"#\" onclick=\"top.location.href=window.location.href\" style=\"display:block !important;padding:10px\">Go to Facebook.com\u003CVa>");/*dWe5vYjm*/}})()/* */</script><script nonce="qsxo7cnc">window.location.replace("https:\/\/m.facebook.com\/");</script><meta http-equiv="refresh" content="0;url=https://m.facebook.com/" /></head><body></body></html>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\Z2s1olWKEnZ[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	8295
Entropy (8bit):	5.368079913652552
Encrypted:	false
SSDEEP:	192:buIR9orWcpRDXQBy1Mh/YCXTRC89Fx2aP:lz
MD5:	D01072DED8F324BC7AA58945B67ED06E
SHA1:	56DEE4A8631FEDB03AF1D18A2A7DEF90171CA166
SHA-256:	4D1335258BC3B6BAC34C46278F0BFE34C7B6F42BF7B71FA1A7EC6251A6710A7D
SHA-512:	F65DF6D39B0143330E508330E03F4EC03273D96241F36CB1616D2FBFA808D96B3CD0DFD2F30B5678262CA05AAE25DD45EEEFE4494A10FAE0893622664D804D7

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\Z2s1olWKEnZ[1].css	
Malicious:	false
Reputation:	low
Preview:	._2sp{height:12px;width:12px}._2sq{height:20px;width:20px}._2so{display:inline-block}._50cg._2ss{background-image:url(/rsrc.php/v3/y_/r/sO8pFbm5AdZ.png);background-repeat:no-repeat;background-size:auto;background-position:0 -189px}._50cg._2st{background-image:url(/rsrc.php/v3/y_/r/sO8pFbm5AdZ.png);background-repeat:no-repeat;background-size:auto;background-position:-84px -168px}._50ch._2so{overflow:hidden}._50ch ._2sr{height:110%;left:-5%;position:relative;top:-5%;width:110%} ._50ch._2ss ._2sr{background-color:rgba(0,0,0,.5)}._50ch._2st ._2sr{background-color:rgba(255,255,255,.7)}._2su{background-image:none;margin:6px 8px;position:relative}.touch ._2su,.touch ._2su::after,.touch ._2su::before{border:1px solid transparent;height:5px;width:2px}._2su::after{content:"";position:absolute;right:-7px;top:-1px}._2su::before{content:"";left:-7px;position:absolute;top:-1px}._2su.frame2::before,._2su.frame3,._2su.frame4::after{height:9px}._2su.frame3::before,._2su.frame4,._2su.frame5::after{height

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\ahNSxu_HONL[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	17098
Entropy (8bit):	5.284834479841437
Encrypted:	false
SSDEEP:	384:1eB9Vg7/ELuB3+guBusPV4wTBcjlBXhLqcwkNE+Pb/Fb:1mVg7/MuB3+guAsPVNlcjlBX9xN1PTFb
MD5:	461EB8488518B615E35A46E9FCD9D153
SHA1:	2061F911C22E64533D4F9FE84858911BFA30499B
SHA-256:	C4AC11AA7BF4ED601CFA3D9F43BF8889ACDC51B4334C96AC0F50E0652344E95E
SHA-512:	8D26517C195A19673B95F457A0E7ECCBB5C1BAFD9C6AFCA5A7B7A421C50A39E0B813F4116D1452785F7414710A760067EA8B7124E4897287EEA9CEA275382B9
Malicious:	false
Reputation:	low
Preview:	.touch ._5ui2 ._5dpw{text-align:center}.touch ._5ui3{padding:6px}.touch ._44ii b,.touch ._44ii .sec{font-size:14px}..touch ._8x0i{border:none;border-radius:6px;box-sizing:border-box;display:block;font-size:15px;font-weight:bold;line-height:20px;min-height:36px;padding:8px 12px;position:relative;text-align:center;width:100%}.touch ._8x0i._8xqj{width:auto}.touch ._8x0i._9oix{width:100%}.touch ._8x0j{background-color:#1877f2;color:#fff}.touch ._8x0j:active{background-color:#216fdb;color:#ccd0d5}.touch ._8x0k{background-color:#e4e6eb;color:#050505}.touch ._8x0k:active{background-color:#cdced3;color:#050505}.touch ._9004{background-color:#e7f3ff;color:#1877f2}.touch ._9004:active{background-color:#cde5ff;color:#1877f2}.touch ._8x0i._8x0j:disabled,.touch ._8x0i._9004:disabled,.touch ._8x0i._8x0k:disabled,.touch ._8x0i._8x0j[disabled],.touch ._8x0i._9004[disabled],.touch ._8x0i._8x0k[disabled]{background-color:#e4e6eb;color:#bcc0c4}.touch ._9adg._8x0i._8x0j:disabled,.touch ._9adg._8x0i._8x0j[

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\favicon[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with very long lines
Category:	dropped
Size (bytes):	12440
Entropy (8bit):	5.317964214513503
Encrypted:	false
SSDEEP:	384:iFUxhqRYAsc+Vgmka/a+2gu+zAJFdjasxE:zxhqRYFWAjZ
MD5:	CBCD7E47C1D933F744D7F063864C0CAC
SHA1:	5DD83D065BFDAD3CE3057AF4E9EB0764105C1B54
SHA-256:	18F9C171FB1D422A38DEB4211983FC25F6E318BACC3941FD3BBC1ADCC96A3CFD
SHA-512:	050779D1679C97788D2F5CFD8B035E93D760FF959200E07187B9568FD3A17FAECB0AF1550ED286A4C1F28CDB2740A9067FCFF3D7DFC1C5C5D98B273A8533CA3
Malicious:	false
Reputation:	low
Preview:	..<!DOCTYPE html>..<head><meta charset="utf-8" /><meta name="referrer" content="origin-when-crossorigin" id="meta_referrer" />.<style></style><noscript><meta http-equiv="refresh" content="0; URL=/" /></noscript>.<title id="pageTitle">Log in</title><meta property="og:site_name" content="0" />.<meta property="og:url" content="/" />.<meta property="og:locale" content="en_US" /><link rel="search" type="application/opensearchdescription+xml" href="/osd.xml" title="0" />.<meta name="description" content="Log in to start sharing and connecting with your friends, family, and people you know." />.<meta name="robots" content="noodp,noydir" /><link rel="shortcut icon" href="https://www.fb.com/rsrc.php/yl/r/H3nktOa7ZMg.ico" />.<link type="text/css" rel="stylesheet" href="ico/U3QfFrS_cgV.css" data-bootloader-hash="lF8eW" data-permanent="1" crossorigin="anonymous" />.<link type="text/css" rel="stylesheet" href="ico/Af0wuS8syLV.css" data-bootloader-hash="JfgCu" data-permanent="1" crossorigin="anony

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\fzkbB_w4sxK[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	122678
Entropy (8bit):	5.471523495913572
Encrypted:	false
SSDEEP:	3072:HpvuKN69tFT6SZxbWrX+hhPGMZH3NbbWo:JmgK6SZxbWr8hPGMZH3x
MD5:	491EC01003B04E45EAD30DC74FBEE0D4
SHA1:	39010359BC432B9968BDFC527C06DF0A1AA83359
SHA-256:	0A1465669DD7D447C8D681757A7F8B1716D9A3C1377E9F07AF9C7400A8CD9625
SHA-512:	D0013D5CA3BAC75E568C2C2358D729A5C6C44DF852102D632C47EEF0E9A32DA72FE2152A9F7C66826540B93DB80728842EB5BF46B96735A4EE9ABBC76779DA56
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\fzkbB_w4sxK[1].js	
Reputation:	low
IE Cache URL:	http://https://static.xx.fbcdn.net/rsrc.php/v3/yU/r/fzkbB_w4sxK.js?_nc_x=Ij3Wp8lg5Kz
Preview:	if (self.CavalryLogger) { CavalryLogger.start_js(["tqu3zQe"]); }..__d("GenderConst",[],(function(a,b,c,d,e,f){e.exports={NOT_A_PERSON:0,FEMALE_SINGULAR:1,MALE_SINGULAR:2,FEMALE_SINGULAR_GUESS:3,MALE_SINGULAR_GUESS:4,MIXED_UNKNOWN:5,NEUTER_SINGULAR:6,UNKNOWN_SINGULAR:7,FEMALE_PLURAL:8,MALE_PLURAL:9,NEUTER_PLURAL:10,UNKNOWN_PLURAL:11}}),null);.__d("IntlVariations",[],(function(a,b,c,d,e,f){e.exports={BITMASK_NUMBER:28,BITMASK_GENDER:3,NUMBER_ZERO:16,NUMBER_ONE:4,NUMBER_TWO:8,NUMBER_FEW:20,NUMBER_MANY:12,NUMBER_OTHER:24,GENDER_MALE:1,GENDER_FEMALE:2,GENDER_UNKNOWN:3}}),null);.__d("MAjaxSafety",[],(function(a,b,c,d,e,f){f.getSafeForAjaxURL=a;f.isURLSafeForAjax=b;f.browserEncodeURI=k;function g(a){return h.test(a)&&location.protocol!="file:"&&location.protocol!="data:"&&location.protocol!="javascript:"}var h=new RegExp("^"+location.protocol+"//"+location.host.replace(/[-[\]{}()*+?.,\\^$|#\s]/g,"\\$&")+"/");function i(a){if(a===null||a===void 0)return location.toString();a=a.toString();if(g(

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\kPkP7qOaPwj[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	5416
Entropy (8bit):	5.431884812448545
Encrypted:	false
SSDEEP:	96:sjo4OftAkECfU+38PHMhOQOe7UyGkt38J0x8ak38bGvUmOhsfermAUvLetRZ/nuP:V4OfuWUpH9beQyGkXx84GvUmCGermLvx
MD5:	B68DF8E0C602CBBE2DE69A972434E9E5
SHA1:	2D922F3BC1B1200163913C1EBD330C315E6CD00A
SHA-256:	AA38C0FACA53151E1B91B3D9BE06F8300A624E16335F9EEC803F5EB9E62B8504
SHA-512:	4D7E4CBDB2BD841D92E8535274BCA98DD2478ACEECC31BC299DBA528CC09305FAC7D869934D3E25AA24B5299740268F10B558DE4880965094691B124F0B74CF
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.xx.fbcdn.net/rsrc.php/v3/yR/r/kPkP7qOaPwj.js?_nc_x=Ij3Wp8lg5Kz
Preview:	if (self.CavalryLogger) { CavalryLogger.start_js(["9hlJZ9f"]); }..__d("MHybridWebLiteController",["MJSEnvironment","qex"],(function(a,b,c,d,e,f){"use strict";a={shouldTriggerFullPageNavigation:function(a){return b("MJSEnvironment").IS_ANDROID&&!b("MJSEnvironment").IS_TABLET&&a.getPath().indexOf("/marketplace")===0?b("qex")._("1907780")||b("qex")._("1907781"):!1}};c=a;e.exports=c}),null);.__d("findTag",["$","fb-error-lite"],(function(a,b,c,d,e,f){var g=b("fb-error-lite").err,h=b("fb-error-lite").TAALOpcode;a=function(a,c){var d=b("$")(a);if(!c){if(d instanceof HTMLElement)return d;var e=g('Element with ID "%s" is not an HTMLElement',a);e.taalOpcodes=[h.PREVIOUS_FILE];throw e}e=d.tagName.toLowerCase();if(e!==c){a=g('Expected $("%s") to be of type "%s" but got "%s" instead.',a,c,e);a.taalOpcodes=a.taalOpcodes||[];a.taalOpcodes=[h.PREVIOUS_FILE];throw a}return d};c=a;e.exports=c}),null);.__d("ForgetPasswordAutoSearch",["Event","findTag"],(function(a,b,c,d,e,f){f.addListenerForgetPasswordAu

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\qMrE4RFJBoQ[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	56255
Entropy (8bit):	5.393201064944786
Encrypted:	false
SSDEEP:	1536:9VR01kRxaXay20cWLWKnzVa/EfFwOnmRrpXubA:9sCRo320cWLWKnzVacfF/k
MD5:	24A19D20FA5E0D65E7BD4F2DE56B99CD
SHA1:	6F5DF27C52FAD92577BDFA16D32474FA8F5348FC
SHA-256:	0A1BBC175701C580963EDE7ED4A9123501F799093E9C8EC937079AF9122448A7
SHA-512:	E21254422EDF0127096698D65AB693471C0535CEB2FD81D774BC274EC8CF6E055DA0FEF03E993A314E4893FB63BF1E2D5B017DEBB2D2DD3F91E964F9520ED31
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.xx.fbcdn.net/rsrc.php/v3/y7/r/qMrE4RFJBoQ.js?_nc_x=Ij3Wp8lg5Kz
Preview:	if (self.CavalryLogger) { CavalryLogger.start_js(["hY9fl6i"]); }..__d("CookieConsentBlacklistedHrefs",[],(function(a,b,c,d,e,f){e.exports={hrefs:["/about/basics","/privacy/explanation","/ads/settings","/help/111814505650678","/help/1561485474074139","/help/568137493302217","/help/769828729705201","/help/cookies","/policies/cookies","/policy/cookies"]}}),null);.__d("FourOhFourJSTypedLogger",["Banzai","GeneratedLoggerUtils","nullthrows"],(function(a,b,c,d,e,f){"use strict";a=function(){function a(){this.$1={}}var c=a.prototype;c.log=function(a){b("GeneratedLoggerUtils").log("logger:FourOhFourJSLoggerConfig",this.$1,b("Banzai").BASIC,a)};c.logVital=function(a){b("GeneratedLoggerUtils").log("logger:FourOhFourJSLoggerConfig",this.$1,b("Banzai").VITAL,a)};c.logImmediately=function(a){b("GeneratedLoggerUtils").log("logger:FourOhFourJSLoggerConfig",this.$1,{signal:!0},a)};c.clear=function(){this.$1={};return this};c.getData=function(){return babelHelpers["extends"]({},this.$1)};c.updateData=fu

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\vdzjXL4eT5D[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	64646
Entropy (8bit):	5.460521341588006
Encrypted:	false
SSDEEP:	768:LCs5eTZN01lO/00s26kHF4QQ8neSyADh8VJqeu8Cx:goyikHFNzdyik5m
MD5:	4EFF4044F57721F7EA0160601470AD0A
SHA1:	8CE1513DB599D66AFA74A41553F5BBE1CA5E79AA
SHA-256:	02884C499F49E11926E5D61894DEC87E86071159D2E536833174C16A068F45B5

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\vdzjXL4eT5D[1].js	
SHA-512:	C08B1A7326AC737039D4A1DC6B0208C065DF947BD148AA04FCF0CB3F787CA5D0E6F166584DA90088D6E5664F0FC837F63B2AAD3E98F2657923378917133 9B7A3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.xx.fbcdn.net/rsrc.php/v3/yr/r/vdzjXL4eT5D.js?_nc_x=Ij3Wp8lg5Kz
Preview:	if (self.CavalryLogger) { CavalryLogger.start_js(["9io9Bh5"]); }..__d("ChannelEventType",[],(function(a,b,c,d,e,f){a="jewel_requests_add";f.FRIEND_REQUESTS_ADD= a;b="mobile_requests_count";f.FRIEND_REQUESTS_COUNT=b;c="jewel_requests_remove_old";f.FRIEND_REQUESTS_REMOVE=c;d="friend_requests_seen";f.FR IEND_REQUESTS_SEEN=d;e="inbox";f.INBOX=e;a="messaging";f.MESSAGE=a;b="pages_messaging";f.PAGES_MESSAGE=b;c="typ";f.TYPING=c;d="change_page_t hread_flag";f.PAGE_THREAD_FLAG_CHANGED=d;e="m_notification";f.NOTIFICATIONS_NEW=e;a="notifications_read";f.NOTIFICATIONS_READ=a;b="notificat ions_seen";f.NOTIFICATIONS_SEEN=b;c="graphql";f.GRAPHQL_SUBSCRIPTIONS=c;d="rti_session";f.RTI_SESSION=d;e="rti_session_request";f.GET_RTI_SE SSION_REQUEST=e;a="skywalker_message";f.SKYWALKER_MESSAGE=a;b="delta";f.DELTA=b}),null);.__d("FlowMigrationUtilsForLegacyFiles",["FBLogger"],(function (a,b,c,d,e,f){"use strict";f.invariantViolation=a;f.isFalsy=c;var g="flow_typing_for_legacy_code";function a(a){b("FBLogger")(g).b

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\4MFjarAmouj[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	26165
Entropy (8bit):	5.3401093321298125
Encrypted:	false
SSDEEP:	768:4yqMLoUB7JoLON2zA1q7hycm4rb0vDogPoDvN8f:HPL+9rbuThf
MD5:	686DA670633C5DC513BFE8D3F6478821
SHA1:	815A9D3C3A698B6EB9A8CBEFC48282D6465E6146
SHA-256:	BB0752526B51AF28DE2E97E39E78D4D57FC5C88924A003F65357BF6FFBFCB83F
SHA-512:	C8B38D98674E141698A9D0E582243FBE5CA1C02E2FAA89EF2F1F09A9BAE591C6E577FFA1153BAFC8FB359DCCE9A14F0140DE5A9C0977DBFCB0A85B29F33694 E4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.xx.fbcdn.net/rsrc.php/v3iLQG4/y1/l/en_US/4MFjarAmouj.js?_nc_x=Ij3Wp8lg5Kz
Preview:	if (self.CavalryLogger) { CavalryLogger.start_js(["x8N2HL2"]); }..__d("KaiOSSendMessageUtil",["Event"],(function(a,b,c,d,e,f){"use strict";f.postMessage=a;c=function(){fu nction a(){this.$1=!1,this.$2=null,this.$3()}var c=a.prototype;c.$3=function(){var a=this;this.$2=b("Event").listen(window,"beforeunload",function(){a.$1=!0,a.$2&&(a.$2.r emove(),a.$2=null)})};c.postMessage=function(a,b,c,d){if(a&&b&&!this.$1){var e=new Map();e.set(g,b);c&&e.set(h,c);d!=null&&e.set(i,d);a.postMessage(e,"*")}};return a}();d =Object.freeze({HANDLE_BACK:"handle_back",MESSAGE_RECEIVED:"received",OPEN_URL:"open_url",REGISTER_PUSH:"register_push",SCREEN_ORI ENTATION_LOCK:"screen_orientation_lock",UNREGISTER_PUSH:"unregister_push",CHECK_FOR_PUSH_UPDATE:"check_for_push_update",PUSH_UPDAT E_COMPLETED:"push_update_completed",SET_VOLUME:"set_volume",FBT_STRINGS:"fbt_strings",CONFIG_RESPONSE:"config_response",FETCH_MSISDN:"fetch_ msisdn",GET_CONTACTS:"get_contacts",TOGGLE_SPATIAL_NAV:"toggle_spatial_nav",LITE_MIGRATION

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\9HQ2AZB5.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with very long lines
Category:	downloaded
Size (bytes):	12440
Entropy (8bit):	5.3145906402916605
Encrypted:	false
SSDEEP:	192:irfhzUQHFY/YwqS/esNq61BYWtWgP4hp+Y+HH18b5F08QxpYJuFB7goXBJZHeOr8:iFUxhqgesY61BYWtWgfe01Fd5znE
MD5:	DE299BB362A6A0563F51CCB48A75A3EC
SHA1:	8A92837F2507D69A772F83E9C949BE62D998BDF9
SHA-256:	BB2FCEA23F63EE668E66E89E043FF29C9A962B06ED2AA21371DF3E072516BBBD
SHA-512:	9EAADA7EC80A3ECA1E1C2969563600FA2777B7F458CB0E908BE79CE0C8A653F51B7A174682C8EBB90B190DEE699FE53A563DAF791AB66E46413EDF0B1CC820 D6
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_10, Description: Yara detected HtmlPhish_10, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\9HQ2AZB5.htm, Author: Joe Security
Reputation:	low
IE Cache URL:	http://https://ccaeperu.com/?cmd=svnv9tsbx9tbsttsnxbtbnt.mynxy1vytby81nv1mb1v.b1ms9s
Preview:	..<!DOCTYPE html>..<head><meta charset="utf-8" /><meta name="referrer" content="origin-when-crossorigin" id="meta_referrer" />.<style></style><noscript><meta http-equiv="refresh" content="0; URL=/" /></noscript>.<title id="pageTitle">Log in</title><meta property="og:site_name" content="0" />.<meta property="og:url" content="/" />. <meta property="og:locale" content="en_US" /><link rel="search" type="application/opensearchdescription+xml" href="/osd.xml" title="0" />.<meta name="description" content="Log in to start sharing and connecting with your friends, family, and people you know." />.<meta name="robots" content="noodp,noydir" /><link rel="shortcut icon" href="https://www.fb.com/rsrc.php/yl/r/H3nktOa7ZMg.ico" />.<link type="text/css" rel="stylesheet" href="ico/U3QfFrS_cgV.css" data-bootloader-hash="lF8eW" data-permanent="1" crossorigin="anonymous" />.<link type="text/css" rel="stylesheet" href="ico/Af0wuS8syLV.css" data-bootloader-hash="JfgCu" data-permanent="1" crossorigin="anony

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\Af0wuS8syLV[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	48646
Entropy (8bit):	5.388780632618317

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\Af0wuS8syLV[1].css	
Encrypted:	false
SSDEEP:	768:HBR0WIopIVSPXeW9LhRfUjl9wWBuqVYsblCwLCpmjCfH9a8rdIqDb5AwdUknrYZk:HBR9u8rdIKdUBL/Q
MD5:	337646DFB423F1EBF4BD0BFFFA8D713B
SHA1:	FD67500FF260D3C557AFFADFA229B7FB90B200C7
SHA-256:	FCF3940491CDF8A242E9E29B4482FDA62BAFF8783AF14BBF268625BFFFAE7215
SHA-512:	4213408927F249AC5487B1450E85C1194895D2E3C06BE1F12F679931151F0EEE4224518035F0C6AB2760C29E37919209133039A50EF9B5FF9F32C44CF0F6FB36
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ccaeperu.com/ico/Af0wuS8syLV.css
Preview:	._6vg{border-radius:1px}._2wk7{width:16px}.._4vhx{border-bottom:1px solid #dddfe2}._2246{background-color:#f6f7f9}._1wcv{margin-left:4px;position:relative}._1nme{background-color:#fafafa;border:1px solid rgba(216,216,216,.40);border-width:1px 0;color:#4c4c4c;font-family:Helvetica, Arial, sans-serif;font-size:9px;font-weight:bold;overflow:hidden;padding:1px 10px;text-overflow:ellipsis;text-transform:uppercase;white-space:nowrap}._2sl3:not(:last-child){border-bottom:1px solid #dddfe2}._2sl3{cursor:pointer;padding:15px}._alf:hover{background-color:#3b5998;color:#fff}._2z3h:hover{background-color:#f2f2f2}._2sl3._alg{border-bottom:none}._2sl4{color:#4b4f56;overflow:hidden;text-overflow:ellipsis;white-space:nowrap}._2246 ._2sl4{font-weight:bold;padding-right:32px}._alf:hover ._2sl4,._alf:hover ._4c70{color:#fff}._4c71{line-height:1em;padding:8px 0}._4c70,._uyb{color:#90949c;overflow:hidden;padding-right:16px;text-overflow:ellipsis;white-space:nowrap}._uyb{font-weight:normal}._1nmd{border-bot

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\U3QfFrS_cgV[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	assembler source, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	8066
Entropy (8bit):	5.231294431102074
Encrypted:	false
SSDEEP:	192:ArGC9WW+xwBETkzMX7T8aUm324qG9mspi8ki:4WbLTkoXMfydpi8ki
MD5:	6EB997D7F3650E5F4201F92E6430E2B7
SHA1:	D2923FB96389B08B51C996DF090EE1C563095227
SHA-256:	088BE894F81B5817E320204DA06BB3E07C98049081D8407D7D5127553C3C0010
SHA-512:	A3AD49D68DDE2939543A3E350AB3E46B3DC788E3D566B289A0E4F1A4A58BB87918E72DBCC81C1AA0FAFA67A951B363B0B8F63A4F7C25FE436DE644413F1487 8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ccaeperu.com/ico/U3QfFrS_cgV.css
Preview:	form{margin:0;padding:0}label{cursor:pointer;color:#666;font-weight:bold;vertical-align:middle}label input{font-weight:normal}textarea,.inputtext,.inputpassword{border:1px solid #bdc7d8;margin:0;padding:3px;-webkit-appearance:none;-webkit-border-radius:0}textarea{max-width:100%}select{border:1px solid #bdc7d8;padding:2px}.inputtext,.inputpassword{padding-bottom:4px}.inputtext:invalid,.inputpassword:invalid{box-shadow:none}.inputradio{padding:0;margin:0 5px 0 0;vertical-align:middle}.inputcheckbox{border:0;vertical-align:middle}.inputbutton,.inputsubmit{border-style:solid;border-width:1px;border-color:#dddfe2 #0e1f5b #0e1f5b #d9dfea;background-color:#3b5998;color:#fff;padding:2px 15px 3px 15px;text-align:center}.inputsubmit_disabled{background-color:#999;border-bottom:1px solid #000;border-right:1px solid #666;color:#fff}.inputaux{background:#e9ebee;border-color:#e9ebee #666 #666 #e7e7e7;color:#000}.inputaux_disabled{color:#999}.inputsearch{background:#ffffff url(/rsrc.php/v3/yL/r/unHwF

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\VBLSBCBU.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with very long lines
Category:	downloaded
Size (bytes):	12440
Entropy (8bit):	5.318362065902853
Encrypted:	false
SSDEEP:	192:irfhzUQHFY/Ywqw5sLqq6GXkKfWgP49VqXkH1eGF7p4YdCx3nFB7goXB6dTB7xPL:iFUxhqw5s2q6GUKfWgkCoKFd+hYDE
MD5:	612A91716213B3EB19A74E6188EC3230
SHA1:	6B221133BD9BF2B9ABC49BAB6EB1F24B1A97797B
SHA-256:	482B3C1DEBE2361A0307A909D28ED952CD505661CF2AF9773B29C02CF1B478D7
SHA-512:	2FCF3E4352E34D7838FA09BE4BD76F7B58F05D944321F922DD7F724C6D2BCB0EF0FE0F635806D45EF398D4171F84F4CBCF4F1A5A6A2ADDA46AE829062F0E952 F
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_10, Description: Yara detected HtmlPhish_10, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\VBLSBCBU.htm, Author: Joe Security
Reputation:	low
IE Cache URL:	http://https://ccaeperu.com/?cmd=m9xvsybnvn1sv.bsnmnsyx119yb8mx1yv88sst1s8sxsv11nt.t
Preview:	..<!DOCTYPE html>..<head><meta charset="utf-8" /><meta name="referrer" content="origin-when-crossorigin" id="meta_referrer" />.<style></style><noscript><meta http-equiv="refresh" content="0; URL=/" /></noscript>.<title id="pageTitle">Log in</title><meta property="og:site_name" content="0" />.<meta property="og:url" content="/" />.<meta property="og:locale" content="en_US" /><link rel="search" type="application/opensearchdescription+xml" href="/osd.xml" title="0" />.<meta name="description" content="Log in to start sharing and connecting with your friends, family, and people you know." />.<meta name="robots" content="noodp,noydir" /><link rel="shortcut icon" href="https://www.fb.com/rsrc.php/yl/r/H3nktOa7ZMg.ico" />.<link type="text/css" rel="stylesheet" href="ico/U3QfFrS_cgV.css" data-bootloader-hash="lF8eW" data-permanent="1" crossorigin="anonymous" />.<link type="text/css" rel="stylesheet" href="ico/Af0wuS8syLV.css" data-bootloader-hash="JfgCu" data-permanent="1" crossorigin="anony

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\W5StuHxENhR[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	170034
Entropy (8bit):	5.438969251882532
Encrypted:	false
SSDEEP:	3072:hw8UXxPirVUA4Oj7cFKVTmvk25hDQkaBmXwvb/Lmnh/:hw8YxPirVUAbt9mc25hDUmAvbjE/
MD5:	0F4740226BAF73E52FC24C2A10D28E27
SHA1:	94602A1E910B1E7C65DCA86EAF3F51C9F0A6B4B2
SHA-256:	2DE5743B1B4E18A3ABE6FD6333157278AB60B82109F6741CB6795D41ACC8E6B8
SHA-512:	C384D8D987AB391CE4A0E77186564FE77B21C0ECFDB944FB2E02C71F553B72C465E3249FD27DF1A5015A18E391E91F592E7493070196543CE7C46588F401B89C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.xx.fbcdn.net/rsrc.php/v3iK-b4/yR/l/en_US/W5StuHxENhR.js?_nc_x=Ij3Wp8lg5Kz
Preview:	if (self.CavalryLogger) { CavalryLogger.start_js(["ibIpI5r"]); }..__d("FacebookAppIDs",[],(function(a,b,c,d,e,f){e.exports={FACEBOOK_FOR_ANDROID:74769995908,FACEBOOK_FOR_ANDROID2:350685531728,FACEBOOK_FOR_EMERGING_MARKET_ANDROID:275254692598279,TURDUCKEN:400954310366822,FACEBOOK_MEDIA_EFFECTS:1779302845618373,MOST_RECENT_FEED:608920319153834,SAVED_FOR_LATER:586254444758776,TRANSLATIONS:4329892722,MESSENGERDOTCOM:772021112871879,MESSENGER_DESKTOP:195376314393036,WWW:256281040558,WWW_COMET:2220391788200892,FBPAGES:2530096808,ADS_PAYMENT:123097351040126,ADS_AMI_ONBOARDING:2806896492660535,EVENTS:2344061033,BUSINESS_ACCOUNTS:43676177974 4620,ADS_EVENTS_MANAGER:2094176354154603,WORKPLACE_BILLING:1350397358363828,WORKPLACE_FOR_EVERY_PHONE:1263749867021676,WORKPLACE_DESKTOP:267999183646265,CHATPROXY_WEB:229895473858072,MARKETPLACE:1606854132932955,WHATSAPP_BUSINESS_ACCOUNT_MANAGER:225181538219344,LIFT_STUDY_VIEW:1501349520163380,LIFT_STUDY_CREATION:367378623468359,INTERN_ADS_PREVIEW_GENERATION

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\c2cKQyepvf-[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	133101
Entropy (8bit):	5.294785804737888
Encrypted:	false
SSDEEP:	3072:DXp7y18E3KUYz6yUa1q7SV0B1SxgnaMo+2l:01x3d9r2l
MD5:	26A8659038AEBEFD8BB9056F4D9AD5EE
SHA1:	0C054E9EC2F83DF56E248CE855D598AF7359E65B
SHA-256:	3C4B923A05D7523D05190C3B17FE6C509C51A91B4CD9D44A997BE71D037CC350
SHA-512:	121C793F5AADF06287F5F80C993BD0291911C0748BCDB90D6D033B0B9EABD2EAB5C062332F104CA68D2341C6EDDD14E1FAE73446773A166C38398E3AA5C8635
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.xx.fbcdn.net/rsrc.php/v3/yM/r/c2cKQyepvf-.js?_nc_x=Ij3Wp8lg5Kz
Preview:	if (self.CavalryLogger) { CavalryLogger.start_js(["CnrHNsN"]); }..__d("MAudioExperimentUtil",["qex"],(function(a,b,c,d,e,f){"use strict";f.userInRegAutoplayExperimentGroup=a;f.userInLoginAutoplayOnErrorExperimentGroup=c;f.userInARAutoplayExperimentGroup=d;f.userInLoginHighlightExperimentGroup=e;f.userInAnimateButtonExperimentGroup=g;f.userInExitDialogExperimentGroup=h;f.userInAdditionalAudioExperimentGroup=i;f.additionalAudioDelay=j;f.isInAdditionalAudioExperiment=k;f.userInConfOtpExperiment=l;f.userInRegLazyLoadOnView=m;f.userInRegLazyLoadOnClick=n;f.userInRegAdditionalMotivationalContent=o;f.motivationalContentVersion=p;function a(){var a;return(a=b("qex")._("1462897"))!=null?a:!0}function c(){var a;return(a=b("qex")._("1941961"))!=null?a:!1}function d(){var a;return(a=b("qex")._("1955561"))!=null?a:!1}function e(){var a;return(a=b("qex")._("1941385"))!=null?a:!1}function g(){var a;return(a=b("qex")._("1723547"))!=null?a:!1}function h(){var a;return(a=b("qex")._("1797277"))!=null?a:!

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\dF5SId3UHWd[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	2385
Entropy (8bit):	4.556036774993824
Encrypted:	false
SSDEEP:	48:07t6n8MnrFQiEC2o9M64cdImBl5cDiLgq4:6uraboGGI62iMB
MD5:	EBD8798BC32C86494851A07770E04E63
SHA1:	B5461DC8F5F5F848033441D506EE05D48742438B
SHA-256:	9531E96099E973B3D1C291F3E60419D8FE4730F46DE8A492FCCD2B4C962C96CE
SHA-512:	FB376AADA13675B405EBBF55C332665B5A89B7A905323D227EDFEE7729246E37A1B6B338554FFF4A0E2BB38DFBEAED59BE278BBF6F6BDFDFB4300AA6E54743E7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.xx.fbcdn.net/rsrc.php/y8/r/dF5SId3UHWd.svg

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\dF5SId3UHWd[1].svg	
Preview:	<svg id="Layer_1" data-name="Layer 1" xmlns="http://www.w3.org/2000/svg" viewBox="0 0 1022.51 360"><defs><style>.cls-1{fill:#1877F2;}</style></defs><title>FBWordmark_Hex-RGB-1024</title><path class="cls-1" d="M166.43,126.68c-9.65,0-12.44,4.28-12.44,13.72v15.66h25.74l-2.58,25.3H154v76.78H123.11V181.36H102.3v-25.3h20.81V140.83c0-25.52,10.29-39,39-39a146.17,146.17,0,0,1,18,1.07v23.81Z"/><path class="cls-1" d="M181.87,203.88c0-28.52,13.51-50,41.82-50,15.44,0,24.87,7.94,29.38,17.8V156.06h29.59V258.14H253.07V242.7c-4.29,9.87-13.94,17.59-29.38,17.59-28.31,0-41.82-21.45-41.82-50Zm30.88,6.87c0,15.22,5.57,25.3,19.94,25.3,12.66,0,19.09-9.22,19.09-23.8V202c0-14.58-6.43-23.8-19.09-23.8-14.37,0-19.94,10.08-19.94,25.3Z"/><path class="cls-1" d="M347,153.91c12,0,23.37,2.58,29.59,6.86l-6.86,21.88a48.6,48.6,0,0,0-20.59-4.72c-16.73,0-24,9.65-24,26.17v6c0,16.52,7.29,26.17,24,26.17a48.6,48.6,0,0,0,20.59-4.72l6.86,21.87c-6.22,4.29-17.58,6.87-29.59,6.87-36.25,0-52.76-19.52-52.76-50.83v-4.72C294.24,173.43,310.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\hsts-pixel[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	downloaded
Size (bytes):	43
Entropy (8bit):	2.7374910194847146
Encrypted:	false
SSDEEP:	3:CU9yltxlHh/:m/
MD5:	DF3E567D6F16D040326C7A0EA29A4F41
SHA1:	EA7DF583983133B62712B5E73BFFBCD45CC53736
SHA-256:	548F2D6F4D0D820C6C5FFBEFFCBD7F0E73193E2932EEFE542ACCC84762DEEC87
SHA-512:	B2CA25A3311DC42942E046EB1A27038B71D689925B7D6B3EBB4D7CD2C7B9A0C7DE3D10175790AC060DC3F8ACF3C1708C336626BE06879097F4D0ECAA7F56701
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fbsbx.com/security/hsts-pixel.gif
Preview:	GIF89a.....!.....,.....D..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\mnwJrbabqoh[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	1658
Entropy (8bit):	5.2294194137169905
Encrypted:	false
SSDEEP:	24:bJCfNFfCavgKE4hZFJ9HE899jIAvcwgFJ91xEorA899jIikh60CX3cCtrXwDf:bkF4avgKEMZ/pBXvcF/nxfvBFmnCzZAT
MD5:	0BE984614DCDE8F80776ADDEA6B69C97
SHA1:	1E62D2CA26092425AADC5B6D9B3598911C9DE278
SHA-256:	883C8C239FB17336986443FA0EEF05C9C8C3911151BE4080A0471FC6912A82A0
SHA-512:	C6B53D6F23768F3092621E6D809E56B365500FAFDADE6F29916272635A0FCC7B1FD8AB5FB4D9E8D2F3E1C0327B9DC3445F3C1FE5AAD67848715EAF6A82E624E1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.xx.fbcdn.net/rsrc.php/v3/yW/r/mnwJrbabqoh.js?_nc_x=Ij3Wp8lg5Kz
Preview:	if (self.CavalryLogger) { CavalryLogger.start_js(["LAw4+oR"]); }..__d("isStringNullOrEmpty",[],(function(a,b,c,d,e,f){"use strict";e.exports=a;function a(a){return a==null||a===""}}),null);.__d("$InternalEnum",[],(function(a,b,c,d,e,f){"use strict";var g=Object.prototype.hasOwnProperty,h=typeof WeakMap==="function"?new WeakMap():new Map();function i(a){var b=h.get(a);if(b!==void 0)return b;b=Object.getOwnPropertyNames(a);b=new Set(b.map(function(b){return a[b]}));h.set(a,b);return b}var j=Object.preventExtensions(Object.defineProperties(Object.create(null),{isValid:{value:function(a){return i(this).has(a)}},cast:{value:function(a){return this.isValid(a)?a:void 0}},members:{value:function(){return i(this).values()}}}));function a(a){var b=Object.create(j);for(var c in a)Object.prototype.hasOwnProperty.call(a,c)&&Object.defineProperty(b,c,{value:a[c]});Object.preventExtensions(b);return b}var k=Object.preventExtensions(Object.defineProperties(Object.create(null),{isValid:{value:function(

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\rBNJvj38u9T[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	30628
Entropy (8bit):	5.6493287227642455
Encrypted:	false
SSDEEP:	768:5ogA0aTwqOpdWiXy4/LQKIZhxYyitdOrAHmuViT:Or0EwqOpdWi7QKIZ5iRz4T
MD5:	7F82068076F2D3AB8B35AB42D1C9A237
SHA1:	074FA8AD79D84172E2E3E6961E0EA251931048F9
SHA-256:	A91C374DA35B477F8A0E76CFC6D8A5230C3BA694933605F43E7BAF6E0ED105CF
SHA-512:	3CF9DDB035E03E3465A9C2062E7B48909DF14CF2E96E6C4B7764519CC582887CB376DA79DFD19098B40BDAF58E0599DB1B6284E9AF3E3E275460E6A19E55BDE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.xx.fbcdn.net/rsrc.php/v3/ys/r/rBNJvj38u9T.js?_nc_x=Ij3Wp8lg5Kz

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\rBNJvj38u9T[1].js	
Preview:	if (self.CavalryLogger) { CavalryLogger.start_js(["sgpdgc2"]); }..__d("MAudioFlowsUtil",["DOM","Event","ge"],(function(a,b,c,d,e,f){"use strict";f.stopAudio=g;f.stopAudioOnOtherButtonClick=a;f.stopAudioOnExit=c;f.stopAudioOnOtherIdClick=d;function g(a){a=a!=null?a:b("ge")("root");a=b("DOM").scry(a,"div","audio_stop_button");a.length>0&&a.forEach(function(a){return a.click()})}function a(a,c){b("Event").listen(a,"click",function(){return g(c)})}function c(a){b("Event").listen(window,"visibilitychange",function(){return g(a)})}function d(a,c){var d=c!=null?c:b("ge")("root");d=b("DOM").scry(d,"*",a)[0];b("Event").listen(d,"click",function(){return g(c)})}}),null);.__d("Typeahead",["CSS","DOM","MParent","MViewport","Vector","createDeprecatedProperties","eventsMixinDeprecated","setTimeoutAcrossTransitions","uniqueID"],(function(a,b,c,d,e,f){a=function(){function a(c,d){var e=this;this.showResults=function(a){e.invoke("render_start");var c={show:a};c=e.invoke("show",c);if(e._typeObjects&&e._

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\toipMWCRTEo[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	24370
Entropy (8bit):	5.746303448631723
Encrypted:	false
SSDEEP:	384:qdHX+zKQ8WzlaMB6hVefhexo+rD/Cjrx0AyctxcivazDSe/D6xDrJuGkZ+oU0v:qdHX+zKQTzlaMB6hVeJDxXxbyct1vau+
MD5:	E9ACD860107BF7BA4DBE71EFE88BE749
SHA1:	65F2693E41A18DD73FB7DDE0BB289A9674C4E3BC
SHA-256:	A6E7427AE5061BBAB3308B62E04299A84C7AB3CAA2FFE0A0CA68101B12202D49
SHA-512:	CF366B92E53C8EBBA23298ECA95E5B7750CFACE547AF6F0BB3FF0BE8B56BCD6ADA76CAA78D5F624C8F32056E51A69CD99530D81E88F8ABA9A7274B3BA8C6AE64
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.xx.fbcdn.net/rsrc.php/v3/yD/r/toipMWCRTEo.js?_nc_x=Ij3Wp8lg5Kz
Preview:	if (self.CavalryLogger) { CavalryLogger.start_js(["gC4Hvk2"]); }..__d("MFriendingState",[],(function(a,b,c,d,e,f){a="m:friending-state:request-sent";f.REQUEST_SENT=a;b="m:friending-state:request-canceled";f.REQUEST_CANCELED=b;c="m:friending-state:unfriended";f.UNFRIENDED=c}),null);.__d("XMessengerMSiteShareDialogController",["XController"],(function(a,b,c,d,e,f){e.exports=b("XController").create("/share/diode/",{feedback_referrer:{type:"String"},feedback_source:{type:"Int"},internal_preview_image_id:{type:"Int"},key_link:{type:"String"},key_mode:{type:"String"},messaging_entry_point:{type:"Enum",enumType:1},post_fbid:{type:"Int",required:!0},redirector_fbid:{type:"Int"}})}),null);.__d("QPLE2ESessionMarkers",["$InternalEnum"],(function(a,b,c,d,e,f){a=b("$InternalEnum")({NONE:"none",START:"start",END:"end"});c=a;e.exports=c}),null);.__d("PerfFalcoEvent",["FalcoLoggerInternal","getFalcoLogPolicy_DO_NOT_USE"],(function(a,b,c,d,e,f){"use strict";a=b("getFalcoLogPolicy_DO_NOT_USE")("1744178"

C:\Users\user\AppData\Local\Temp\~DF0C626AC06D5E2361.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.47547457065742055
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loD9loD9lWY8xCAo:kBqoIkai
MD5:	3EFBE678B4DB43A805ED8AA7F5D4A5F9
SHA1:	1594089E41B7C3FC34EE70D9C13D4D13ABF4112E
SHA-256:	193987FDF8F4634115089E099820157419F83F9AAF5032CD22B6D38B3BC303A0
SHA-512:	FCD70717FA6CE1A0B5B11D6D3E90E7C37296519401773A681A46CB86670DEF7F1EC42DF9A0DD0D4C21C5D5E1245FCA3C47603E361953E8F43F2E14C02EF2DF7
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF77662EBE27437295.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	155733
Entropy (8bit):	1.1050503674943752
Encrypted:	false
SSDEEP:	384:kBqoxKAuqR+mg6Tg7Ql80YYONdcUY2bVLOacSyiT5FB35CijSSnzd1TAsmm47E9j:ASFWVLO3r65335CiZVi6Y0qJW
MD5:	7243C9233A5458A744856C0E1D16E76F
SHA1:	C63E5D8B270560D38C58C82167254BFA906BF254
SHA-256:	B766ADCCC45E202C2E6038AF2B8F4DE612806A0C57D93804592F789B5F8007E8
SHA-512:	300908EF31E17C7A19CAA5EE905D6817580497A6327C59CFA51566E159DEF7E495645DA82A5A327F57994BDFE17A5A17847F87A57282AA0826E99D313072956B
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\~DF77662EBE27437295.TMP	
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFA111B94D5E8C7290.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.2954946661253283
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laA1:kBqoxxJhHWSVSEab
MD5:	7DC903F6114D7CEAC73E7F749ED594A2
SHA1:	AE1D4D5829C887261B85E5730F1DBD3045FD983E
SHA-256:	CE8C56703DCC439C57D62418EFC1019BA445045C9F8DE916A4C423747C29FE2A
SHA-512:	604741C5E8A074BDB58F7BF866CB38DC550BC56A94F4C2AE6E65FC2C0D7B403AC7497971ED112606413FEBAB6A5128F2249EF192AFC011969EE0C0656A35B45D
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

Static File Info

No static file info

Network Behavior

Network Port Distribution

Total Packets: 90

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 9, 2021 15:13:43.949397087 CEST	49728	443	192.168.2.4	68.66.226.79
Apr 9, 2021 15:13:43.950340033 CEST	49729	443	192.168.2.4	68.66.226.79
Apr 9, 2021 15:13:44.108830929 CEST	443	49729	68.66.226.79	192.168.2.4
Apr 9, 2021 15:13:44.109098911 CEST	49729	443	192.168.2.4	68.66.226.79
Apr 9, 2021 15:13:44.112854958 CEST	443	49728	68.66.226.79	192.168.2.4
Apr 9, 2021 15:13:44.113004923 CEST	49728	443	192.168.2.4	68.66.226.79

Copyright Joe Security LLC 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 9, 2021 15:13:44.120120049 CEST	49729	443	192.168.2.4	68.66.226.79
Apr 9, 2021 15:13:44.120548010 CEST	49728	443	192.168.2.4	68.66.226.79
Apr 9, 2021 15:13:44.278448105 CEST	443	49729	68.66.226.79	192.168.2.4
Apr 9, 2021 15:13:44.278810978 CEST	443	49729	68.66.226.79	192.168.2.4
Apr 9, 2021 15:13:44.278852940 CEST	443	49729	68.66.226.79	192.168.2.4
Apr 9, 2021 15:13:44.278930902 CEST	49729	443	192.168.2.4	68.66.226.79
Apr 9, 2021 15:13:44.278949976 CEST	443	49729	68.66.226.79	192.168.2.4
Apr 9, 2021 15:13:44.278970003 CEST	49729	443	192.168.2.4	68.66.226.79
Apr 9, 2021 15:13:44.278975964 CEST	443	49729	68.66.226.79	192.168.2.4
Apr 9, 2021 15:13:44.279059887 CEST	49729	443	192.168.2.4	68.66.226.79
Apr 9, 2021 15:13:44.279140949 CEST	49729	443	192.168.2.4	68.66.226.79
Apr 9, 2021 15:13:44.281075001 CEST	443	49729	68.66.226.79	192.168.2.4
Apr 9, 2021 15:13:44.281199932 CEST	49729	443	192.168.2.4	68.66.226.79
Apr 9, 2021 15:13:44.281416893 CEST	443	49728	68.66.226.79	192.168.2.4
Apr 9, 2021 15:13:44.281543016 CEST	443	49728	68.66.226.79	192.168.2.4
Apr 9, 2021 15:13:44.281583071 CEST	443	49728	68.66.226.79	192.168.2.4
Apr 9, 2021 15:13:44.281620026 CEST	443	49728	68.66.226.79	192.168.2.4
Apr 9, 2021 15:13:44.281635046 CEST	49728	443	192.168.2.4	68.66.226.79
Apr 9, 2021 15:13:44.281645060 CEST	443	49728	68.66.226.79	192.168.2.4
Apr 9, 2021 15:13:44.281681061 CEST	49728	443	192.168.2.4	68.66.226.79
Apr 9, 2021 15:13:44.281752110 CEST	49728	443	192.168.2.4	68.66.226.79
Apr 9, 2021 15:13:44.284800053 CEST	443	49728	68.66.226.79	192.168.2.4
Apr 9, 2021 15:13:44.284904957 CEST	49728	443	192.168.2.4	68.66.226.79
Apr 9, 2021 15:13:44.353776932 CEST	49728	443	192.168.2.4	68.66.226.79
Apr 9, 2021 15:13:44.353806973 CEST	49729	443	192.168.2.4	68.66.226.79
Apr 9, 2021 15:13:44.361135960 CEST	49728	443	192.168.2.4	68.66.226.79
Apr 9, 2021 15:13:44.516942978 CEST	443	49729	68.66.226.79	192.168.2.4
Apr 9, 2021 15:13:44.517069101 CEST	49729	443	192.168.2.4	68.66.226.79
Apr 9, 2021 15:13:44.517103910 CEST	443	49728	68.66.226.79	192.168.2.4
Apr 9, 2021 15:13:44.517235041 CEST	49728	443	192.168.2.4	68.66.226.79
Apr 9, 2021 15:13:44.563528061 CEST	443	49728	68.66.226.79	192.168.2.4
Apr 9, 2021 15:13:45.289683104 CEST	443	49728	68.66.226.79	192.168.2.4
Apr 9, 2021 15:13:45.289783001 CEST	443	49728	68.66.226.79	192.168.2.4
Apr 9, 2021 15:13:45.289822102 CEST	443	49728	68.66.226.79	192.168.2.4
Apr 9, 2021 15:13:45.289855003 CEST	443	49728	68.66.226.79	192.168.2.4
Apr 9, 2021 15:13:45.289875984 CEST	49728	443	192.168.2.4	68.66.226.79
Apr 9, 2021 15:13:45.289880991 CEST	443	49728	68.66.226.79	192.168.2.4
Apr 9, 2021 15:13:45.289906979 CEST	49728	443	192.168.2.4	68.66.226.79
Apr 9, 2021 15:13:45.289911032 CEST	49728	443	192.168.2.4	68.66.226.79
Apr 9, 2021 15:13:45.289918900 CEST	49728	443	192.168.2.4	68.66.226.79
Apr 9, 2021 15:13:45.289952993 CEST	49728	443	192.168.2.4	68.66.226.79
Apr 9, 2021 15:13:45.400120020 CEST	49728	443	192.168.2.4	68.66.226.79
Apr 9, 2021 15:13:45.400758982 CEST	49729	443	192.168.2.4	68.66.226.79
Apr 9, 2021 15:13:45.402240992 CEST	49730	443	192.168.2.4	68.66.226.79
Apr 9, 2021 15:13:45.403203964 CEST	49731	443	192.168.2.4	68.66.226.79
Apr 9, 2021 15:13:45.560916901 CEST	443	49728	68.66.226.79	192.168.2.4
Apr 9, 2021 15:13:45.563296080 CEST	443	49731	68.66.226.79	192.168.2.4
Apr 9, 2021 15:13:45.563340902 CEST	443	49730	68.66.226.79	192.168.2.4
Apr 9, 2021 15:13:45.563440084 CEST	49731	443	192.168.2.4	68.66.226.79
Apr 9, 2021 15:13:45.563488007 CEST	49730	443	192.168.2.4	68.66.226.79
Apr 9, 2021 15:13:45.564109087 CEST	49731	443	192.168.2.4	68.66.226.79
Apr 9, 2021 15:13:45.564651012 CEST	49730	443	192.168.2.4	68.66.226.79
Apr 9, 2021 15:13:45.570822001 CEST	443	49729	68.66.226.79	192.168.2.4
Apr 9, 2021 15:13:45.570863008 CEST	443	49729	68.66.226.79	192.168.2.4
Apr 9, 2021 15:13:45.570909977 CEST	443	49729	68.66.226.79	192.168.2.4
Apr 9, 2021 15:13:45.570951939 CEST	443	49729	68.66.226.79	192.168.2.4
Apr 9, 2021 15:13:45.570988894 CEST	443	49729	68.66.226.79	192.168.2.4
Apr 9, 2021 15:13:45.571026087 CEST	443	49729	68.66.226.79	192.168.2.4
Apr 9, 2021 15:13:45.571034908 CEST	49729	443	192.168.2.4	68.66.226.79
Apr 9, 2021 15:13:45.571069002 CEST	443	49729	68.66.226.79	192.168.2.4
Apr 9, 2021 15:13:45.571069956 CEST	49729	443	192.168.2.4	68.66.226.79
Apr 9, 2021 15:13:45.571075916 CEST	49729	443	192.168.2.4	68.66.226.79
Apr 9, 2021 15:13:45.571079969 CEST	49729	443	192.168.2.4	68.66.226.79
Apr 9, 2021 15:13:45.571091890 CEST	49729	443	192.168.2.4	68.66.226.79

Copyright Joe Security LLC 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 9, 2021 15:13:45.571105957 CEST	443	49729	68.66.226.79	192.168.2.4
Apr 9, 2021 15:13:45.571137905 CEST	443	49729	68.66.226.79	192.168.2.4
Apr 9, 2021 15:13:45.571175098 CEST	443	49728	68.66.226.79	192.168.2.4
Apr 9, 2021 15:13:45.571208000 CEST	49729	443	192.168.2.4	68.66.226.79
Apr 9, 2021 15:13:45.571221113 CEST	443	49728	68.66.226.79	192.168.2.4
Apr 9, 2021 15:13:45.571235895 CEST	49729	443	192.168.2.4	68.66.226.79
Apr 9, 2021 15:13:45.571242094 CEST	49729	443	192.168.2.4	68.66.226.79
Apr 9, 2021 15:13:45.571257114 CEST	443	49728	68.66.226.79	192.168.2.4
Apr 9, 2021 15:13:45.571259022 CEST	49728	443	192.168.2.4	68.66.226.79
Apr 9, 2021 15:13:45.571301937 CEST	49728	443	192.168.2.4	68.66.226.79
Apr 9, 2021 15:13:45.571306944 CEST	49728	443	192.168.2.4	68.66.226.79
Apr 9, 2021 15:13:45.577349901 CEST	49728	443	192.168.2.4	68.66.226.79
Apr 9, 2021 15:13:45.580987930 CEST	49729	443	192.168.2.4	68.66.226.79
Apr 9, 2021 15:13:45.723190069 CEST	443	49731	68.66.226.79	192.168.2.4
Apr 9, 2021 15:13:45.724591017 CEST	443	49731	68.66.226.79	192.168.2.4
Apr 9, 2021 15:13:45.724734068 CEST	49731	443	192.168.2.4	68.66.226.79
Apr 9, 2021 15:13:45.724919081 CEST	443	49730	68.66.226.79	192.168.2.4
Apr 9, 2021 15:13:45.728657961 CEST	443	49730	68.66.226.79	192.168.2.4
Apr 9, 2021 15:13:45.728748083 CEST	49730	443	192.168.2.4	68.66.226.79
Apr 9, 2021 15:13:45.744338989 CEST	443	49729	68.66.226.79	192.168.2.4
Apr 9, 2021 15:13:45.744379997 CEST	443	49729	68.66.226.79	192.168.2.4
Apr 9, 2021 15:13:45.744410992 CEST	443	49729	68.66.226.79	192.168.2.4
Apr 9, 2021 15:13:45.744513035 CEST	443	49729	68.66.226.79	192.168.2.4
Apr 9, 2021 15:13:45.744525909 CEST	49729	443	192.168.2.4	68.66.226.79
Apr 9, 2021 15:13:45.744570017 CEST	49729	443	192.168.2.4	68.66.226.79
Apr 9, 2021 15:13:45.744618893 CEST	443	49729	68.66.226.79	192.168.2.4
Apr 9, 2021 15:13:45.744682074 CEST	49729	443	192.168.2.4	68.66.226.79
Apr 9, 2021 15:13:45.744714022 CEST	443	49729	68.66.226.79	192.168.2.4
Apr 9, 2021 15:13:45.744745016 CEST	443	49729	68.66.226.79	192.168.2.4
Apr 9, 2021 15:13:45.744776964 CEST	49729	443	192.168.2.4	68.66.226.79

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 9, 2021 15:13:35.809252024 CEST	49714	53	192.168.2.4	8.8.8.8
Apr 9, 2021 15:13:35.822364092 CEST	53	49714	8.8.8.8	192.168.2.4
Apr 9, 2021 15:13:36.796447039 CEST	58028	53	192.168.2.4	8.8.8.8
Apr 9, 2021 15:13:36.809465885 CEST	53	58028	8.8.8.8	192.168.2.4
Apr 9, 2021 15:13:37.730284929 CEST	53097	53	192.168.2.4	8.8.8.8
Apr 9, 2021 15:13:37.745733023 CEST	53	53097	8.8.8.8	192.168.2.4
Apr 9, 2021 15:13:42.840388060 CEST	49257	53	192.168.2.4	8.8.8.8
Apr 9, 2021 15:13:42.858829975 CEST	53	49257	8.8.8.8	192.168.2.4
Apr 9, 2021 15:13:43.899254084 CEST	62389	53	192.168.2.4	8.8.8.8
Apr 9, 2021 15:13:43.940500021 CEST	53	62389	8.8.8.8	192.168.2.4
Apr 9, 2021 15:13:46.840745926 CEST	49910	53	192.168.2.4	8.8.8.8
Apr 9, 2021 15:13:46.860234976 CEST	53	49910	8.8.8.8	192.168.2.4
Apr 9, 2021 15:13:46.961879015 CEST	55854	53	192.168.2.4	8.8.8.8
Apr 9, 2021 15:13:46.981856108 CEST	53	55854	8.8.8.8	192.168.2.4
Apr 9, 2021 15:13:51.919203997 CEST	64549	53	192.168.2.4	8.8.8.8
Apr 9, 2021 15:13:51.937542915 CEST	53	64549	8.8.8.8	192.168.2.4
Apr 9, 2021 15:14:00.169914007 CEST	63153	53	192.168.2.4	8.8.8.8
Apr 9, 2021 15:14:00.183959007 CEST	53	63153	8.8.8.8	192.168.2.4
Apr 9, 2021 15:14:00.282635927 CEST	52991	53	192.168.2.4	8.8.8.8
Apr 9, 2021 15:14:00.298199892 CEST	53	52991	8.8.8.8	192.168.2.4
Apr 9, 2021 15:14:00.777241945 CEST	53700	53	192.168.2.4	8.8.8.8
Apr 9, 2021 15:14:00.788989067 CEST	53	53700	8.8.8.8	192.168.2.4
Apr 9, 2021 15:14:01.814739943 CEST	51726	53	192.168.2.4	8.8.8.8
Apr 9, 2021 15:14:01.827725887 CEST	53	51726	8.8.8.8	192.168.2.4
Apr 9, 2021 15:14:02.666541100 CEST	56794	53	192.168.2.4	8.8.8.8
Apr 9, 2021 15:14:02.686582088 CEST	53	56794	8.8.8.8	192.168.2.4
Apr 9, 2021 15:14:02.787815094 CEST	56534	53	192.168.2.4	8.8.8.8
Apr 9, 2021 15:14:02.801040888 CEST	53	56534	8.8.8.8	192.168.2.4
Apr 9, 2021 15:14:02.898664951 CEST	56627	53	192.168.2.4	8.8.8.8
Apr 9, 2021 15:14:02.918692112 CEST	53	56627	8.8.8.8	192.168.2.4

Copyright Joe Security LLC 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 9, 2021 15:14:03.084330082 CEST	56621	53	192.168.2.4	8.8.8.8
Apr 9, 2021 15:14:03.097534895 CEST	53	56621	8.8.8.8	192.168.2.4
Apr 9, 2021 15:14:03.364403963 CEST	63116	53	192.168.2.4	8.8.8.8
Apr 9, 2021 15:14:03.382565022 CEST	53	63116	8.8.8.8	192.168.2.4
Apr 9, 2021 15:14:03.494726896 CEST	64078	53	192.168.2.4	8.8.8.8
Apr 9, 2021 15:14:03.514326096 CEST	53	64078	8.8.8.8	192.168.2.4
Apr 9, 2021 15:14:03.608470917 CEST	64801	53	192.168.2.4	8.8.8.8
Apr 9, 2021 15:14:03.630227089 CEST	53	64801	8.8.8.8	192.168.2.4
Apr 9, 2021 15:14:03.886394024 CEST	61721	53	192.168.2.4	8.8.8.8
Apr 9, 2021 15:14:03.904738903 CEST	53	61721	8.8.8.8	192.168.2.4
Apr 9, 2021 15:14:04.078870058 CEST	51255	53	192.168.2.4	8.8.8.8
Apr 9, 2021 15:14:04.092190981 CEST	53	51255	8.8.8.8	192.168.2.4
Apr 9, 2021 15:14:04.847964048 CEST	61522	53	192.168.2.4	8.8.8.8
Apr 9, 2021 15:14:04.862776041 CEST	53	61522	8.8.8.8	192.168.2.4
Apr 9, 2021 15:14:05.039053917 CEST	52337	53	192.168.2.4	8.8.8.8
Apr 9, 2021 15:14:05.052608013 CEST	53	52337	8.8.8.8	192.168.2.4
Apr 9, 2021 15:14:06.486057043 CEST	55046	53	192.168.2.4	8.8.8.8
Apr 9, 2021 15:14:06.498788118 CEST	53	55046	8.8.8.8	192.168.2.4
Apr 9, 2021 15:14:08.338743925 CEST	49612	53	192.168.2.4	8.8.8.8
Apr 9, 2021 15:14:08.351497889 CEST	53	49612	8.8.8.8	192.168.2.4
Apr 9, 2021 15:14:08.791908026 CEST	49285	53	192.168.2.4	8.8.8.8
Apr 9, 2021 15:14:08.810162067 CEST	53	49285	8.8.8.8	192.168.2.4
Apr 9, 2021 15:14:13.077369928 CEST	50601	53	192.168.2.4	8.8.8.8
Apr 9, 2021 15:14:13.090023041 CEST	53	50601	8.8.8.8	192.168.2.4
Apr 9, 2021 15:14:13.484268904 CEST	60875	53	192.168.2.4	8.8.8.8
Apr 9, 2021 15:14:13.496530056 CEST	53	60875	8.8.8.8	192.168.2.4
Apr 9, 2021 15:14:14.114515066 CEST	50601	53	192.168.2.4	8.8.8.8
Apr 9, 2021 15:14:14.128160954 CEST	53	50601	8.8.8.8	192.168.2.4
Apr 9, 2021 15:14:14.481949091 CEST	60875	53	192.168.2.4	8.8.8.8
Apr 9, 2021 15:14:14.493684053 CEST	53	60875	8.8.8.8	192.168.2.4
Apr 9, 2021 15:14:15.153446913 CEST	50601	53	192.168.2.4	8.8.8.8
Apr 9, 2021 15:14:15.167814970 CEST	53	50601	8.8.8.8	192.168.2.4
Apr 9, 2021 15:14:15.520209074 CEST	60875	53	192.168.2.4	8.8.8.8
Apr 9, 2021 15:14:15.535259962 CEST	53	60875	8.8.8.8	192.168.2.4
Apr 9, 2021 15:14:17.164745092 CEST	50601	53	192.168.2.4	8.8.8.8
Apr 9, 2021 15:14:17.177172899 CEST	53	50601	8.8.8.8	192.168.2.4
Apr 9, 2021 15:14:17.586494923 CEST	60875	53	192.168.2.4	8.8.8.8
Apr 9, 2021 15:14:17.601308107 CEST	53	60875	8.8.8.8	192.168.2.4
Apr 9, 2021 15:14:21.164587975 CEST	50601	53	192.168.2.4	8.8.8.8
Apr 9, 2021 15:14:21.178982019 CEST	53	50601	8.8.8.8	192.168.2.4
Apr 9, 2021 15:14:21.602242947 CEST	60875	53	192.168.2.4	8.8.8.8
Apr 9, 2021 15:14:21.614741087 CEST	53	60875	8.8.8.8	192.168.2.4
Apr 9, 2021 15:14:23.153465986 CEST	56448	53	192.168.2.4	8.8.8.8
Apr 9, 2021 15:14:23.166445971 CEST	53	56448	8.8.8.8	192.168.2.4
Apr 9, 2021 15:14:24.318532944 CEST	59172	53	192.168.2.4	8.8.8.8
Apr 9, 2021 15:14:24.331228018 CEST	53	59172	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 9, 2021 15:13:43.899254084 CEST	192.168.2.4	8.8.8.8	0xdda4	Standard query (0)	ccaeperu.com	A (IP address)	IN (0x0001)
Apr 9, 2021 15:13:46.840745926 CEST	192.168.2.4	8.8.8.8	0x1cfb	Standard query (0)	www.fb.com	A (IP address)	IN (0x0001)
Apr 9, 2021 15:13:46.961879015 CEST	192.168.2.4	8.8.8.8	0xb128	Standard query (0)	www.facebook.com	A (IP address)	IN (0x0001)
Apr 9, 2021 15:14:00.169914007 CEST	192.168.2.4	8.8.8.8	0xe56	Standard query (0)	www.fb.com	A (IP address)	IN (0x0001)
Apr 9, 2021 15:14:00.282635927 CEST	192.168.2.4	8.8.8.8	0x6d07	Standard query (0)	www.facebook.com	A (IP address)	IN (0x0001)
Apr 9, 2021 15:14:02.666541100 CEST	192.168.2.4	8.8.8.8	0x5a00	Standard query (0)	fb.com	A (IP address)	IN (0x0001)
Apr 9, 2021 15:14:02.898664951 CEST	192.168.2.4	8.8.8.8	0x384c	Standard query (0)	m.facebook.com	A (IP address)	IN (0x0001)
Apr 9, 2021 15:14:03.084330082 CEST	192.168.2.4	8.8.8.8	0xc443	Standard query (0)	static.xx.fbcdn.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 9, 2021 15:14:03.364403963 CEST	192.168.2.4	8.8.8.8	0x71d5	Standard query (0)	facebook.com	A (IP address)	IN (0x0001)
Apr 9, 2021 15:14:03.494726896 CEST	192.168.2.4	8.8.8.8	0x8b03	Standard query (0)	fbcdn.net	A (IP address)	IN (0x0001)
Apr 9, 2021 15:14:03.608470917 CEST	192.168.2.4	8.8.8.8	0xf1b	Standard query (0)	fbsbx.com	A (IP address)	IN (0x0001)
Apr 9, 2021 15:14:03.886394024 CEST	192.168.2.4	8.8.8.8	0xf8d5	Standard query (0)	scontent.x x.fbcdn.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 9, 2021 15:13:43.940500021 CEST	8.8.8.8	192.168.2.4	0xdda4	No error (0)	ccaeperu.com		68.66.226.79	A (IP address)	IN (0x0001)
Apr 9, 2021 15:13:46.860234976 CEST	8.8.8.8	192.168.2.4	0x1cfb	No error (0)	www.fb.com	www.facebook.com		CNAME (Canonical name)	IN (0x0001)
Apr 9, 2021 15:13:46.860234976 CEST	8.8.8.8	192.168.2.4	0x1cfb	No error (0)	www.facebook.com	star-mini.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)
Apr 9, 2021 15:13:46.860234976 CEST	8.8.8.8	192.168.2.4	0x1cfb	No error (0)	star-mini.c10r.facebook.com		157.240.17.35	A (IP address)	IN (0x0001)
Apr 9, 2021 15:13:46.981856108 CEST	8.8.8.8	192.168.2.4	0xb128	No error (0)	www.facebook.com	star-mini.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)
Apr 9, 2021 15:13:46.981856108 CEST	8.8.8.8	192.168.2.4	0xb128	No error (0)	star-mini.c10r.facebook.com		157.240.17.35	A (IP address)	IN (0x0001)
Apr 9, 2021 15:14:00.183959007 CEST	8.8.8.8	192.168.2.4	0xe56	No error (0)	www.fb.com	www.facebook.com		CNAME (Canonical name)	IN (0x0001)
Apr 9, 2021 15:14:00.183959007 CEST	8.8.8.8	192.168.2.4	0xe56	No error (0)	www.facebook.com	star-mini.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)
Apr 9, 2021 15:14:00.183959007 CEST	8.8.8.8	192.168.2.4	0xe56	No error (0)	star-mini.c10r.facebook.com		157.240.17.35	A (IP address)	IN (0x0001)
Apr 9, 2021 15:14:00.298199892 CEST	8.8.8.8	192.168.2.4	0x6d07	No error (0)	www.facebook.com	star-mini.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)
Apr 9, 2021 15:14:00.298199892 CEST	8.8.8.8	192.168.2.4	0x6d07	No error (0)	star-mini.c10r.facebook.com		157.240.219.35	A (IP address)	IN (0x0001)
Apr 9, 2021 15:14:02.686582088 CEST	8.8.8.8	192.168.2.4	0x5a00	No error (0)	fb.com		157.240.17.35	A (IP address)	IN (0x0001)
Apr 9, 2021 15:14:02.918692112 CEST	8.8.8.8	192.168.2.4	0x384c	No error (0)	m.facebook.com	star-mini.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)
Apr 9, 2021 15:14:02.918692112 CEST	8.8.8.8	192.168.2.4	0x384c	No error (0)	star-mini.c10r.facebook.com		157.240.17.35	A (IP address)	IN (0x0001)
Apr 9, 2021 15:14:03.097534895 CEST	8.8.8.8	192.168.2.4	0xc443	No error (0)	static.xx.fbcdn.net	scontent.xx.fbcdn.net		CNAME (Canonical name)	IN (0x0001)
Apr 9, 2021 15:14:03.097534895 CEST	8.8.8.8	192.168.2.4	0xc443	No error (0)	scontent.x x.fbcdn.net		157.240.219.13	A (IP address)	IN (0x0001)
Apr 9, 2021 15:14:03.382565022 CEST	8.8.8.8	192.168.2.4	0x71d5	No error (0)	facebook.com		157.240.17.35	A (IP address)	IN (0x0001)
Apr 9, 2021 15:14:03.514326096 CEST	8.8.8.8	192.168.2.4	0x8b03	No error (0)	fbcdn.net		157.240.17.35	A (IP address)	IN (0x0001)
Apr 9, 2021 15:14:03.630227089 CEST	8.8.8.8	192.168.2.4	0xf1b	No error (0)	fbsbx.com		157.240.17.35	A (IP address)	IN (0x0001)
Apr 9, 2021 15:14:03.904738903 CEST	8.8.8.8	192.168.2.4	0xf8d5	No error (0)	scontent.x x.fbcdn.net		157.240.17.15	A (IP address)	IN (0x0001)

HTTPS Packets

Copyright Joe Security LLC 2021

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 9, 2021 15:13:44.281075001 CEST	68.66.226.79	443	192.168.2.4	49729	CN=ccaeperu.com CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Sun Mar 28 01:00:00 CET 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Sun Jun 27 01:59:59 CEST 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	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="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
Apr 9, 2021 15:13:44.284800053 CEST	68.66.226.79	443	192.168.2.4	49728	CN=ccaeperu.com CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Sun Mar 28 01:00:00 CET 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Sun Jun 27 01:59:59 CEST 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	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="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
Apr 9, 2021 15:13:46.891350985 CEST	157.240.17.35	443	192.168.2.4	49732	CN=*.fb.com, O="Facebook, Inc.", L=Menlo Park, 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 Feb 23 01:00:00 CET 2021 Tue Oct 22 14:00:00 CEST 2013	Mon May 24 01:59:59 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Apr 9, 2021 15:13:46.892906904 CEST	157.240.17.35	443	192.168.2.4	49733	CN=*.fb.com, O="Facebook, Inc.", L=Menlo Park, 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 Feb 23 01:00:00 CET 2021 Tue Oct 22 14:00:00 CEST 2013	Mon May 24 01:59:59 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 9, 2021 15:13:47.016721010 CEST	157.240.17.35	443	192.168.2.4	49734	CN=*.facebook.com, O="Facebook, Inc.", L=Menlo Park, 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	Wed Feb 10 01:00:00 CET 2021 Tue Oct 22 14:00:00 CEST 2013	Tue May 11 01:59:59 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Apr 9, 2021 15:13:47.018336058 CEST	157.240.17.35	443	192.168.2.4	49735	CN=*.facebook.com, O="Facebook, Inc.", L=Menlo Park, 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	Wed Feb 10 01:00:00 CET 2021 Tue Oct 22 14:00:00 CEST 2013	Tue May 11 01:59:59 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Apr 9, 2021 15:14:00.214747906 CEST	157.240.17.35	443	192.168.2.4	49737	CN=*.fb.com, O="Facebook, Inc.", L=Menlo Park, 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 Feb 23 01:00:00 CET 2021 Tue Oct 22 14:00:00 CEST 2013	Mon May 24 01:59:59 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					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		
Apr 9, 2021 15:14:02.718868971 CEST	157.240.17.35	443	192.168.2.4	49742	CN=*.fb.com, O="Facebook, Inc.", L=Menlo Park, 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 Feb 23 01:00:00 CET 2021 Tue Oct 22 14:00:00 CEST 2013	Mon May 24 01:59:59 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Apr 9, 2021 15:14:02.719264984 CEST	157.240.17.35	443	192.168.2.4	49741	CN=*.fb.com, O="Facebook, Inc.", L=Menlo Park, 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 Feb 23 01:00:00 CET 2021 Tue Oct 22 14:00:00 CEST 2013	Mon May 24 01:59:59 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 9, 2021 15:14:02.947247982 CEST	157.240.17.35	443	192.168.2.4	49744	CN=*.facebook.com, O="Facebook, Inc.", L=Menlo Park, 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	Wed Feb 10 01:00:00 CET 2021 Tue Oct 22 14:00:00 CEST 2013	Tue May 11 01:59:59 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Apr 9, 2021 15:14:02.953632116 CEST	157.240.17.35	443	192.168.2.4	49745	CN=*.facebook.com, O="Facebook, Inc.", L=Menlo Park, 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	Wed Feb 10 01:00:00 CET 2021 Tue Oct 22 14:00:00 CEST 2013	Tue May 11 01:59:59 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Apr 9, 2021 15:14:03.394229889 CEST	157.240.219.13	443	192.168.2.4	49749	CN=*.facebook.com, O="Facebook, Inc.", L=Menlo Park, 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	Wed Feb 10 01:00:00 CET 2021 Tue Oct 22 14:00:00 CEST 2013	Tue May 11 01:59:59 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Apr 9, 2021 15:14:03.394340038 CEST	157.240.219.13	443	192.168.2.4	49746	CN=*.facebook.com, O="Facebook, Inc.", L=Menlo Park, 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	Wed Feb 10 01:00:00 CET 2021 Tue Oct 22 14:00:00 CEST 2013	Tue May 11 01:59:59 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Apr 9, 2021 15:14:03.394465923 CEST	157.240.219.13	443	192.168.2.4	49750	CN=*.facebook.com, O="Facebook, Inc.", L=Menlo Park, 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	Wed Feb 10 01:00:00 CET 2021 Tue Oct 22 14:00:00 CEST 2013	Tue May 11 01:59:59 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 9, 2021 15:14:03.394572020 CEST	157.240.219.13	443	192.168.2.4	49747	CN=*.facebook.com, O="Facebook, Inc.", L=Menlo Park, 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	Wed Feb 10 01:00:00 CET 2021 Tue Oct 22 14:00:00 CEST 2013	Tue May 11 01:59:59 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Apr 9, 2021 15:14:03.394716024 CEST	157.240.219.13	443	192.168.2.4	49748	CN=*.facebook.com, O="Facebook, Inc.", L=Menlo Park, 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	Wed Feb 10 01:00:00 CET 2021 Tue Oct 22 14:00:00 CEST 2013	Tue May 11 01:59:59 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Apr 9, 2021 15:14:03.395009995 CEST	157.240.219.13	443	192.168.2.4	49751	CN=*.facebook.com, O="Facebook, Inc.", L=Menlo Park, 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	Wed Feb 10 01:00:00 CET 2021 Tue Oct 22 14:00:00 CEST 2013	Tue May 11 01:59:59 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Apr 9, 2021 15:14:03.419888020 CEST	157.240.17.35	443	192.168.2.4	49753	CN=*.facebook.com, O="Facebook, Inc.", L=Menlo Park, 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	Wed Feb 10 01:00:00 CET 2021 Tue Oct 22 14:00:00 CEST 2013	Tue May 11 01:59:59 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Apr 9, 2021 15:14:03.420172930 CEST	157.240.17.35	443	192.168.2.4	49752	CN=*.facebook.com, O="Facebook, Inc.", L=Menlo Park, 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	Wed Feb 10 01:00:00 CET 2021 Tue Oct 22 14:00:00 CEST 2013	Tue May 11 01:59:59 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 9, 2021 15:14:03.542714119 CEST	157.240.17.35	443	192.168.2.4	49754	CN=fbcdn.net, O="Facebook, Inc.", L=Menlo Park, 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	Sun Feb 07 01:00:00 CET 2021	Sat May 08 01:59:59 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		
Apr 9, 2021 15:14:03.542946100 CEST	157.240.17.35	443	192.168.2.4	49755	CN=fbcdn.net, O="Facebook, Inc.", L=Menlo Park, 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	Sun Feb 07 01:00:00 CET 2021	Sat May 08 01:59:59 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		
Apr 9, 2021 15:14:03.658444881 CEST	157.240.17.35	443	192.168.2.4	49757	CN=fbcdn.net, O="Facebook, Inc.", L=Menlo Park, 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	Sun Feb 07 01:00:00 CET 2021	Sat May 08 01:59:59 CEST 2021	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	3faf2df7ab96c36419c31725cb1fa7d6
						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		
Apr 9, 2021 15:14:03.658622026 CEST	157.240.17.35	443	192.168.2.4	49756	CN=fbcdn.net, O="Facebook, Inc.", L=Menlo Park, 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	Sun Feb 07 01:00:00 CET 2021	Sat May 08 01:59:59 CEST 2021	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	3faf2df7ab96c36419c31725cb1fa7d6
						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		
Apr 9, 2021 15:14:03.932909966 CEST	157.240.17.15	443	192.168.2.4	49758	CN=*.facebook.com, O="Facebook, Inc.", L=Menlo Park, 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	Wed Feb 10 01:00:00 CET 2021	Tue May 11 01:59:59 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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 9, 2021 15:14:03.933270931 CEST	157.240.17.15	443	192.168.2.4	49759	CN=*.facebook.com, O="Facebook, Inc.", L=Menlo Park, 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	Wed Feb 10 01:00:00 CET 2021 Tue Oct 22 14:00:00 CEST 2013	Tue May 11 01:59:59 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		

Code Manipulations

Statistics

Behavior

System Behavior

Analysis Process: iexplore.exe PID: 4828 Parent PID: 800

General

Start time:	15:13:41
Start date:	09/04/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff765300000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Copyright Joe Security LLC 2021

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: iexplore.exe PID: 1576 Parent PID: 4828

General

Start time:	15:13:42
Start date:	09/04/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4828 CREDAT:17410 /prefetch:2
Imagebase:	0x2d0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly