ID: 383613
Sample Name: Payment Report.html
Cookbook: defaultwindowshtmlcookbook.jbs
Time: 02:53:22
Date: 08/04/2021
Version: 31.0.0 Emerald

Table of Contents

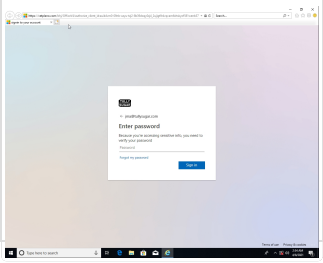
Analysis Report Payment Report.html

Overview

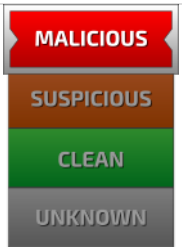
General Information

Sample Name:	Payment Report.html
Analysis ID:	383613
MD5:	00b8795cb028a9..
SHA1:	4dff056dc7d6857..
SHA256:	89901d174c786d..
Infos:	

Most interesting Screenshot:



Detection



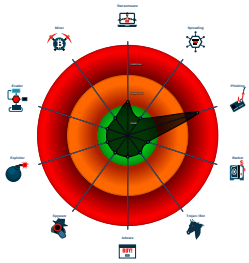
HTMLPhisher

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

Signatures

- Antivirus detection for URL or domain
- Phishing site detected (based on fav…
- Yara detected HtmlPhish10
- JA3 SSL client fingerprint seen in co…

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 5764 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5820 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5764 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

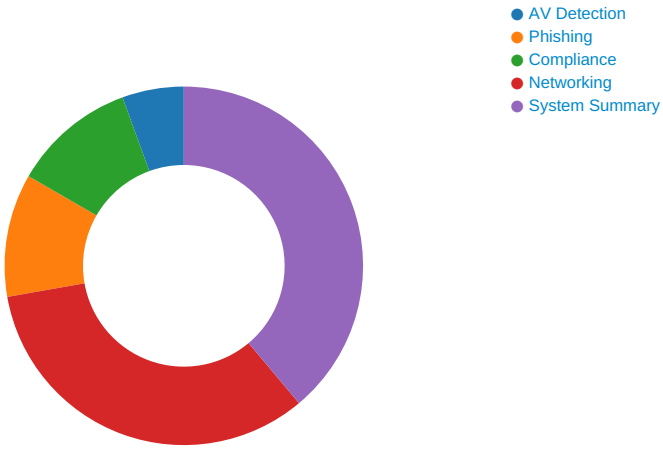
Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\authorize_client_id_auik4vm0-09nb-xayu-tzj2-8b39doqy0xj4_2ujigt9r4vqcam6xhskyof581wenb37dpzl0x7cpazksi4u9jfndvor60bqwm2hgy358t1leatz8peo3dxuk1vhcq0f29gy5bjim6ns4r7wl[1].htm	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Phishing:

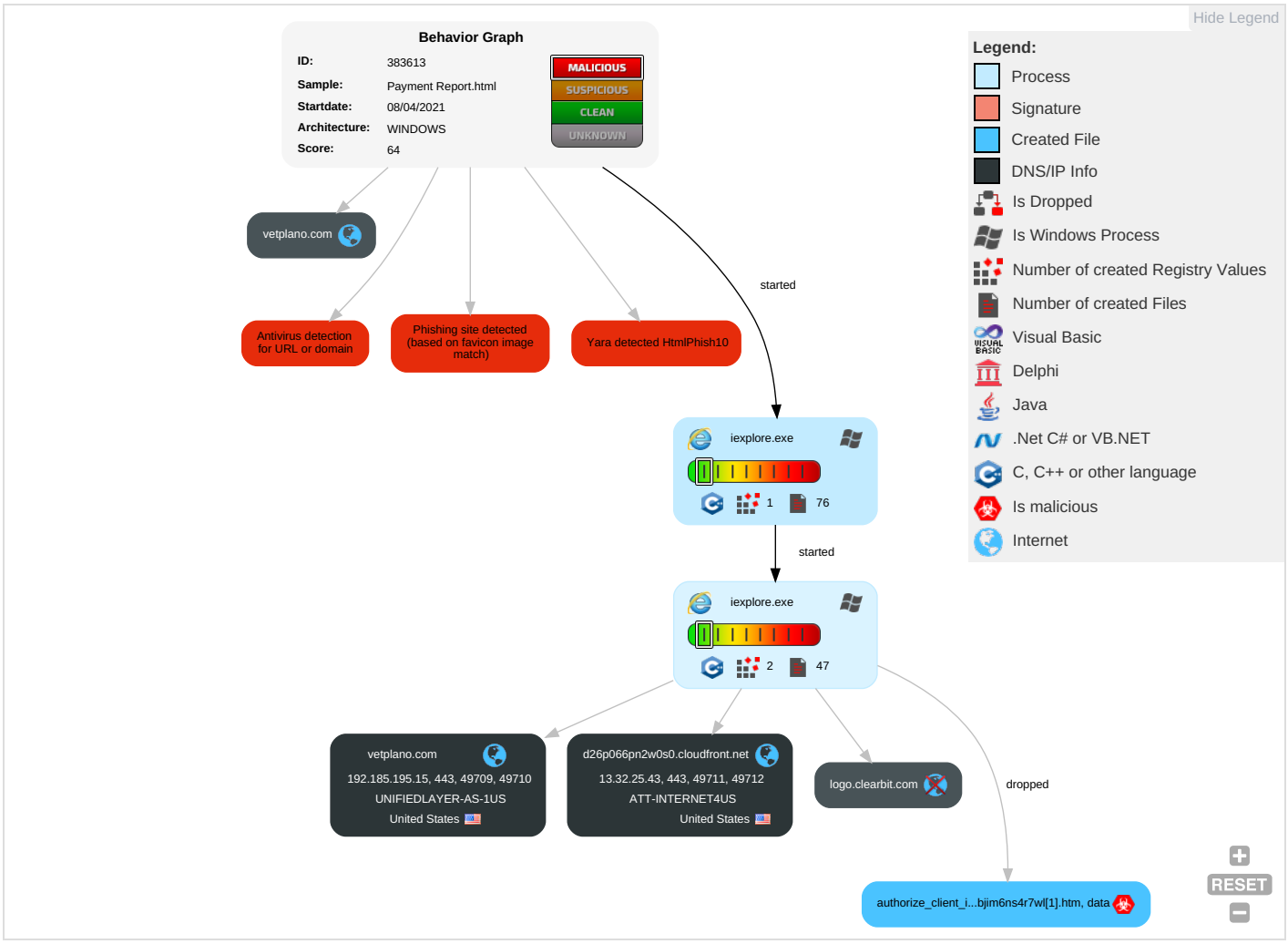
Phishing site detected (based on favicon image match)

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

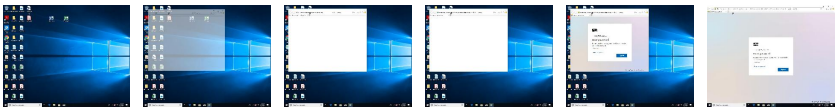
Behavior Graph

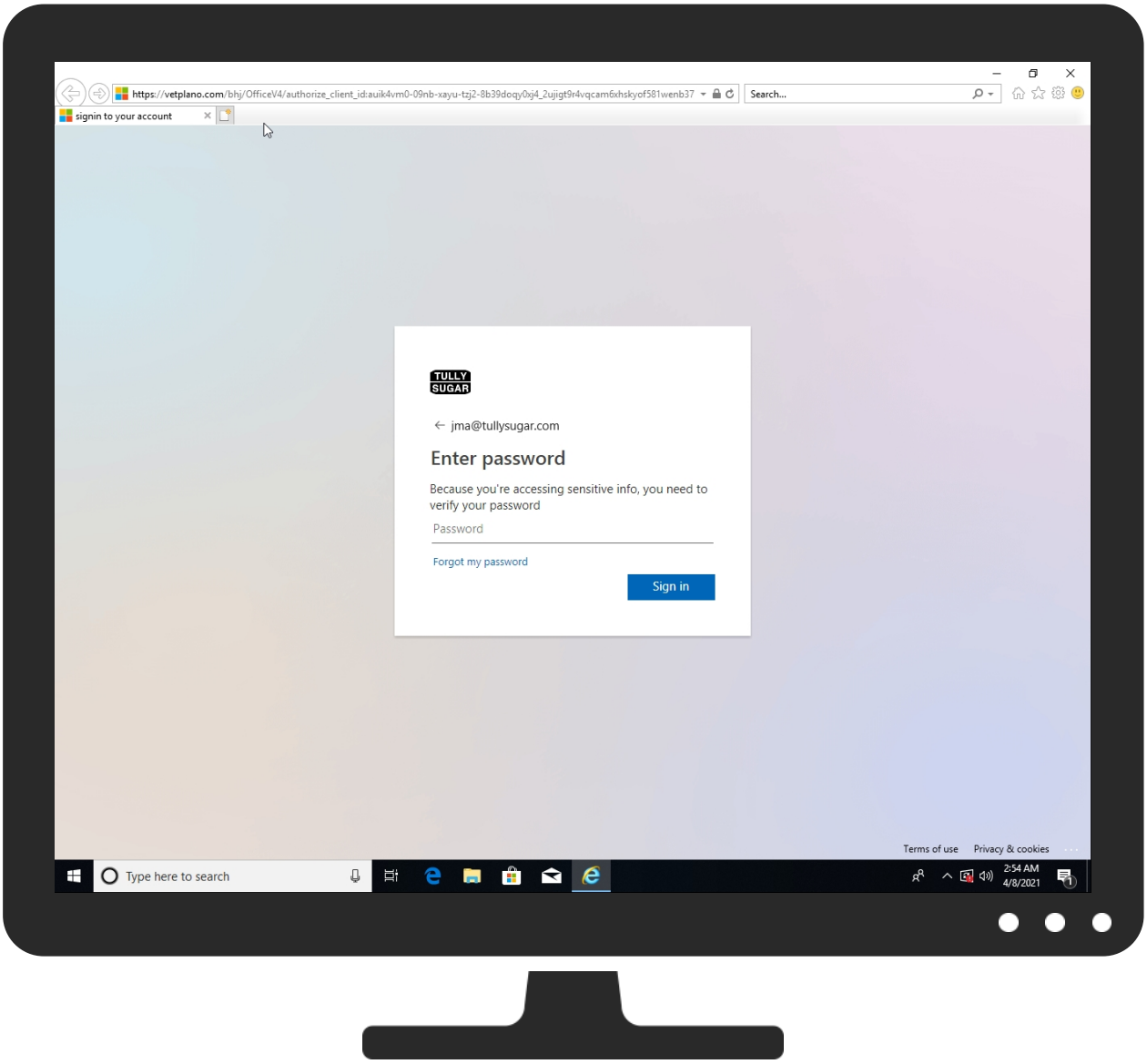


Screenshots

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
Payment Report.html	0%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
vetplano.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://vetplano.com/bhj/OfficeV4/authorize_client_id:auik4vm0-09nb-xayu-tzj2-8b39doqy0xj4_2ujigt9r4vqcam6xhskyof581wenb37dpzl0x7cpazksi4u9jfndvor60bqwm2hgy358t1leatz8peo3dxuk1vhcq0f29gy5bjim6ns4r7wl?data=am1hQHR1bGx5c3VnYXIuY29t	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	

Source	Detection	Scanner	Label	Link
http://https://vetplano.com/bhj/OfficeV4/images/favicon.ico~	0%	Avira URL Cloud	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://https://vetplano.com/bhj/OfficeV4/jma	0%	Avira URL Cloud	safe	
http://https://vetplano.com/bhj/OfficeV4/authorize_client_id:auik4vm0-09nb-xayu-tzj2-8b39doqy0xj4_2ujigt9r4	0%	Avira URL Cloud	safe	
http://https://vetplano.com/b/Desktop/Payment%20Report.htmlhj/OfficeV4/authorize_client_id:auik4vm0-09nb-xa	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
d26p066pn2w0s0.cloudfront.net	13.32.25.43	true	false		high
vetplano.com	192.185.195.15	true	false	• 0%, Virustotal, Browse	unknown
logo.clearbit.com	unknown	unknown	false		high

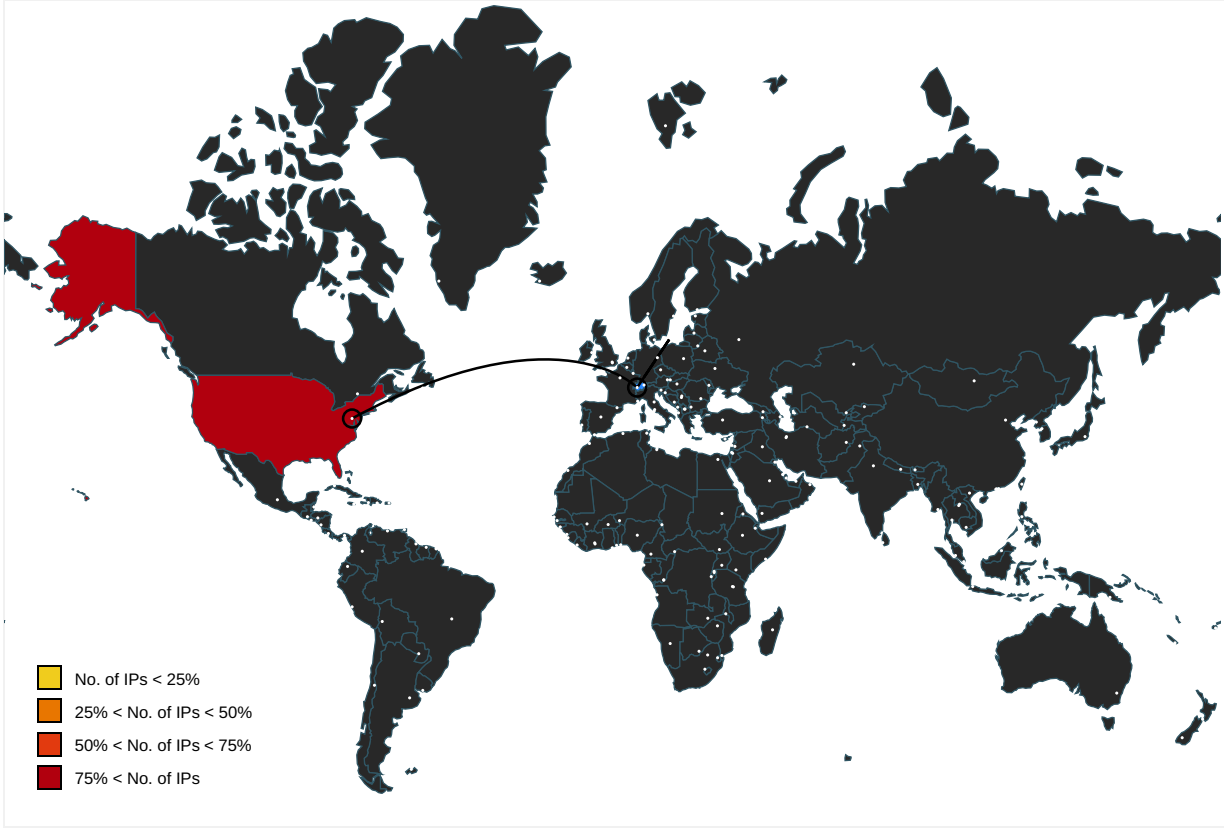
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://vetplano.com/bhj/OfficeV4/authorize_client_id:auik4vm0-09nb-xayu-tzj2-8b39doqy0xj4_2ujigt9r4vqcam6xhskyof581wenb37dpzl0x7cpazksi4u9jfndvor60bqwm2hgy358t1leatz8peo3dxuk1vhcq0f29gy5bjim6ns4r7wl?data=am1hQHR1bGx5c3VnYXIuY29t	true	• SlashNext: Fake Login Page type: Phishing & Social Engineering	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.nytimes.com/	msapplication.xml3.1.dr	false		high
http://www.youtube.com/	msapplication.xml7.1.dr	false		high
http://https://logo.clearbit.com/tullysugar.com	authorize_client_id_auik4vm0-09nb-xayu-tzj2-8b39doqy0xj4_2ujigt9r4vqcam6xhskyof581wenb37dpzl0x7cpazksi4u9jfndvor60bqwm2hgy358t1leatz8peo3dxuk1vhcq0f29gy5bjim6ns4r7wl[1].htm.2.dr	false		high
http://https://vetplano.com/bhj/OfficeV4/images/favicon.ico~	imagestore.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://www.wikipedia.com/	msapplication.xml6.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.amazon.com/	msapplication.xml.1.dr	false		high
http://www.live.com/	msapplication.xml2.1.dr	false		high
http://https://vetplano.com/bhj/OfficeV4/jma	Payment Report.html	false	• Avira URL Cloud: safe	unknown
http://www.reddit.com/	msapplication.xml4.1.dr	false		high
http://www.twitter.com/	msapplication.xml5.1.dr	false		high
http://https://vetplano.com/bhj/OfficeV4/authorize_client_id:auik4vm0-09nb-xayu-tzj2-8b39doqy0xj4_2ujigt9r4	~DFF0FCE8FDE9A2DE4D.TMP.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://vetplano.com/b/Desktop/Payment%20Report.htmlhj/OfficeV4/authorize_client_id:auik4vm0-09nb-xa	{EB817EBD-9804-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
13.32.25.43	d26p066pn2w0s0.cloudfront.net	United States		7018	ATT-INTERNET4US	false
192.185.195.15	vetplano.com	United States		46606	UNIFIEDLAYER-AS-1US	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	383613
Start date:	08.04.2021
Start time:	02:53:22
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 50s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Payment Report.html
Cookbook file name:	defaultwindowshtmlcookbook.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	7
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal64.phis.winHTML@3/29@3/2

Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .html
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, ielowutil.exe, wermgr.exe, UsoClient.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 104.83.120.32, 52.147.198.201, 13.88.21.125, 104.43.193.48, 152.199.19.161, 23.0.174.185, 23.0.174.200, 104.42.151.234, 52.255.188.83 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, ie9comview.vo.msecnd.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, skypedataprdcolcus15.cloudapp.net, e11290.dspg.akamaiedge.net, skypedataprdcoleus16.cloudapp.net, iecvlist.microsoft.com, skypedataprdcoleus17.cloudapp.net, go.microsoft.com, go.microsoft.com.edgekey.net, blobcollector.events.data.trafficmanager.net, audownload.windowsupdate.nsatc.net, watson.telemetry.microsoft.com, skypedataprdcolwus15.cloudapp.net, au-bg-shim.trafficmanager.net, skypedataprdcolwus16.cloudapp.net, cs9.wpc.v0cdn.net

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
d26p066pn2w0s0.cloudfront.net	SOC_0#7198, INV#512 Via GoogleDocs gracechung.html	Get hash	malicious	Browse	• 143.204.11.45
	BR-415364.htm	Get hash	malicious	Browse	• 52.84.148.48
	BR-278630.htm	Get hash	malicious	Browse	• 52.84.148.85
	Pds-ch-UPDATE.htm	Get hash	malicious	Browse	• 143.204.11.4
	RemittanceAdvice-000010434.htm	Get hash	malicious	Browse	• 143.204.2.94
	TICKET#030599_Stanfordhealthcareserv.htm	Get hash	malicious	Browse	• 143.204.2.94
	658908343Bel.html	Get hash	malicious	Browse	• 143.204.2.88
	658908343Bel.html	Get hash	malicious	Browse	• 143.204.2.94
	PolicyUpdate.htm	Get hash	malicious	Browse	• 143.204.202.86
	http://recp.mkt91.net/ctt?m=804040&r=Njg0NjYxMDU1NQS2&b=0&j=NjAwMDczOTg3S0&k=NCLogo&kx=1&kt=12&kd=http://silverphoto.my1.ru/go?https://u2ll1.csb.app#david.alvey@jomaxgb.us	Get hash	malicious	Browse	• 13.224.196.53
	http://www.663915-7531.wdfilmworks.com/1/exrobotosv4/am9uLm1hcnNoYWxsQGJyaXRpc2hnYXMuY28udWs=	Get hash	malicious	Browse	• 65.9.68.128

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://u19684446.ct.sendgrid.net/ls/click?upn=ExCkaDW5fRF4b0-2BdFzzXOpGVxUmUBkTQVDYtz6-2F-2F6sQpB9ec4YeTvc-2FPnUnDIMDIb2AubMzHga4hpNymDGbgcQ-3D-3DzXHV_gseYrccm3Yg9g0U-2Fb6V-2FwOEfVhEyzfJUY9CKuT6j1x6hD-2BVD-2FXrrL753UneC8JwdlSdsJxeT4uZO2-2FnkyzzY-2FV4KbpQiqBePez19ri47JFNd1qeGYdXzsneczJdxlKZq6YKBiHln2o-2BHlyeGrx7mmd-2FKEF6vDKuYmaVkkahRHIdR6pgQGZ4Xb00Ac-2FmtYPK8xGHgIeKMLtkPB0f7wUUc0nz2xc91qH5nUCgfdkLP-2ByM-3D	Get hash	malicious	Browse	• 13.224.93.64
	Ctr-066970-xlsx.HtmL	Get hash	malicious	Browse	• 13.224.93.64
	http://https://agentfortravellers.com/mark.spalding/crowecw.co/uk	Get hash	malicious	Browse	• 13.224.194.53
	keithie_graham@deanfoods.com.html	Get hash	malicious	Browse	• 143.204.11.4
	http://t8.al.alerteimmo.com/r/?id=h2423fa57,b481f3e,b481f45&p1=of85za0f.firebaseapp.com#TGVvbi5CcmFkbGV5QHBhcmFnb24tY2MuY28udWs=	Get hash	malicious	Browse	• 13.224.194.15
	http://https://vectecinc.com/aud/gyaltq2p80356chrwju1o4kdnzi7bfsxm9verektci7xygv12aw6p980bmjzq3nuf5dh4losobcj6twfavgsq12eku0r83pz59mh4xy7ndli?data=Y2FybG9zLmZyb250ZXJhQGJtcy5jb20=	Get hash	malicious	Browse	• 13.224.93.68
	Ctr-975552-xlsx.HtmL	Get hash	malicious	Browse	• 65.9.68.128
	http://t8.al.alerteimmo.com/r/?id=h2423fa57,b481f3e,b481f45&p1=jqm0psxu.firebaseapp.com#QW50b25lbGxhLkxhenplcmluaUBhZXNpY2EtcGhhcm1hLmNvbQ==	Get hash	malicious	Browse	• 143.204.215.18
	http://https://u19254403.ct.sendgrid.net/ls/click?upn=8KOHCqYdrmokF7XLscf1LPgUtjzOIjzkVGpq-2Bf8Ly3JTZf1tTynJgjpQKNe8-2BF0qpGD2O2LBfi7Xsvxtn9K9MQwfi3EVv0L7i-2BE9thOQnMY-3Db9OA_5Pgd5SEWYGWyGNZOcptdDlALrar2lxD23HFBzHgjYngkkj8Qmba9Axcei1zeYMM-2FstUioB1fWvvNFmhAeL7HvdBPCA7lQFO240WbkeiAbqRGffFAGG7TKmixkZG45ibxLRzjh2hxR-2FIq2lPExJ8V0l4pls-2BziqI3hRyzvAIb8S4dPVLxzjUSl3xUIosc3Z2mpbG5WfCy2Xv4xYTIp-2B-2FqKWttk-2Feo0JOzTE6x2tV5hp0-3D	Get hash	malicious	Browse	• 13.224.93.114

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
UNIFIEDLAYER-AS-1US	receipt-xxxx.htm	Get hash	malicious	Browse	• 162.241.124.32
	Order-027165.exe	Get hash	malicious	Browse	• 192.232.218.185
	Ewkoo9igCN.dll	Get hash	malicious	Browse	• 162.241.54.59
	49Bvnq7iFK.dll	Get hash	malicious	Browse	• 162.241.54.59
	OtOXfybCmW.dll	Get hash	malicious	Browse	• 162.241.54.59
	Ewkoo9igCN.dll	Get hash	malicious	Browse	• 162.241.54.59
	W3aLwWHvWB.dll	Get hash	malicious	Browse	• 162.241.54.59
	IJh1SAcSNP.dll	Get hash	malicious	Browse	• 162.241.54.59
	OtOXfybCmW.dll	Get hash	malicious	Browse	• 162.241.54.59
	afC9TbiOWl.dll	Get hash	malicious	Browse	• 162.241.54.59
	wABiemJeyB.dll	Get hash	malicious	Browse	• 162.241.54.59
	I316Yh2noM.dll	Get hash	malicious	Browse	• 162.241.54.59
	W3aLwWHvWB.dll	Get hash	malicious	Browse	• 162.241.54.59
	IJh1SAcSNP.dll	Get hash	malicious	Browse	• 162.241.54.59
	afC9TbiOWl.dll	Get hash	malicious	Browse	• 162.241.54.59
	9iJMZNQTad.dll	Get hash	malicious	Browse	• 162.241.54.59
	wABiemJeyB.dll	Get hash	malicious	Browse	• 162.241.54.59
	r4fUczb42h.dll	Get hash	malicious	Browse	• 162.241.54.59
	I316Yh2noM.dll	Get hash	malicious	Browse	• 162.241.54.59
	Gp23ivGAlH.dll	Get hash	malicious	Browse	• 162.241.54.59
ATT-INTERNET4US	PaymentAdvice-copy.htm	Get hash	malicious	Browse	• 13.32.25.94
	agmz0F8LbA.dll	Get hash	malicious	Browse	• 13.32.16.68
	aunobp.dll	Get hash	malicious	Browse	• 13.32.16.68
	document-1848152474.xlsm	Get hash	malicious	Browse	• 13.32.16.68
	PDjf628Sns.exe	Get hash	malicious	Browse	• 69.232.46.139
	1637.xlsm	Get hash	malicious	Browse	• 13.32.16.68
	993.xlsm	Get hash	malicious	Browse	• 13.32.16.68
	2139.xlsm	Get hash	malicious	Browse	• 13.32.16.68

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	3023.xlsm	Get hash	malicious	Browse	• 13.32.16.68
	2638.xlsm	Get hash	malicious	Browse	• 13.32.16.68
	3230.xlsm	Get hash	malicious	Browse	• 13.32.16.68
	2744.xlsm	Get hash	malicious	Browse	• 13.32.16.68
	document-759334105.xls	Get hash	malicious	Browse	• 13.32.16.68
	document-1784086484.xls	Get hash	malicious	Browse	• 13.32.16.68
	document-1597268706.xls	Get hash	malicious	Browse	• 13.32.16.68
	document-1315363159.xls	Get hash	malicious	Browse	• 13.32.16.68
	document-1137036824.xls	Get hash	malicious	Browse	• 13.32.16.68
	document-1981182525.xls	Get hash	malicious	Browse	• 13.32.16.68
	document-170129283.xls	Get hash	malicious	Browse	• 13.32.16.68
	document-2064292974.xls	Get hash	malicious	Browse	• 13.32.16.68

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
9e10692f1b7f78228b2d4e424db3a98c	receipt-xxxx.htm	Get hash	malicious	Browse	• 13.32.25.43 • 192.185.195.15
	Mortgagor Request719350939.html	Get hash	malicious	Browse	• 13.32.25.43 • 192.185.195.15
	Receipt779G0D675432.html	Get hash	malicious	Browse	• 13.32.25.43 • 192.185.195.15
	PaymentAdvice-copy.htm	Get hash	malicious	Browse	• 13.32.25.43 • 192.185.195.15
	agmz0F8LbA.dll	Get hash	malicious	Browse	• 13.32.25.43 • 192.185.195.15
	vniSIKfm4h.dll	Get hash	malicious	Browse	• 13.32.25.43 • 192.185.195.15
	61mwzdX4GC.dll	Get hash	malicious	Browse	• 13.32.25.43 • 192.185.195.15
	WbQrxxnmAO.dll	Get hash	malicious	Browse	• 13.32.25.43 • 192.185.195.15
	Invoice 880121.html	Get hash	malicious	Browse	• 13.32.25.43 • 192.185.195.15
	msals.pumpl.dll	Get hash	malicious	Browse	• 13.32.25.43 • 192.185.195.15
	Nickha #U0421#U0430ll Notification.mp3.htm	Get hash	malicious	Browse	• 13.32.25.43 • 192.185.195.15
	aunobp.dll	Get hash	malicious	Browse	• 13.32.25.43 • 192.185.195.15
	606d810b8ff92.pdf.dll	Get hash	malicious	Browse	• 13.32.25.43 • 192.185.195.15
	syscshost.dll	Get hash	malicious	Browse	• 13.32.25.43 • 192.185.195.15
	syscshost.dll	Get hash	malicious	Browse	• 13.32.25.43 • 192.185.195.15
	DropDll.dll	Get hash	malicious	Browse	• 13.32.25.43 • 192.185.195.15
	lc.dll	Get hash	malicious	Browse	• 13.32.25.43 • 192.185.195.15
	FARASIS.xlsx	Get hash	malicious	Browse	• 13.32.25.43 • 192.185.195.15
	msals.pumpl.dll	Get hash	malicious	Browse	• 13.32.25.43 • 192.185.195.15
	ofcRreui1e.dll	Get hash	malicious	Browse	• 13.32.25.43 • 192.185.195.15
37f463bf4616ecd445d4a1937da06e19	dMeVLLeyLc.exe	Get hash	malicious	Browse	• 192.185.195.15
	avast_secure_browser_setup.exe	Get hash	malicious	Browse	• 192.185.195.15
	PaymentAdvice-copy.htm	Get hash	malicious	Browse	• 192.185.195.15
	57fvgYpwnN.exe	Get hash	malicious	Browse	• 192.185.195.15
	8e29685862fc0d569411c311852d3bb2da2eedb25fc9085a95020b17ddc073a9.xls	Get hash	malicious	Browse	• 192.185.195.15
	9mm case for ROYAL METAL INDUSTRIES 3milmonth Specification drawings.exe	Get hash	malicious	Browse	• 192.185.195.15
	Scan emco Bautechni specification.pps	Get hash	malicious	Browse	• 192.185.195.15
	Lista e porosive te blerjes.exe	Get hash	malicious	Browse	• 192.185.195.15
	Notice-039539.xlsm	Get hash	malicious	Browse	• 192.185.195.15
	IMG_767893434432.exe	Get hash	malicious	Browse	• 192.185.195.15
	OH76.vbs	Get hash	malicious	Browse	• 192.185.195.15
	INVOICE_.EXE	Get hash	malicious	Browse	• 192.185.195.15

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	FED8GODpaD.xlsb	Get hash	malicious	Browse	• 192.185.195.15
	JANUARY OVERDUE INVOICE.pdf.exe	Get hash	malicious	Browse	• 192.185.195.15
	elef.exe	Get hash	malicious	Browse	• 192.185.195.15
	FARASIS.xlsx	Get hash	malicious	Browse	• 192.185.195.15
	dl8.exe	Get hash	malicious	Browse	• 192.185.195.15
	Ordine d'acquisto 240517_04062021.exe	Get hash	malicious	Browse	• 192.185.195.15
	catalogue-41.xlsb	Get hash	malicious	Browse	• 192.185.195.15
	ddff.exe	Get hash	malicious	Browse	• 192.185.195.15

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{EB817EBB-9804-11EB-90EB-ECF4BBEA1588}.dat

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8492867202673156
Encrypted:	false
SSDEEP:	192:rHZgZ/2nW2+t2y2if2dU222zMm2u2Br2I2Dn2sfMU2X2jX:r5wuW2+2c2gpOFF
MD5:	8C0E48005B9B27712BE1C171FC1E4D5A
SHA1:	35EB7A7B02155D6AB0B8009C47A63073D3815D01
SHA-256:	FE001C13807924A6BDAB73636149D95411032AF4D04D1B907DEFB1FBADBE3F55
SHA-512:	F5F6F89366C53940C8D98DEF8B8D46510E930231B844C6B1734131A9A711C62AA4E43D8A4047A79D5F97247AA5771781430A055954933D4FA5A38B0B79EA4A1E
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\{EB817EBD-9804-11EB-90EB-ECF4BBEA1588}.dat

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27192
Entropy (8bit):	1.7284016236617306
Encrypted:	false
SSDEEP:	48:lwjGcprqGwpaiG4pQeGrapbSOGQpB6GHHpcTTGUp89GzYpmSEGoptc6rQG6XpXcW:rZZyQS6QBSGjB2tWDMbjp6liQuMcwr
MD5:	1BAC53387AFD0DF5C55681AA20C69A91
SHA1:	4F24E82CD20F9C7B4513744B9959C7732B919FD4
SHA-256:	9E9DD0C8E27338D9F82FD56D15F641DF8D9A834188E8FB468C3F80AF6DDFEE9E
SHA-512:	F90726DEF8170181B31856E1528A8B50F95D09CBFB5556F72982FA13C909EAD306EF0FE742C7F225CEA41AB28665138C2D4EFE5F4B41D8CC6E8975F1D09F996D
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\{F2B4769A-9804-11EB-90EB-ECF4BBEA1588}.dat

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5642774901400458
Encrypted:	false
SSDEEP:	48:IwlMGcprLXGwpauG4pQ2GrapbSIGQpKSG7HpRATGIpG:raZdQO64BSwA9TUA
MD5:	C998CFF2E50522EF08B6E9F9E7B2B0F8

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{F2B4769A-9804-11EB-90EB-ECF4BBEA1588}.dat	
SHA1:	7E6DFA50EB24C2FC5C7A844BD2828FD597AE80BF
SHA-256:	77D216276E7C977CC4C937997CFB326C981B1F9BA285410FCD69C1A3E847442A
SHA-512:	47B417A213E25B83AB0C94F0D796B75C10A07343F5F625710E311547BC5F0155C761B160248B168D278D2EF7637BCEF7B0922AEF92ADF0E43DD96A89F5E6D7BE
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.02426293634196
Encrypted:	false
SSDEEP:	12:TMHdNMNxOE1nWimI002EtM3MHdNMNxOE1nWimI00OYGVbkEtMb:2d6NxOcSZHKd6NxOcSZ7YLb
MD5:	D7AAD8C561C94A7986A4C2C4F5E69B17
SHA1:	AA890516A8550B71A1BB4754E1D4AAECD0970604
SHA-256:	43E39D00BF9E85247186B8000416C17EA8594480BD19E63C2195C2BFA36AA391
SHA-512:	63D48D8A88E95AE7566468B5DBF9E5462F962C77FF1DE2700A490DC9882FD950250FAAA103E4B966AB1671C2C01EA489F3F2CCB2340C55055334AFDC9F01EF1
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0xc3e7731c,0x01d72c11</date><accdate>0xc3e7731c,0x01d72c11</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0xc3e7731c,0x01d72c11</date><accdate>0xc3e7731c,0x01d72c11</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Twitter.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.128207085532373
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kOMEB/MEB8nWimI002EtM3MHdNMNxe2kOMEB/MEB8nWimI00OYGkan:2d6NxrldB/dB8SZHKd6NxrldB/dB8SZN
MD5:	C85F4BC6D6BF8AC759CCE8E2B17BE6F8
SHA1:	9AF45172CF47519E1B0CFB3CD9B7E789506AB2A3
SHA-256:	9CEC44418CFD12E1832C03CEA0C6E8DA37AB91375083EC253AAF6B6BDF3FEC06
SHA-512:	D2B36FA4206A6A6CB88DF8710F710754898BCB3284A55A8B5C958CC6E05D9EFAB40DC1BB20D87A4C7E728A01C0222F6917F4543C3A82B0EEFEEA7C248FB303A
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0xc3d46094,0x01d72c11</date><accdate>0xc3d46094,0x01d72c11</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0xc3d46094,0x01d72c11</date><accdate>0xc3d46094,0x01d72c11</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Amazon.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	662
Entropy (8bit):	5.045215891516582
Encrypted:	false
SSDEEP:	12:TMHdNMNxvL1nWimI002EtM3MHdNMNxvL1nWimI00OYGmZEtMb:2d6NxvBSZHKd6NxvBSZ7Yjb
MD5:	DCEE248F058F074249ACB9F46D2B2403
SHA1:	0B3722EF633B0A337874F561C33422D8BAEDC1D1
SHA-256:	013E4745CFCAE86E62EA677367DCF9B557D63FAD65483C6BAC6922AF138AD042
SHA-512:	1910F5023A158DEA8B7380F6F6C8A86FEED841F4A31FE541B90961CC33ADC84ACEFB19F4FA2C6666F2DA024458AD1C118DDB66B3F88612566D09BF37C9B4180
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0xc3e7731c,0x01d72c11</date><accdate>0xc3e7731c,0x01d72c11</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0xc3e7731c,0x01d72c11</date><accdate>0xc3e7731c,0x01d72c11</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Wikipedia.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	647
Entropy (8bit):	5.032558694706543
Encrypted:	false
SSDEEP:	12:TMHdNMNxibvVRvVpnWimI002EtM3MHdNMNxibvVRvVpnWimI00OYGd5EtMb:2d6Nx2fpSZHKd6Nx2fpSZ7YEjb
MD5:	E9589143A2726FFED6F0C7EC52193F52
SHA1:	5438BE456CEDDD5036C12526E9E9067D8A06A72B
SHA-256:	AD7D3D23C15D33BF2741588B712E7CDF30DCD53C1389E0C5E3EA626B6B5ADB23
SHA-512:	77B54644FEDA860F37621BF005615066CF19EDC966428C2AC7104799281951964E97E5F8E8C672FDF50A0AC3B4E4A8172485E8B0EFB19DEECB75D793D3B4F30E
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0xc3e510e1,0x01d72c11</date><accdate>0xc3e510e1,0x01d72c11</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0xc3e510e1,0x01d72c11</date><accdate>0xc3e510e1,0x01d72c11</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Live.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.058564389506221
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGw1nWimI002EtM3MHdNMNxhGw1nWimI00OYG8K075EtMb:2d6NxQgSZHKd6NxQgSZ7YrKajb
MD5:	797A03555984A4426640E4BB6A6B6B58
SHA1:	9AD429DB88EEC32876FBD7709D9D72F8942789E2
SHA-256:	697575294134AE87951CEE5B4BDA2BB0799269F1A711D38006CA10799834783B
SHA-512:	7BA09087E62627DAB39EA126D4267D11EDC1EE0DAAFF6B9900E31E6890291B11683769F6809674EA99C3B22CDFF0AA925D52320F419BA37BA66A9B1414766B78
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0xc3e7731c,0x01d72c11</date><accdate>0xc3e7731c,0x01d72c11</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0xc3e7731c,0x01d72c11</date><accdate>0xc3e7731c,0x01d72c11</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Youtube.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.027705103901905
Encrypted:	false
SSDEEP:	12:TMHdNMNx0n1nWimI002EtM3MHdNMNx0n1nWimI00OYGxEtMb:2d6Nx01SZHKd6Nx01SZ7Ygb
MD5:	0E462C8BE7EC349EEBE96ED6C4772D87
SHA1:	A8C34699C235C2A8B696F8E21258A3EB68ED3BC6
SHA-256:	1C03A0A65CD5EAF323883173D9C40C54F8811E77700C769FA14E36B6286A0853
SHA-512:	89C92FA0D468E60C1052DFA4A6C445A7F439162DFD922C7DAE874BCC339868D1EB5424CED20D7078FCF9A0A8730F4A8F2E34E463C7D90C1A0B195C1E0A930C3
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0xc3e7731c,0x01d72c11</date><accdate>0xc3e7731c,0x01d72c11</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0xc3e7731c,0x01d72c11</date><accdate>0xc3e7731c,0x01d72c11</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Reddit.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.057786059554545
Encrypted:	false
SSDEEP:	12:TMHdNMNxxbvVRvVpnWimI002EtM3MHdNMNxxbvVRvVpnWimI00OYG6Kq5EtMb:2d6NxrfpSZHKd6NxrfpSZ7Yhb
MD5:	BD2B6C5AC1A7DADC9D31C4EB8757995C
SHA1:	B464272578292A7C19FB890D62569A66E465D12D
SHA-256:	77401FDA1FB170BE0E2E72D05D31514F54AED26FC81D4B514110F5DBAB59CC8F
SHA-512:	FE19F986E3B9A0D98EA255BCFAA93B75F23B847140169AD2A95FFEA772C6BC287834752917C537FB799312C834330562D2AD8E084C3CE5554531315F66AFFB83
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0xc3e510e1,0x01d72c11</date><accdate>0xc3e510e1,0x01d72c11</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0xc3e510e1,0x01d72c11</date><accdate>0xc3e510e1,0x01d72c11</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\NYTimes.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	659
Entropy (8bit):	5.058587956548334
Encrypted:	false
SSDEEP:	12:TMHdNMNxcgOTOCnWimI002EtM3MHdNMNxcgOTOCnWimI00OYGVEtMb:2d6Nxm6CSZHKd6Nxm6CSZ7Ykb
MD5:	25BCD2BD63C027DBA28AECDB12DAB82F
SHA1:	7B9B9087057A01E760FF1F59F6B949D7C8F024E7
SHA-256:	931F2A402AB5AD230AF60461702F0972E28A046AD189F2443F2D3D24EF74BA5A
SHA-512:	2C2722E98E6936C3F6D444E742DA64B03374CD14763385D56E210F74CB98B1196FB5170CDDD54FD78276564B25E444DF77F40999C0C3FF32E6E408E88A82EC99
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0xc3e2ae78,0x01d72c11</date><accdate>0xc3e2ae78,0x01d72c11</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0xc3e2ae78,0x01d72c11</date><accdate>0xc3e2ae78,0x01d72c11</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Facebook.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.0186078836388734
Encrypted:	false
SSDEEP:	12:TMHdNMNxfnbvVRvVpnWimI002EtM3MHdNMNxfnbvVRvVpnWimI00OYGe5EtMb:2d6NxJfpSZHKd6NxJfpSZ7YLjb
MD5:	D857632B1DD571C94B3ACDCDF2F00DB0
SHA1:	74E5F39C74FC5E243A78E0FA319B8ECA29B9647B
SHA-256:	E195A5FBAD060451607A7FE070ACA4F716773E140AE010FAFD80E75877F9145E
SHA-512:	03B1E39E963393CEBC7A3BADD3F014B753F0F771BC109150458897271BF8E2052321A592B2660089387C0965031E83F2BEC43F9FB712DDB44AEA2A129DDB7061
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0xc3e510e1,0x01d72c11</date><accdate>0xc3e510e1,0x01d72c11</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0xc3e510e1,0x01d72c11</date><accdate>0xc3e510e1,0x01d72c11</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Google.url"/></tile></msapplication></browserconfig>..

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:	modified
Size (bytes):	1292
Entropy (8bit):	4.9703117313775165
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\gee00pr\imagestore.dat	
SSDEEP:	24:3ZyHmyQOyrQZ9FjFjFjFAZ4qCYORlzi+fzi+fzi+fziAVR9e:3Zym5OyoBBB6ZvORlzi0zi0ziGR9e
MD5:	9C1AC597BD949635BA668814DB518994
SHA1:	9C6252A68008D1DBDDA39B88BF3088ADC73DD3AD
SHA-256:	2F9DA2EBB2D546F77FA15C5AAEB5657F6325B092A1E21E8E2032DC5F6E48788B
SHA-512:	895E51BB317542E1D200B8CAC948D9787966461B8A54713E88EB3C8324F0A348B55943140EAAB10F0660CA7254E4B14ED999C1FA6B538690310CF2F4189F7EDA
Malicious:	false
Reputation:	low
Preview:	4.h.t.t.p.s.:././.v.e.t.p.l.a.n.o...c.o.m./.b.h.j./.O.f.f.i.c.e.V.4./.i.m.a.g.e.s./.f.a.v.i.c.o.n...i.c.o.~..... .h.....(..... ....P..$..%..%..%..%.."...}.....9e..<h..<h..<h..<h..;f..c....2.....f.w....K...N...N...N...N...L..Iq...3.....g.w....L...O...O...O...O...N..Jr...3.....g.w....L...O...O...O...O...N..Jr...3.....g.w... .L...O...O...O...O...N..Jr...3.....g.w....L...O...O...O...O...N..Jr...2.....f.u...I...L...L...L...L...K..Gp.....g...i...i...i...i...i...f.....f...g...g...g...g...e. .....g..i..i..i..i..h...../.....j...d....{...}...}...}...}...}...|.6..0.....k...f....}.....~.8..0.....k...f....}.....~.8..0.....k... f....}.....~.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\arrow_left[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	513
Entropy (8bit):	4.720499940334011
Encrypted:	false
SSDEEP:	12:t4BdU/uRqv6DLfBHKFWJCDLfBSU1pRXIFl+MJ4bADc:t4TU/uRff0EcfIU1XXU+t2c
MD5:	A9CC2824EF3517B6C4160DCF8FF7D410
SHA1:	8DB9AEBAD84CA6E4225BFDD2458FF3821CC4F064
SHA-256:	34F9DB946E89F031A80DFCA7B16B2B686469C9886441261AE70A44DA1DFA2D58
SHA-512:	AA3DDAB0A1CFF9533F9A668ABA4FB5E3D75ED9F8AFF8A1CAA4C29F9126D85FF4529E82712C0119D2E81035D1CE1CC491FF9473384D211317D4D00E0E234AD9F
Malicious:	false
Reputation:	moderate, very likely benign file
IE Cache URL:	http://https://vetplano.com/bhj/OfficeV4/images/arrow_left.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="24" height="24" viewBox="0 0 24 24"><title>assets</title><path d="M18,11.578v.844H7.617l3.921,3.928-.594.594L6,12l4.944-4.944.594.594L7.617,11.578Z" fill="#404040"/><path d="M10.944,7.056l.594.594L7.617,11.578H18v.844H7.617l3.921,3.928-.594.594L6,12l4.944-4.944m0-.141-.071.07L5.929,11.929,5.858,12l.071.071,4.944,4.944.071.07.071-.07.594-.595.071-.07-.071-.071L7.858,12.522H18.1V11.478H7.858l3.751-3.757.071-.071-.071-.07-.594-.595-.071-.07Z" fill="#404040"/></svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\authorize_client_id_auik4vm0-09nb-xayu-tzj2-8b39doqy0xj4_2ujigt9r4vqcam6xhskyof581wenb37dpzl0x7cpazksi4u9jfndvor60bqwm2hgy358t1leatz8peo3dxuk1vhcq0f29gy5bjim6ns4r7wl[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12551
Entropy (8bit):	5.612227253232923
Encrypted:	false
SSDEEP:	384:1EieroBIld6UTyv6R0+nQKrlibQmYMH/pMa1E:rbu/yvCndhi8yfpH1E
MD5:	028E9ADEDBF10369DBD6EE6E85CA753A
SHA1:	7E608145F95C29C6E1D439C9ABD18F7C953A39F5
SHA-256:	29F162E1A487C0EA7826EEFC3FC4919E404C668A43B3004EE8EEF8D3A429EA8C
SHA-512:	59C7E8EB696F4248FA46193E790FF81F602DCE9C97F577B13C6874C86F6767665C8B4FB7927601E3EED68FD8A12985A1F3C01F2A3E535F13584B811BBE8A00FF
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_10, Description: Yara detected HtmlPhish_10, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\authorize_client_id_auik4vm0-09nb-xayu-tzj2-8b39doqy0xj4_2ujigt9r4vqcam6xhskyof581wenb37dpzl0x7cpazksi4u9jfndvor60bqwm2hgy358t1leatz8peo3dxuk1vhcq0f29gy5bjim6ns4r7wl[1].htm, Author: Joe Security
Reputation:	low
Preview:	<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">.<html dir="ltr" class="" lang="en"><head><meta http-equiv="Content-Type" content="text/html; charset=utf-8">. <title>signin to your account</title>. . <meta http-equiv="X-UA-Compatible" content="IE=edge">. <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=2.0, user-scalable=yes">. <meta http-equiv="Pragma" content="no-cache">. <meta http-equiv="Expires" content="-1">. <meta name="referrer" content="no-referrer"/>. <meta name="robots" content="none">. <noscript>. <meta http-equiv="Refresh" content="0; URL=./" />. < /noscript>. <link rel="icon" href="images/favicon.ico" type="image/x-icon">. <link href="css/style.css" rel="stylesheet" >.</head>..<body id="t6qk07b" class="nd cua jy0k9" style="display: block;">. .. <div style="background-image: url("images/inv-small-backgro

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\forgpass[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 121 x 20, 8-bit/color RGB, non-interlaced
Category:	downloaded
Size (bytes):	713
Entropy (8bit):	7.532865305314849

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\forgpass[1].png	
Encrypted:	false
SSDEEP:	12:6v/7WGu/MYrBNPY+iJy9aiXYgAITAmdQWjCxKy8wQg+dBH6m67tjtbYjGNgUFu56:3TrBNP7iJy9adGrQWjoDZOSUGNB4vOOm
MD5:	B19CAC60E41C79BD974C1080088C6FEF
SHA1:	FFE553D8CA430DD309494E910A989271648A4DDD
SHA-256:	E29DB32031DC537AEE9CB557B408395F3324F1E0F744349C0CDF943A3AF39296
SHA-512:	04169E96DD18AA3BB6A56D60388D05CEF24418CB109A7613E2378F275E65BE57A1D4057E12BB90126A07CAC89578830A66E2036835CE0817CB6E22BC11BA0A19
Malicious:	false
Reputation:	moderate, very likely benign file
IE Cache URL:	http://https://vetplano.com/bhj/OfficeV4/images/forgpass.png
Preview:	.PNG.....IHDR...y.....&.....sRGB.....gAMA.....a.....pHYs.....o.d...^IDATXG.V...0..C..H..-..."U....Q...]...xn.....yz+.8.;.B.z?t..C.....=.7.t9....hj...B..Q..y?.N?^^.\..}<.3%t<...R,2..D...&..s.:XAkr5,..D .J.....u.a...nl%.c.&4...k.,_..+7.B.Y.1GEyA-.....#p..b....r.nSb.....tu.F.q.^...b.B..?/.6....s4`.C.. ..5f...:._p...._.+.w...[O.S*...@.I.d0..."i..hcLA^.....<F.t...VnIEQ.7.C..2.P.^Ekhg.Hx.$...%F..%@....K..l[.Z#.cN.jZY:hg.Z.E.aYk..RvZ.....{...*.LH.[..bK.\|... ..}..Z..G.*.\|.t.k.....ON..a.1..D.....$..pT.v..8.J....F.....1..!....D\y.....g..n.....#<..d.q.i!0...H>z..ZA\.-.].4.....G.....8..e..f..%Z....z.7....E...}....~.Z..^x....Q,.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\style[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	96336
Entropy (8bit):	5.237139828082104
Encrypted:	false
SSDEEP:	1536:qUBpw+kGaazA/PWrF7qvEAFiQcpm7tEGyf5c:qiS7yfC
MD5:	9F94F80A5DC09BB962778175292195BC
SHA1:	A7F2E32B422AC9654F39EA870E403599791FCE1C
SHA-256:	1CF4B3AD7ABF3189E78C1B3BD07308C92A03FA795FDBC5821FCDE24030CFEAD0
SHA-512:	85BADDE06E879CBF558163B123BD6A35D58498F15013B981EDB849699C31FC1915B2494595C6FF0E146365413E007C2D3AB32BC83AC70632E64EE08B2B040E44
Malicious:	false
IE Cache URL:	http://https://vetplano.com/bhj/OfficeV4/css/style.css
Preview:	html{font-family:sans-serif;-ms-text-size-adjust:100%;-webkit-text-size-adjust:100%}body{margin:0}article,aside,details,figcaption,figure,footer,header,hgroup,main,menu,nav,section,summary{display:block}audio,canvas,progress,video{display:inline-block;vertical-align:baseline}audio:not([controls]){display:none;height:0}[hidden],template{display:none}a{background-color:transparent}a:active,a:hover{outline:0}abbr[title]{border-bottom:1px dotted}b,strong{font-weight:700}dfn{font-style:italic}h1{font-size:2em;margin:.67em 0}mark{background:#ff0;color:#000}small{font-size:80%}sub,sup{font-size:75%;line-height:0;position:relative;vertical-align:baseline}sup{top:-.5em}sub{bottom:-.25em}img{border:0}svg:not(:root){overflow:hidden}figure{margin:1em 40px}hr{-moz-box-sizing:content-box;box-sizing:content-box;height:0}pre{overflow:auto}code,kbd,pre,samp{font-family:monospace,monospace;font-size:1em}button,input,optgroup,select,textarea{color:inherit;font:inherit;margin:0}button{overflow:visible}but

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\favicon[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 1 icon, 16x16, 32 bits/pixel
Category:	downloaded
Size (bytes):	1150
Entropy (8bit):	4.895279695172972
Encrypted:	false
SSDEEP:	24:NrQZ9FjFjFjFAZ4qCYORlzi+fzi+fzi+fziAVR9:NoBBB6ZvORlzi0zi0zi0ziGR9
MD5:	7CDD5A7E87E82D145E7F82358F9EBD04
SHA1:	265104CAD00300E4094F8CE6A9EDC86E54812EAD
SHA-256:	5D91563B6ACD54468AE282083CF9EE3D2C9B2DAA45A8DE9CB661C2195B9F6CBF
SHA-512:	407919CB23D24FD8EA7646C941F4DCEE922B9B4021B6975DD30C738E61E1A147E10A473956A8FBB2DDF7559695E540F2CDF8535DB2C66FA6C7DECDA38BB1B12
Malicious:	false
IE Cache URL:	http://https://vetplano.com/bhj/OfficeV4/images/favicon.ico
Preview:	..... .h.....(..... ....P..$..%..%..%..%.."...}.....9e..<h..<h..<h..<h..;f..c....2.....f.w....K...N...N...N...N...L..Iq...3.....g.w....L...O...O...O...O...O...N..Jr...3.....g.w....L...O...O...O...O...N..Jr...3.....g.w....L...O...O...O...O...N..Jr...3.....g.w....L...O...O...O...O...N..Jr...2.....f.u....I...L...L...L...L...K..Gp.....g...i...i...i...i...f.....f...g...g...g...g...e.....g..i..i..i..i..i..h...../.....j...d....{...}...}...}...}...}...|..6..0.....k...f....}.....~.8..0.....k...f....}.....~.8..0.....k...f....}.....~.8..0.....k...f....}.....~.8..0.....k...f....}.....~.8../.....j...e....|...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\tullysugar[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 128 x 128, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	5262
Entropy (8bit):	7.923934727909639
Encrypted:	false
SSDEEP:	96:FDae6866J/TuNPGuw5gHnlOz9R0XHn8KIhSRUsn4PDz3kJxdIt+VGF9pKm:tK85JKN+V5AnlOWc2RR4exdIE4Om
MD5:	F9BC7F22111D0FC589DC64A92168C519
SHA1:	389601ABA2D2ED82F4167735115CCED24DE262B3

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\tullysugar[1].png	
SHA-256:	10505AD140E4DA699252680C9BD43626471F44F98731AFA84122A5B5F91C40D8
SHA-512:	EE7A1C7F6891EE16392211B0D62F386A4006BA2EA5626EC0E7E1EF8363559710120E7ADDEFEB1884A0ED7C3D5CF42D1AC1A1A60C713A6A28074F66176B8CE83A
Malicious:	false
IE Cache URL:	http://https://logo.clearbit.com/tullysugar.com
Preview:	.PNG.....IHDR.....>a....UIDATx..]ytM...L.".!f.R....z.y....Vi..@.....U-.Z^.K.U.T.-.5....Rm...H..%.L...g.{..s...+n{.g.....9{....C... ..!.`r......&. ..!.`r......&. ..!.`r......&. ..!.`r.....&. ..!.`r....~.....M.....53g.,.....b.PMM.....TUUY.$..c5.*....."%%%`.A.....UUU...(e..AD.....e..q"....,.....,_.....,K..b.....P.....".HD.].O...c...hbyyy..7oF.. ..L..;....".v..wDt.....D.....X/.....-.....4 ./....*#...2..".=.U+.....D....b.3w..".>....h...;..>>>.X,.*/(..w.....jKD.[..]@..|@?..'..A..}.C.qP.~}.=z4...<.d....Pff&....C.=Dm.U|...aJKK.|.....v..m .....[S||.".##.~..Wb..T. ^....Lu....={\J'<<....) @....Q:}.....5jD.>.(.....s'].|.h.....=.ysVTT.j...j..3..4....M.....)S.8,..?..].}...{v.av.-[.....<..6m.....im..Y,.....b.....,,,..{.'OV...O.:.BBB\...;. .....q....4o.<*--U....RBB..;.zC..U.A.|..7T\\.r..^.B.zc.....;O....3grQ.FLL....)..AA..^...pK.WUU.3g.-..d.~..."..XK7Ao....S.....|

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\inv-big-background[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 1920 x 1080, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	174883
Entropy (8bit):	7.933595362471097
Encrypted:	false
SSDEEP:	3072:NCe5AF33GgclaMBMtNxgFlxIUtjFJIj6lTmE/ORHhAFPy+huXdVnwNAH:NTOFeKtN6DIUtjdl3TgoyH
MD5:	62DDD263C8A6A4C9074E205B91182D04
SHA1:	1B56D11B012DD79DD99212EBB54ADCFB60920A9D
SHA-256:	A59EA699D353D00FF2999111F9FA11FB73A47EDA7800642609CA230560EA3703
SHA-512:	0BDAE93DDE9753BB7FB2B80B63226F3AC04F9CF58D3F954F0E9B8900F4AE5971D3B1270D4E5101E9A346B218689F7A40D70823683FBB719248A53648C02648F2
Malicious:	false
IE Cache URL:	http://https://vetplano.com/bhj/OfficeV4/images/inv-big-background.png
Preview:	.PNG.....IHDR.....8.....1q...bPLTEqart]c)L.qpwC..ykfX...pC.xHw`..m.JQ.7M.lYK..th.r..?...j<hW}e...lKit...^T....S..r@M.gUouZ.XR.?..m.!J.h;.k..i.+K.@..m..ZQ._U.WQ.K.. .mB._..g..l.|\.._Vog.M..JQ..k..h..cL8M.c..Z..~^..c.RP.._.fX..nJ.xS>L.dn.gV...j.`..c._~.ZU..e.eU..i.{|r5N.Zu.0J..ye.b..g..b@S~..e.{.{.\lqZ..a.lTcNN.?L..`..d.v[.xXVHM..g..u X.e:.d.aQp.{^.d..g..zg.e.XO}k...f..d.<...c.u.tvVV.c7.....vtRNS/.-.-/.-0/&..-/-,/*)/.-1.20--0/.*-&")*)/-*.++11,+-)+*.&-(.,/-./.*/'*000-,-)/0/-*+/-,***/*.*+++000+,-,$-*/)0,**,'0&(,)!.Y]$.... IDATx..A..0.Eg.;..U.d....9....._..%..(.p.$.....}.....yg.vV...V.A<.WW..V...yP.5....5...F}Y.|..|...?*.`...M...6'....<w..x.a;'..=.5....l...\....].On.l[gdg....|^.YO....x.LE..p...._.....0.$..Ky..*L ...]m]...v..!.IL.[..#x.uz..^M(...A.RE..';..e..|.#.<b}..J..GC...0i.[.[-ZW/._P8....M.,.....q.....dg...B.*Q...M.|.j...XwD....d.bJ..../....._.....z5.P...}.....^...K..=rH..k.p%g...+:..-}_..6. ..^%0.z.V.n..C#.a....y....`...h...{.%.{..05.1ry..p..'.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\passwrd[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 69 x 34, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	902
Entropy (8bit):	7.5760721199160015
Encrypted:	false
SSDEEP:	24:D8kvmvmvmvmvmvmvmvp/Hsj2IruKpPUjMFp5z/xkvAVtaWpX9gCEQ:D8mYYYYYYRMquHnn5OvIaK8Q
MD5:	4F2A1D382216546E2C3BC620497FD4E3
SHA1:	F785EC5967B5666387304F779306F9C3E3359FF4
SHA-256:	105C03D3360CDB953585482374B2CC953D090741037502B0609629F5BB0135B7
SHA-512:	6307ADD035382E50C1B8751E567810AF9C258D8A126C536A9582D2B80C6BEDB87308E991519C7BA07041B9F108C058FF80D90BCC3E36E1FA965C287097522473
Malicious:	false
IE Cache URL:	http://https://vetplano.com/bhj/OfficeV4/images/passwrd.png
Preview:	.PNG.....IHDR...E..."......|.....sRGB.....gAMA.....a.....pHYs.....+.....IDAThC.r.0...n.....e1..#..E.....a....aX..o.-.r..c.~3.....3....L.-... .. ..OcH.4. [.TNo..H....X.Q..v.X.e{..T..i.n.e{..w..u(.w.0|6.2s.K#.?.'r....".X.S...J:...v..A.P.c;>...1..;.lLc.d.m....d.H....2.M..x.7|..C.{.<.e8a{.n...P.+.ZJ....zi.....z/...C..?...-..3..cw=a.?.....YJ}> ..XFpQ...n.i..ZJ.Un....D...kZ+C.>6.....gCY.....(....32...I.g.^.MJ0{.L.#...s.F:.;.p]..(.`.....F1%..w...."#.Y].. ..}..T..X.n0..=8.e0N..{0.v_!.#n>.....n.x..u.....R.L..=...y..n.e...|&.Y.. ..g..7...<gN.1Z..:.C..k..".W|)Z...[u.*.Qf.JHq.V.J...GxnA...0..'.v..'....e....c. ...M.`SR.qn.k.....n.Wm.p..&nJb.{....UE.....^.m..?..w..T..#._....g..p.L.....V.H....a..6[.c...8.....x.....6.. =.....J.c..R.7W.....O.....x..x..x..x..x..x..x..|.....Z=..z....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\sigin[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 108 x 32, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	736
Entropy (8bit):	7.584671380578728
Encrypted:	false
SSDEEP:	12:6v/7KF/hTNSsk9V/G4ifz5SwtGfgzKf8v2zbuht0NNCXxT52FBrORsnwClc:N09NG4iL4WGfgqo23v6XRW1CI7lc
MD5:	681B83E88BA6AACCC72705FBF9F2257B
SHA1:	D69957C47026108511225160BE9BD15788D26E14
SHA-256:	F32A760F15530284447282AF5C7D0825BABF8BC4739E073928F6128830819F7A
SHA-512:	393795EAC16AFBEFA38034360C7C886FEA65016A5CEB55E1A91718474B0AE8F3AE7DFC0EA7F6C1C97334C1C6269B702A1C85236A398B78E16D19E696F213521
Malicious:	false
IE Cache URL:	http://https://vetplano.com/bhj/OfficeV4/images/sigin.png

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\sigin[1].png	
Preview:	.PNG.....IHDR...I... .....sRGB.....gAMA.....a.....pHYs.....+.....uIDAThC.AK.A...)Th...!...^....x.....S{K.'.O...[.'...K".I.K...Pj.B(T.$...tf..M"....}?.2ofv..?...!.z...;.+0A.c....."..3D0f.`....1....Z..M..!g_U.p.....X..aX...Y.+../K.91l9{.....h..>...;...".P..V..*.">Cv....8.$.V.8.%.v..bJ...Sw:c..]D:.LcT.6...[.}N.wi....1.t.#....O.a..E.....|...n.p..i....v.3..$.^...|.;-e;s.g..Y.F...c.....u. .L.....1jd.h.w&v6.T.>..A...nXVk|i..{Wx..1.i}a...n.5]ok....<...z..+h..3U=n..OqX.j.....j.....m.x.E..|T.U..LFK0.....:`...of....c.....\_.Kgb.Z.I.C...wu.\.>u.]..z00+....4...7.!.0.2K.XY...O:.Rw...M..7...y...3.FtBb.....3...7....D..e.|....!1x.`....!.1C.c.....".+...|..z.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\ellipsis_grey[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	915
Entropy (8bit):	3.8525277758130154
Encrypted:	false
SSDEEP:	24:t4CvnAVRfFArf1QqCSzGUdiHTVtpRduf1QqCWbVHTVeUV0Uv6f1QqCWbVHTVeUVx:fn1r1QqC4GuiHFXS1QqCWRHQ3V1QqCWz
MD5:	2B5D393DB04A5E6E1F739CB266E65B4C
SHA1:	6A435DF5CAC3D58CCAD655FE022CCF3DD4B9B721
SHA-256:	16C3F6531D0FA5B4D16E82ABF066233B2A9F284C068C663699313C09F5E8D6E6
SHA-512:	3A692635EE8EBD7B15930E78D9E7E808E48C7ED3ED79003B8CA6F9290FA0E2B0FA3573409001489C00FB41D5710E75D17C3C4D65D26F9665849FB7406562A406
Malicious:	false
IE Cache URL:	http://https://vetplano.com/bhj/OfficeV4/images/ellipsis_grey.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16" viewBox="0 0 16 16"><title>assets</title><path fill="#777777" d="M1.143,6.857a1.107,1.107,0,0,1,.446.089,1.164,1.164,0,0,1,.607.607,1.161,1.161,0,0,1,0,.893,1.164,1.164,0,0,1-.607.607,1.107,1.107,0,0,1-.446.089A1.107,1.107,0,0,1,.7,9.054a1.164,1.164,0,0,1-.607-.607,1.161,1.161,0,0,1,0-.893A1.164,1.164,0,0,1,.607.607,1.161,1.161,0,0,1,.7,6.946a1.107,1.107,0,0,1,.446-.089M8,6.857a1.107,1.107,0,0,1,.446.089,1.164,1.164,0,0,1,.607.607,1.161,1.161,0,0,1,0,.893,1.164,1.164,0,0,1-.607.607,1.161,1.161,0,0,1-.446.089,1.164,1.164,0,0,1-.607-.607,1.161,1.161,0,0,1,0-.893,1.164,1.164,0,0,1,.607-.607A1.107,1.107,0,0,1,14.857,6.857Z"/></svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\ellipsis_white[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	915
Entropy (8bit):	3.877322891561989
Encrypted:	false
SSDEEP:	24:t4CvnAVRf83f1QqCSzGUdiHTVtpRduf1QqCWbVHTVeUV0Uv6f1QqCWbVHTVeUV0W:fnL1QqC4GuiHFXS1QqCWRHQ3V1QqCWRV
MD5:	5AC590EE72BFE06A7CECFD75B588AD73
SHA1:	DDA2CB89A241BC424746D8CF2A22A35535094611
SHA-256:	6075736EA9C281D69C4A3D78FF97BB61B9416A5809919BABE5A0C5596F99AAEA
SHA-512:	B9135D934B9EA50B51BB0316E383B114C8F24DFE75FEF11DCBD1C96170EA59202F6BAFE11AAF534CC2F4ED334A8EA4DBE96AF2504130896D6203BFD2DA6913F
Malicious:	false
IE Cache URL:	http://https://vetplano.com/bhj/OfficeV4/images/ellipsis_white.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16" viewBox="0 0 16 16"><title>assets</title><path fill="#ffffff" d="M1.143,6.857a1.107,1.107,0,0,1,.446.089,1.164,1.164,0,0,1,.607.607,1.161,1.161,0,0,1,0,.893,1.164,1.164,0,0,1-.607.607,1.107,1.107,0,0,1-.446.089A1.107,1.107,0,0,1,.7,9.054a1.164,1.164,0,0,1-.607-.607,1.161,1.161,0,0,1,0-.893A1.164,1.164,0,0,1,.607.607,1.161,1.161,0,0,1,.7,6.946a1.107,1.107,0,0,1,.446-.089M8,6.857a1.107,1.107,0,0,1,.446.089,1.164,1.164,0,0,1,.607.607,1.161,1.161,0,0,1,0,.893,1.164,1.164,0,0,1-.607.607,1.161,1.161,0,0,1-.446.089,1.164,1.164,0,0,1-.607-.607,1.161,1.161,0,0,1,0-.893,1.164,1.164,0,0,1,.607-.607A1.107,1.107,0,0,1,14.857,6.857Z"/></svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\enterpass[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 170 x 29, 8-bit/color RGB, non-interlaced
Category:	downloaded
Size (bytes):	1446
Entropy (8bit):	7.796535000569005
Encrypted:	false
SSDEEP:	24:5CytrnsaVZjZ6+qQALzcF6zSyf/UTR8F2DFHTT6bFol73+M2XdU4:5HQaVZ/qQ7Quyf/UVIb+J3+MqU4
MD5:	BD6E291A9A3CC17ED37605E4FF0010CC
SHA1:	6C1EFD74231E3D253E0F51E4656ECED2F3335D71
SHA-256:	706DE242E7C3CFC4B16BA8174723F26FB80566C3171E9E795F057476011A5DE1
SHA-512:	D940D950167404FE53BD6A7AABAAA8C57AC58878AAD045B9F09B1FA331743A8DB5ECA2568F7E1C3D92EDA4C3AC8F1BE11240917102862F65BB0372EE1D82B33
Malicious:	false
IE Cache URL:	http://https://vetplano.com/bhj/OfficeV4/images/enterpass.png

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\enterpass[1].png	
Preview:	.PNG.....IHDR.....`.....sRGB.....gAMA.....a.....pHYs.....o.d...;IDAThC.Y/..<.~?..T..U..B..PU(T?...U.Z.BUUU..PU.I23.@`.z....n.f&.?....+..U.Ec...X._.....E..... o...2.Y.Gw9.Y.....+.5....np..a...X._4~_~i...E....`..k...)....z>$..?....~. =.b.F.....8.k..X.....k.".#3.....8D5&N.V.....m.Q..7h.S.rhp...t.`.....0.L.q...9|JO.pp.Nzl...X..i...C..L..R..D..... 2.n..6.....\.F.....o....9..8.ZJ...S...K..5...yz.6.FF.45q.X..?.....E/..Z...;.....A.7.^/..Y...S....4.....nE".B.....gA..(r..@N.6!>...).g..;mu....9..3.`....G. .i.ak.}`(D.!.4.g.OLb..{..#.. .e.....%.s....O.....Y..<li.Dd.=...a..Y.5.x.;l..J.....[Pp...:.Yhc?..U...9.aD./:.\@w.x..4=....8.}s0L|"..O.UB....ls3E.fT3.. X0+..7.....[.@.....|i..:.yF....E..O-...Z.....:>..s.VO.83.t+.(!..b<.q B1I...p...\mo.....)..)O~..?..U.E..`o...lvE}..tU",...V.v).....K..S.x.....tL.3..k!..u+.....k.C....S{.N`._.%./..r#.}._.N.N.]`.|..j..O.qV.a.....V.....03.....k..T:a...;...&. =G..qkr.<..&..`.c'.Pk..''o

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\firstmsg1[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 353 x 41, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	3372
Entropy (8bit):	7.90561780402093
Encrypted:	false
SSDEEP:	48:akK0iImj1oaWNTm9Nu4Und08QwVu4IrwfrRUN1t4VQ5sjSPJEGNjqLNecGyuSWn9:LRbSVWN6GCwVwikjsa1MctS41FXi4
MD5:	B7EA3983E3C2D7E5F61B8D1B42758189
SHA1:	FE0817947CA4BC53152ED9378470675D9AF189FD
SHA-256:	7B6CF23AC2454B039DDF4F51B7074636ED5B08B6A1D254A47430C4ACE2A3569D
SHA-512:	6B8CD1CD56B4FF84FCAC4F605558AE32B5EF713CFA42EEDE35B7EA0E0737C53B084FB308185422D3515C4C1BD6B5A6426A65BB0D66DEC54B4AB3F018DDBB7FB7
Malicious:	false
IE Cache URL:	http://https://vetplano.com/bhj/OfficeV4/images/firstmsg1.png
Preview:	.PNG.....IHDR...a...).....b....sRGB.....gAMA.....a.....pHYs.....+.....IDATx^.=R#=..{.;.m..K.....p..~....3..-.09.M.h..!x.[.L.F.....Ty.{F?.....a.....7..0...a.0.-bF.0.c.....N. .`O..+.....{S...9.~s.7k....6N.....N.o..x..1...../.m.5.s.t.....>._...n.?](=.....O....}}..N.....s}.....,o..Ml...g.....Ox.....4.....-I.{...j.>.S~Nsr..=./?..%V.....u^..,T...l..?.._G.m..R. ....@Z..%.V.H.Z.=u:Yf...a.. .Z.O..^.....*j..}..._^.W..J...d...$...a..!...d.[dZO...NB..d.u]2rp.j..]....;)..#..s.].<.>Y.....R.&..l].W..d.0?...6.*..n..X..#..^r.T]N.yj~|..n..Q.....E>.8.....,.... k.wMb.....(-Q\.h..c.....:R.A?.k....z...B...u.*M.....b^.:.t.....C.....oA.....>V..Bu....g..}].r....nD....~.#!.....mC.<.t..E.....T.7.ma&<..`.....4.G.....a...sx...-,...;%..g.x. ..7.s....FKx...wb....T...t9..B.y6^..T....Q.....q...../@....`6..H..c8....Q...Og#U/....G.0Z>.S_I.k....Z..0.X.....2.....0Y.u }.7.Fb.=8<t+...

C:\Users\user\AppData\Local\Temp\~DF20FC4EA39C107E96.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.4725226079283373
Encrypted:	false
SSDEEP:	12:c9lCg5/9lCgeK9l26an9l26an9l8fR1F9l8fRv9lTq1EESjt:c9lLh9lLh9lIn9lIn9lov9lov9lW1Ex5
MD5:	579BB30AD59C12773E4BF5C9C3959C4B
SHA1:	D2FCE93AFC8EAA8129BAB09E1057D24625E63F87
SHA-256:	DD00EB3899EEE03C3EC77B3E907D44ED18DA96A65D74AB2FC2B7613EA9544CF4
SHA-512:	0D0AF462C84831B14EB16A23A2F2E9808F4B98DA4B7C93A7DEBCA8F99351A18F17FFEE9A73C2A1DFF3BC1DD3269E4BFAB52C7AA56CF78CA61A4F009B32D5A8A5
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFCE180BCD5C7ADF3A.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.27918767598683664
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laA:kBqoxxJhHWSVSEab
MD5:	AB889A32AB9ACD33E816C2422337C69A
SHA1:	1190C6B34DED2D295827C2A88310D10A8B90B59B
SHA-256:	4D6EC54B8D244E63B0F04FBE2B97402A3DF722560AD12F218665BA440F4CEFDA
SHA-512:	BD250855747BB4CEC61814D0E44F810156D390E3E9F120A12935EFDF80ACA33C4777AD66257CCA4E4003FEF0741692894980B9298F01C4CDD2D8A9C7BB522FB
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFF0FCE8FDE9A2DE4D.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe

C:\Users\user\AppData\Local\Temp\~DFF0FCE8FDE9A2DE4D.TMP	
File Type:	data
Category:	dropped
Size (bytes):	39177
Entropy (8bit):	0.4441372376069725
Encrypted:	false
SSDEEP:	48:kBqoxKAuvScS+d5N/2SIS/c6r7c6rKcQZymEQwTMTICn:kBqoxKAuvScS+d5N/2dGp/pOEQuMcC
MD5:	55CE9EBABB7094DE340175A06091128A
SHA1:	15DD7D88E75F97880541BA9298F2E6CC38ECCF7C
SHA-256:	968FA8DA79BFDD306262710BE2781155D7BEDB3E31E12C2038E9A56760C0E907
SHA-512:	2A489F1BFA7B3C3D9DED00CB9D076AFAC5900D5F6B11C84C7A2FDE2524A4C2B9CFDAD4BF239B53A4DCD56C1A62D361C3BFDCB0FF686897CB72705AB019931EC
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

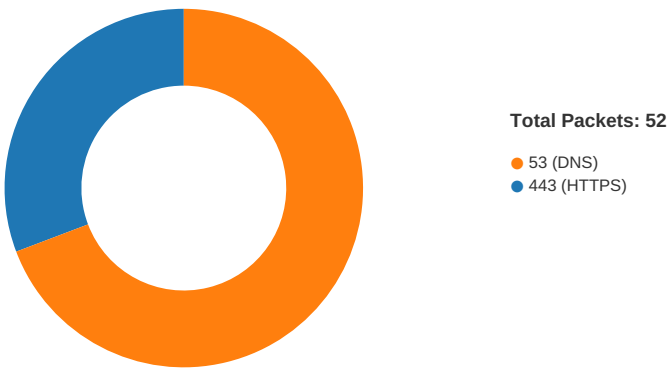
Static File Info

General

File type:	HTML document, ASCII text, with CRLF line terminators
Entropy (8bit):	4.894824690490697
TrID:	• HyperText Markup Language (31031/1) 100.00%
File name:	Payment Report.html
File size:	119
MD5:	00b8795cb028a9c742fc1c6394076d18
SHA1:	4dff056dc7d685775a61e8067b50e47d824d1843
SHA256:	89901d174c786d402fd36cd6d86c1acb3f25f249773b1a81ff230daea30d555c
SHA512:	f5f3b03294437118fb07243b649143de96ba656bd11adc70e1f9e875bd9de6ff875654f6ad0c6818d5537309003515ad675cba74460f6f9ad2d9e605e090de8e
SSDEEP:	3:gnkAqRAdu6/GY7voOkADFqT+GcJcXCEX2k7Mv:7AqJm7+mkqnQCEX2gMv
File Content Preview:	<script type="text/javascript">window.location.href ="https://vetplano.com/bhj/OfficeV4/jma@tullysugar.com";</script>..

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 02:54:09.431755066 CEST	49710	443	192.168.2.4	192.185.195.15
Apr 8, 2021 02:54:09.431812048 CEST	49709	443	192.168.2.4	192.185.195.15
Apr 8, 2021 02:54:09.572468042 CEST	443	49709	192.185.195.15	192.168.2.4
Apr 8, 2021 02:54:09.572736025 CEST	49709	443	192.168.2.4	192.185.195.15
Apr 8, 2021 02:54:09.575337887 CEST	443	49710	192.185.195.15	192.168.2.4
Apr 8, 2021 02:54:09.575561047 CEST	49710	443	192.168.2.4	192.185.195.15
Apr 8, 2021 02:54:09.582647085 CEST	49709	443	192.168.2.4	192.185.195.15
Apr 8, 2021 02:54:09.582747936 CEST	49710	443	192.168.2.4	192.185.195.15
Apr 8, 2021 02:54:09.723562002 CEST	443	49709	192.185.195.15	192.168.2.4
Apr 8, 2021 02:54:09.725843906 CEST	443	49709	192.185.195.15	192.168.2.4
Apr 8, 2021 02:54:09.725931883 CEST	443	49709	192.185.195.15	192.168.2.4
Apr 8, 2021 02:54:09.726007938 CEST	443	49709	192.185.195.15	192.168.2.4
Apr 8, 2021 02:54:09.726078987 CEST	49709	443	192.168.2.4	192.185.195.15
Apr 8, 2021 02:54:09.726147890 CEST	49709	443	192.168.2.4	192.185.195.15
Apr 8, 2021 02:54:09.726155043 CEST	49709	443	192.168.2.4	192.185.195.15
Apr 8, 2021 02:54:09.726572990 CEST	443	49710	192.185.195.15	192.168.2.4
Apr 8, 2021 02:54:09.729939938 CEST	443	49710	192.185.195.15	192.168.2.4
Apr 8, 2021 02:54:09.729981899 CEST	443	49710	192.185.195.15	192.168.2.4
Apr 8, 2021 02:54:09.730010986 CEST	443	49710	192.185.195.15	192.168.2.4
Apr 8, 2021 02:54:09.730014086 CEST	49710	443	192.168.2.4	192.185.195.15
Apr 8, 2021 02:54:09.730040073 CEST	49710	443	192.168.2.4	192.185.195.15
Apr 8, 2021 02:54:09.730082035 CEST	49710	443	192.168.2.4	192.185.195.15
Apr 8, 2021 02:54:09.759074926 CEST	49710	443	192.168.2.4	192.185.195.15
Apr 8, 2021 02:54:09.759202957 CEST	49709	443	192.168.2.4	192.185.195.15
Apr 8, 2021 02:54:09.764760017 CEST	49710	443	192.168.2.4	192.185.195.15
Apr 8, 2021 02:54:09.764914989 CEST	49709	443	192.168.2.4	192.185.195.15
Apr 8, 2021 02:54:09.764929056 CEST	49710	443	192.168.2.4	192.185.195.15
Apr 8, 2021 02:54:09.899859905 CEST	443	49709	192.185.195.15	192.168.2.4
Apr 8, 2021 02:54:09.899905920 CEST	443	49709	192.185.195.15	192.168.2.4
Apr 8, 2021 02:54:09.900131941 CEST	49709	443	192.168.2.4	192.185.195.15
Apr 8, 2021 02:54:09.901921034 CEST	49709	443	192.168.2.4	192.185.195.15
Apr 8, 2021 02:54:09.902925968 CEST	443	49710	192.185.195.15	192.168.2.4
Apr 8, 2021 02:54:09.902959108 CEST	443	49710	192.185.195.15	192.168.2.4
Apr 8, 2021 02:54:09.903094053 CEST	49710	443	192.168.2.4	192.185.195.15
Apr 8, 2021 02:54:09.903896093 CEST	49710	443	192.168.2.4	192.185.195.15
Apr 8, 2021 02:54:09.905011892 CEST	443	49709	192.185.195.15	192.168.2.4
Apr 8, 2021 02:54:09.905124903 CEST	49709	443	192.168.2.4	192.185.195.15
Apr 8, 2021 02:54:09.907577991 CEST	443	49710	192.185.195.15	192.168.2.4
Apr 8, 2021 02:54:09.907867908 CEST	443	49710	192.185.195.15	192.168.2.4
Apr 8, 2021 02:54:09.907942057 CEST	49710	443	192.168.2.4	192.185.195.15
Apr 8, 2021 02:54:10.083803892 CEST	443	49709	192.185.195.15	192.168.2.4
Apr 8, 2021 02:54:10.088649988 CEST	443	49710	192.185.195.15	192.168.2.4
Apr 8, 2021 02:54:12.021650076 CEST	443	49710	192.185.195.15	192.168.2.4
Apr 8, 2021 02:54:12.021698952 CEST	443	49710	192.185.195.15	192.168.2.4
Apr 8, 2021 02:54:12.021723032 CEST	49710	443	192.168.2.4	192.185.195.15
Apr 8, 2021 02:54:12.021738052 CEST	443	49710	192.185.195.15	192.168.2.4
Apr 8, 2021 02:54:12.021759987 CEST	49710	443	192.168.2.4	192.185.195.15
Apr 8, 2021 02:54:12.021776915 CEST	443	49710	192.185.195.15	192.168.2.4
Apr 8, 2021 02:54:12.021785021 CEST	49710	443	192.168.2.4	192.185.195.15
Apr 8, 2021 02:54:12.021821976 CEST	49710	443	192.168.2.4	192.185.195.15
Apr 8, 2021 02:54:12.021825075 CEST	443	49710	192.185.195.15	192.168.2.4
Apr 8, 2021 02:54:12.021861076 CEST	443	49710	192.185.195.15	192.168.2.4
Apr 8, 2021 02:54:12.021876097 CEST	49710	443	192.168.2.4	192.185.195.15
Apr 8, 2021 02:54:12.021917105 CEST	49710	443	192.168.2.4	192.185.195.15
Apr 8, 2021 02:54:12.024094105 CEST	49710	443	192.168.2.4	192.185.195.15
Apr 8, 2021 02:54:12.167038918 CEST	443	49710	192.185.195.15	192.168.2.4
Apr 8, 2021 02:54:12.618088961 CEST	443	49710	192.185.195.15	192.168.2.4
Apr 8, 2021 02:54:12.618140936 CEST	443	49710	192.185.195.15	192.168.2.4
Apr 8, 2021 02:54:12.618180037 CEST	443	49710	192.185.195.15	192.168.2.4
Apr 8, 2021 02:54:12.618205070 CEST	49710	443	192.168.2.4	192.185.195.15
Apr 8, 2021 02:54:12.618221045 CEST	443	49710	192.185.195.15	192.168.2.4
Apr 8, 2021 02:54:12.618261099 CEST	443	49710	192.185.195.15	192.168.2.4
Apr 8, 2021 02:54:12.618269920 CEST	49710	443	192.168.2.4	192.185.195.15
Apr 8, 2021 02:54:12.618293047 CEST	443	49710	192.185.195.15	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 02:54:12.618365049 CEST	49710	443	192.168.2.4	192.185.195.15
Apr 8, 2021 02:54:12.642373085 CEST	49710	443	192.168.2.4	192.185.195.15
Apr 8, 2021 02:54:12.650672913 CEST	49710	443	192.168.2.4	192.185.195.15
Apr 8, 2021 02:54:12.652458906 CEST	49710	443	192.168.2.4	192.185.195.15
Apr 8, 2021 02:54:12.653031111 CEST	49710	443	192.168.2.4	192.185.195.15
Apr 8, 2021 02:54:12.653702974 CEST	49710	443	192.168.2.4	192.185.195.15
Apr 8, 2021 02:54:12.654306889 CEST	49710	443	192.168.2.4	192.185.195.15
Apr 8, 2021 02:54:12.654777050 CEST	49710	443	192.168.2.4	192.185.195.15
Apr 8, 2021 02:54:12.706254959 CEST	49711	443	192.168.2.4	13.32.25.43
Apr 8, 2021 02:54:12.706274986 CEST	49712	443	192.168.2.4	13.32.25.43
Apr 8, 2021 02:54:12.723830938 CEST	443	49711	13.32.25.43	192.168.2.4
Apr 8, 2021 02:54:12.723876953 CEST	443	49712	13.32.25.43	192.168.2.4
Apr 8, 2021 02:54:12.723923922 CEST	49711	443	192.168.2.4	13.32.25.43
Apr 8, 2021 02:54:12.723958015 CEST	49712	443	192.168.2.4	13.32.25.43
Apr 8, 2021 02:54:12.725016117 CEST	49711	443	192.168.2.4	13.32.25.43
Apr 8, 2021 02:54:12.725183964 CEST	49712	443	192.168.2.4	13.32.25.43
Apr 8, 2021 02:54:12.742701054 CEST	443	49711	13.32.25.43	192.168.2.4
Apr 8, 2021 02:54:12.742743015 CEST	443	49712	13.32.25.43	192.168.2.4
Apr 8, 2021 02:54:12.742784023 CEST	443	49711	13.32.25.43	192.168.2.4
Apr 8, 2021 02:54:12.742820978 CEST	443	49711	13.32.25.43	192.168.2.4
Apr 8, 2021 02:54:12.742860079 CEST	49711	443	192.168.2.4	13.32.25.43
Apr 8, 2021 02:54:12.742882013 CEST	49711	443	192.168.2.4	13.32.25.43
Apr 8, 2021 02:54:12.742911100 CEST	443	49711	13.32.25.43	192.168.2.4
Apr 8, 2021 02:54:12.742955923 CEST	443	49712	13.32.25.43	192.168.2.4
Apr 8, 2021 02:54:12.742974997 CEST	49711	443	192.168.2.4	13.32.25.43
Apr 8, 2021 02:54:12.743015051 CEST	443	49712	13.32.25.43	192.168.2.4
Apr 8, 2021 02:54:12.743048906 CEST	49712	443	192.168.2.4	13.32.25.43
Apr 8, 2021 02:54:12.743053913 CEST	443	49712	13.32.25.43	192.168.2.4
Apr 8, 2021 02:54:12.743088961 CEST	49712	443	192.168.2.4	13.32.25.43
Apr 8, 2021 02:54:12.743103981 CEST	49712	443	192.168.2.4	13.32.25.43
Apr 8, 2021 02:54:12.744549990 CEST	443	49712	13.32.25.43	192.168.2.4
Apr 8, 2021 02:54:12.744591951 CEST	443	49711	13.32.25.43	192.168.2.4
Apr 8, 2021 02:54:12.744637012 CEST	49712	443	192.168.2.4	13.32.25.43
Apr 8, 2021 02:54:12.744653940 CEST	49711	443	192.168.2.4	13.32.25.43
Apr 8, 2021 02:54:12.755196095 CEST	49712	443	192.168.2.4	13.32.25.43
Apr 8, 2021 02:54:12.755222082 CEST	49711	443	192.168.2.4	13.32.25.43

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 02:54:08.135896921 CEST	65195	53	192.168.2.4	8.8.8.8
Apr 8, 2021 02:54:08.155268908 CEST	53	65195	8.8.8.8	192.168.2.4
Apr 8, 2021 02:54:09.377226114 CEST	59042	53	192.168.2.4	8.8.8.8
Apr 8, 2021 02:54:09.416199923 CEST	53	59042	8.8.8.8	192.168.2.4
Apr 8, 2021 02:54:12.652861118 CEST	56483	53	192.168.2.4	8.8.8.8
Apr 8, 2021 02:54:12.668771029 CEST	53	56483	8.8.8.8	192.168.2.4
Apr 8, 2021 02:54:18.480206013 CEST	51025	53	192.168.2.4	8.8.8.8
Apr 8, 2021 02:54:18.492789984 CEST	53	51025	8.8.8.8	192.168.2.4
Apr 8, 2021 02:54:19.477955103 CEST	61516	53	192.168.2.4	8.8.8.8
Apr 8, 2021 02:54:19.491672039 CEST	53	61516	8.8.8.8	192.168.2.4
Apr 8, 2021 02:54:20.742645979 CEST	49182	53	192.168.2.4	8.8.8.8
Apr 8, 2021 02:54:20.755881071 CEST	53	49182	8.8.8.8	192.168.2.4
Apr 8, 2021 02:54:21.989634991 CEST	59920	53	192.168.2.4	8.8.8.8
Apr 8, 2021 02:54:22.002552986 CEST	53	59920	8.8.8.8	192.168.2.4
Apr 8, 2021 02:54:23.417186022 CEST	57458	53	192.168.2.4	8.8.8.8
Apr 8, 2021 02:54:23.430715084 CEST	53	57458	8.8.8.8	192.168.2.4
Apr 8, 2021 02:54:25.395915985 CEST	50579	53	192.168.2.4	8.8.8.8
Apr 8, 2021 02:54:25.421710968 CEST	53	50579	8.8.8.8	192.168.2.4
Apr 8, 2021 02:54:26.947426081 CEST	51703	53	192.168.2.4	8.8.8.8
Apr 8, 2021 02:54:26.959750891 CEST	53	51703	8.8.8.8	192.168.2.4
Apr 8, 2021 02:54:27.902379990 CEST	65248	53	192.168.2.4	8.8.8.8
Apr 8, 2021 02:54:27.915177107 CEST	53	65248	8.8.8.8	192.168.2.4
Apr 8, 2021 02:54:30.204446077 CEST	53723	53	192.168.2.4	8.8.8.8
Apr 8, 2021 02:54:30.217848063 CEST	53	53723	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 02:54:31.549846888 CEST	64646	53	192.168.2.4	8.8.8.8
Apr 8, 2021 02:54:31.563515902 CEST	53	64646	8.8.8.8	192.168.2.4
Apr 8, 2021 02:54:32.869395971 CEST	65298	53	192.168.2.4	8.8.8.8
Apr 8, 2021 02:54:32.882663965 CEST	53	65298	8.8.8.8	192.168.2.4
Apr 8, 2021 02:54:34.143342972 CEST	59123	53	192.168.2.4	8.8.8.8
Apr 8, 2021 02:54:34.155826092 CEST	53	59123	8.8.8.8	192.168.2.4
Apr 8, 2021 02:54:35.352252960 CEST	54531	53	192.168.2.4	8.8.8.8
Apr 8, 2021 02:54:35.365058899 CEST	53	54531	8.8.8.8	192.168.2.4
Apr 8, 2021 02:54:38.149477005 CEST	49714	53	192.168.2.4	8.8.8.8
Apr 8, 2021 02:54:38.161897898 CEST	53	49714	8.8.8.8	192.168.2.4
Apr 8, 2021 02:54:38.689912081 CEST	58028	53	192.168.2.4	8.8.8.8
Apr 8, 2021 02:54:38.703174114 CEST	53	58028	8.8.8.8	192.168.2.4
Apr 8, 2021 02:54:38.812633991 CEST	53097	53	192.168.2.4	8.8.8.8
Apr 8, 2021 02:54:38.825975895 CEST	53	53097	8.8.8.8	192.168.2.4
Apr 8, 2021 02:54:39.176177025 CEST	49714	53	192.168.2.4	8.8.8.8
Apr 8, 2021 02:54:39.189470053 CEST	53	49714	8.8.8.8	192.168.2.4
Apr 8, 2021 02:54:39.779470921 CEST	49257	53	192.168.2.4	8.8.8.8
Apr 8, 2021 02:54:39.792664051 CEST	53	49257	8.8.8.8	192.168.2.4
Apr 8, 2021 02:54:39.820843935 CEST	53097	53	192.168.2.4	8.8.8.8
Apr 8, 2021 02:54:39.834328890 CEST	53	53097	8.8.8.8	192.168.2.4
Apr 8, 2021 02:54:40.284782887 CEST	49714	53	192.168.2.4	8.8.8.8
Apr 8, 2021 02:54:40.298157930 CEST	53	49714	8.8.8.8	192.168.2.4
Apr 8, 2021 02:54:41.070004940 CEST	53097	53	192.168.2.4	8.8.8.8
Apr 8, 2021 02:54:41.082653999 CEST	53	53097	8.8.8.8	192.168.2.4
Apr 8, 2021 02:54:41.562659979 CEST	62389	53	192.168.2.4	8.8.8.8
Apr 8, 2021 02:54:41.575057030 CEST	53	62389	8.8.8.8	192.168.2.4
Apr 8, 2021 02:54:42.274288893 CEST	49714	53	192.168.2.4	8.8.8.8
Apr 8, 2021 02:54:42.287309885 CEST	53	49714	8.8.8.8	192.168.2.4
Apr 8, 2021 02:54:43.055491924 CEST	53097	53	192.168.2.4	8.8.8.8
Apr 8, 2021 02:54:43.068723917 CEST	53	53097	8.8.8.8	192.168.2.4
Apr 8, 2021 02:54:46.290366888 CEST	49714	53	192.168.2.4	8.8.8.8
Apr 8, 2021 02:54:46.303070068 CEST	53	49714	8.8.8.8	192.168.2.4
Apr 8, 2021 02:54:47.056406975 CEST	53097	53	192.168.2.4	8.8.8.8
Apr 8, 2021 02:54:47.070516109 CEST	53	53097	8.8.8.8	192.168.2.4
Apr 8, 2021 02:54:57.938244104 CEST	49910	53	192.168.2.4	8.8.8.8
Apr 8, 2021 02:54:57.956238031 CEST	53	49910	8.8.8.8	192.168.2.4
Apr 8, 2021 02:55:14.934590101 CEST	55854	53	192.168.2.4	8.8.8.8
Apr 8, 2021 02:55:14.947097063 CEST	53	55854	8.8.8.8	192.168.2.4
Apr 8, 2021 02:55:16.711055994 CEST	64549	53	192.168.2.4	8.8.8.8
Apr 8, 2021 02:55:16.723630905 CEST	53	64549	8.8.8.8	192.168.2.4
Apr 8, 2021 02:55:17.954253912 CEST	63153	53	192.168.2.4	8.8.8.8
Apr 8, 2021 02:55:17.967612982 CEST	53	63153	8.8.8.8	192.168.2.4
Apr 8, 2021 02:55:19.124948025 CEST	52991	53	192.168.2.4	8.8.8.8
Apr 8, 2021 02:55:19.138056040 CEST	53	52991	8.8.8.8	192.168.2.4
Apr 8, 2021 02:55:20.580780983 CEST	53700	53	192.168.2.4	8.8.8.8
Apr 8, 2021 02:55:20.593812943 CEST	53	53700	8.8.8.8	192.168.2.4
Apr 8, 2021 02:55:22.274555922 CEST	51726	53	192.168.2.4	8.8.8.8
Apr 8, 2021 02:55:22.288059950 CEST	53	51726	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 8, 2021 02:54:09.377226114 CEST	192.168.2.4	8.8.8.8	0x4f5	Standard query (0)	vetplano.com	A (IP address)	IN (0x0001)
Apr 8, 2021 02:54:12.652861118 CEST	192.168.2.4	8.8.8.8	0x4a2	Standard query (0)	logo.clearbit.com	A (IP address)	IN (0x0001)
Apr 8, 2021 02:54:25.395915985 CEST	192.168.2.4	8.8.8.8	0x42b6	Standard query (0)	vetplano.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 8, 2021 02:54:09.416199923 CEST	8.8.8.8	192.168.2.4	0x4f5	No error (0)	vetplano.com		192.185.195.15	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 8, 2021 02:54:12.668771029 CEST	8.8.8.8	192.168.2.4	0x4a2	No error (0)	logo.clearbit.com	d26p066pn2w0s0.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 02:54:12.668771029 CEST	8.8.8.8	192.168.2.4	0x4a2	No error (0)	d26p066pn2w0s0.cloudfront.net		13.32.25.43	A (IP address)	IN (0x0001)
Apr 8, 2021 02:54:12.668771029 CEST	8.8.8.8	192.168.2.4	0x4a2	No error (0)	d26p066pn2w0s0.cloudfront.net		13.32.25.60	A (IP address)	IN (0x0001)
Apr 8, 2021 02:54:12.668771029 CEST	8.8.8.8	192.168.2.4	0x4a2	No error (0)	d26p066pn2w0s0.cloudfront.net		13.32.25.101	A (IP address)	IN (0x0001)
Apr 8, 2021 02:54:12.668771029 CEST	8.8.8.8	192.168.2.4	0x4a2	No error (0)	d26p066pn2w0s0.cloudfront.net		13.32.25.80	A (IP address)	IN (0x0001)
Apr 8, 2021 02:54:25.421710968 CEST	8.8.8.8	192.168.2.4	0x42b6	No error (0)	vetplano.com		192.185.195.15	A (IP address)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 8, 2021 02:54:09.726007938 CEST	192.185.195.15	443	192.168.2.4	49709	CN=cpcalendars.vetplano.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Tue Mar 09 08:44:11 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Mon Jun 07 09:44:11 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Apr 8, 2021 02:54:09.730010986 CEST	192.185.195.15	443	192.168.2.4	49710	CN=cpcalendars.vetplano.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Tue Mar 09 08:44:11 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Mon Jun 07 09:44:11 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Apr 8, 2021 02:54:12.744549990 CEST	13.32.25.43	443	192.168.2.4	49712	CN=clearbit.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed May 20 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Sun Jun 20 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	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=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Apr 8, 2021 02:54:12.744591951 CEST	13.32.25.43	443	192.168.2.4	49711	CN=clearbit.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed May 20 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Sun Jun 20 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	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=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Apr 8, 2021 02:54:25.740557909 CEST	192.185.195.15	443	192.168.2.4	49718	CN=cpcalendars.vetplano.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Tue Mar 09 08:44:11 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Mon Jun 07 09:44:11 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		

Code Manipulations

Statistics

Behavior

● iexplore.exe
● iexplore.exe

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 5764 Parent PID: 800

General

Start time:	02:54:06
Start date:	08/04/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff7f2920000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: iexplore.exe PID: 5820 Parent PID: 5764

General

Start time:	02:54:07

Start date:	08/04/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5764 CREDAT:17410 /prefetch:2
Imagebase:	0x970000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly