ID: 356325
Sample Name:
smartandfinalTicket#51347303511505986.htm
Cookbook:
defaultwindowshtmlcookbook.jbs
Time: 22:46:52
Date: 22/02/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2
Analysis Report smartandfinalTicket#51347303511505986.htm 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Yara Overview 4
Dropped Files 4
Sigma Overview 4
Signature Overview 4
AV Detection: 5
Phishing: 5
Compliance: 5
Mitre Att&ck Matrix 5
Behavior Graph 5
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 7
URLs 7
Domains and IPs 8
Contacted Domains 8
Contacted URLs 8
URLs from Memory and Binaries 8
Contacted IPs 9
Public 9
Private 9
General Information 9
Simulations 10
Behavior and APIs 10
Joe Sandbox View / Context 11
IPs 11
Domains 11
ASN 11
JA3 Fingerprints 12
Dropped Files 13
Created / dropped Files 13
Static File Info 23
General 23
Network Behavior 23
Network Port Distribution 23
TCP Packets 23
UDP Packets 25
DNS Queries 27
DNS Answers 27
HTTPS Packets 27
Code Manipulations 29
Statistics 29
Behavior 29

System Behavior 29
Analysis Process: iexplore.exe PID: 6832 Parent PID: 800 29
General 29
File Activities 30
Registry Activities 30
Analysis Process: iexplore.exe PID: 6924 Parent PID: 6832 30
General 30
File Activities 30
Registry Activities 30
Disassembly 30

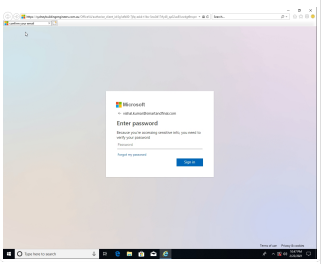
Analysis Report smartandfinalTicket#5134730351150598…

Overview

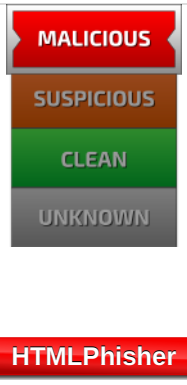
General Information

Sample Name:	smartandfinalTicket#51347303511505986.htm
Analysis ID:	356325
MD5:	5f42d465e7e680e.
SHA1:	843faae5f7d1048..
SHA256:	e4b97c79b4c90c…

Most interesting Screenshot:



Detection



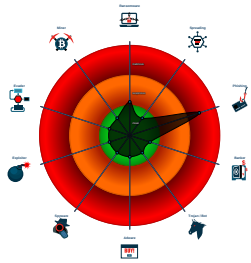
HTMLPhisher

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

Signatures

- Antivirus detection for URL or domain
- Phishing site detected (based on fav…
- Yara detected HtmlPhish_10
- JA3 SSL client fingerprint seen in co…

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 6832 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6924 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6832 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

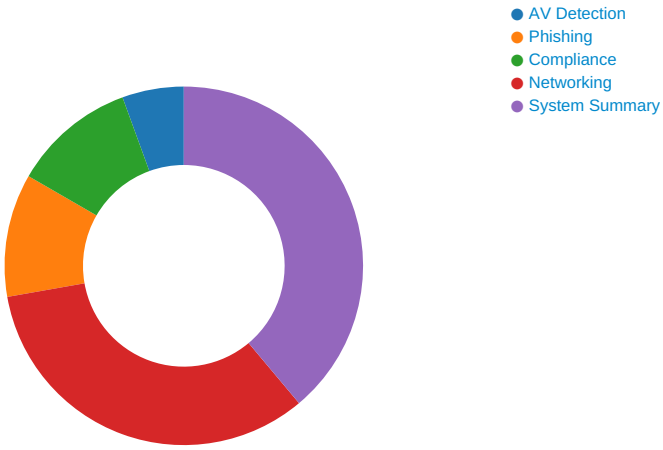
Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\authorize_client_id_5g1afb80-7jfq-ask4-t1bx-5zw0d17rfy48_qa32ux85vsrdgt9ncpmw7ebyo4kz10fjilh6hskufelop5ya3m1i0942tcrv8znqxbwj7gd692ez0tj4dmhkufaqbo7pnvyrxl3568cs1iwg[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 HtmlPhish_10

Compliance:

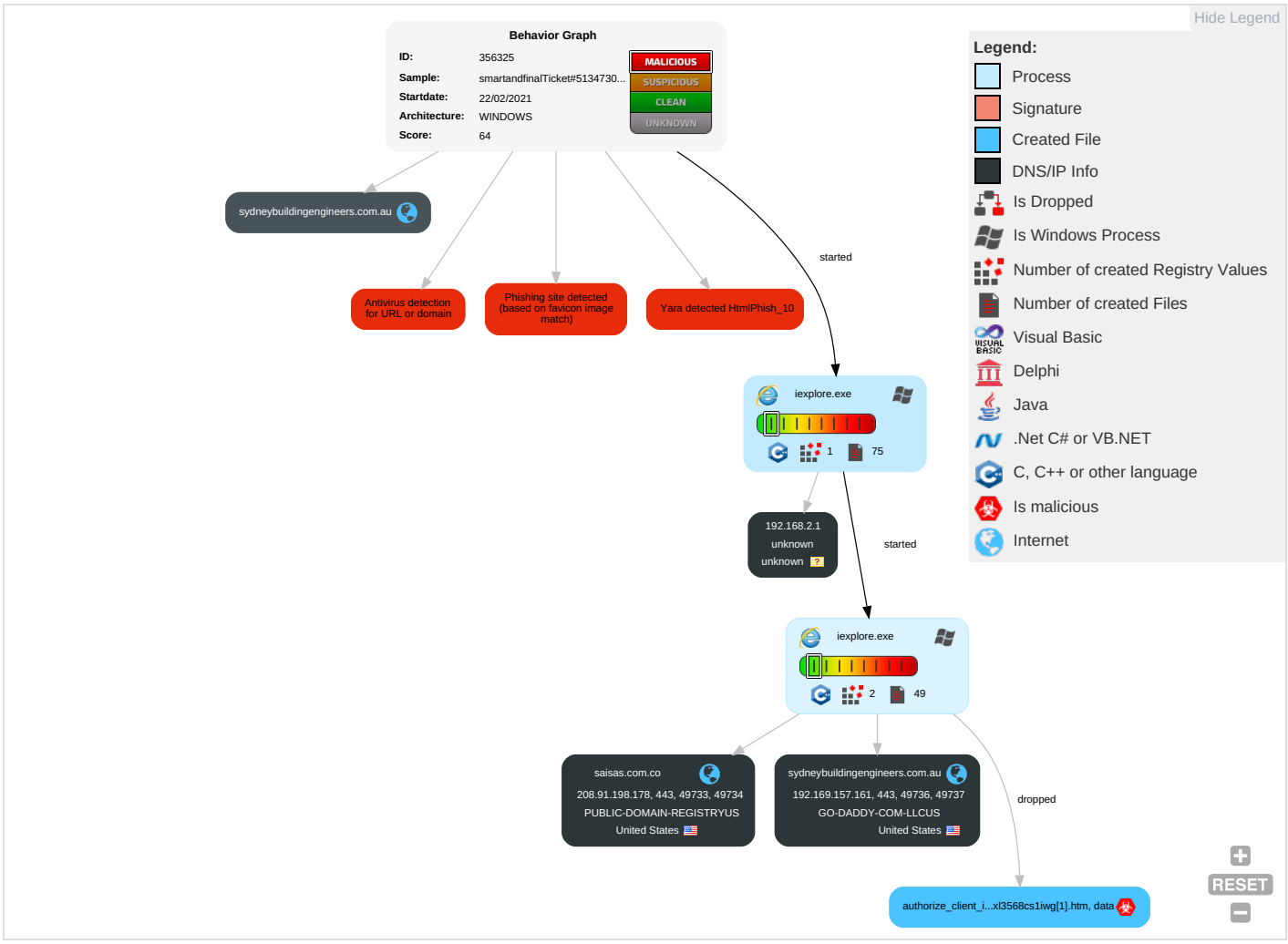
Uses new MSVCR Dlls

Uses secure TLS version for HTTPS connections

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

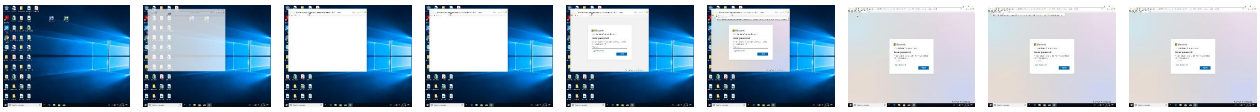
Behavior Graph

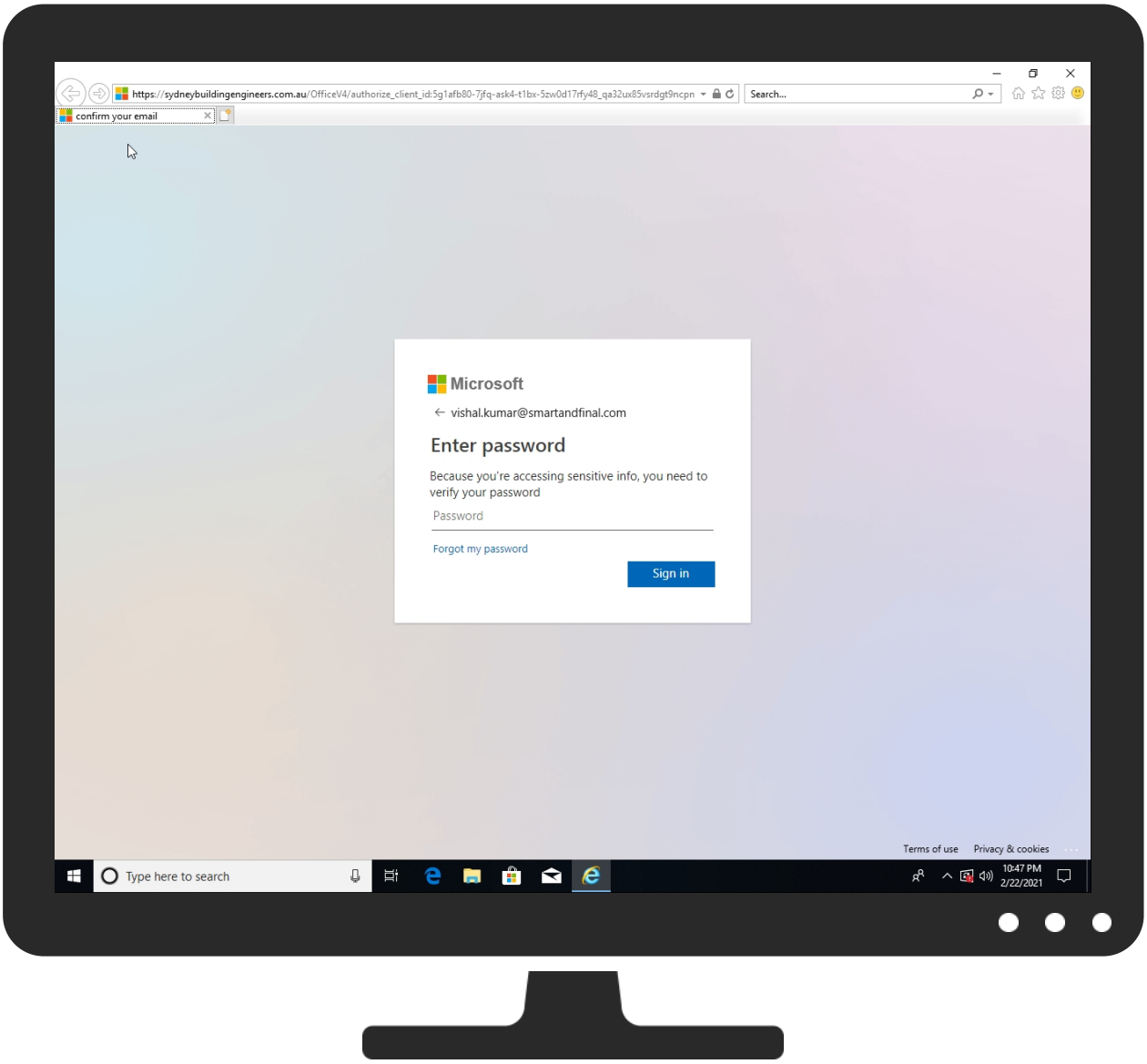


Screenshots

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
smartandfinalTicket#51347303511505986.htm	0%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
saisas.com.co	0%	Virustotal		Browse
sydneybuildingengineers.com.au	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link

Source	Detection	Scanner	Label	Link
http://https://sydneybuildingengineers.com.au/OfficeV4/authorize_client_id:5g1afb80-7jfq-ask4-t1bx-5zw0d17rfy48_qa32ux85vsrdgt9ncpmw7ebyo4kz10fjilh6hskufelop5ya3m1i0942tcrv8znqxbwj7gd692ez0tj4dmhkufaqbo7pnvyrxl3568cs1iwg?data=dmlzaGFsLmt1bWFyQHNtYXJ0YW5kZmluYWwuY29t	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://https://sydneybuildingengineers.com.au/OfficeV4/?/dmlzaGFsLmt1bWFyQHNtYXJ0YW5kZmluYWwuY29t	0%	Avira URL Cloud	safe	
http://https://sydneybuildingexrobotosv4/?vishal.kumar	0%	Avira URL Cloud	safe	
http://https://saisas.com.co//Desktop/smartandfinalTicket#51347303511505986.htmexrobotosv4/?vishal.kumar	0%	Avira URL Cloud	safe	
http://https://saisas.com.co/exrobotosv4/?vishal.kumar	0%	Avira URL Cloud	safe	
http://https://saisas.com.co/exrobotosv4?vishal.kumar	0%	Avira URL Cloud	safe	
http://https://sydneybuildingengineers.com.au/OfficeV4?/dmlzaGFsLmt1bWFyQHNtYXJ0YW5kZmluYWwuY29t	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://https://sydneybuildingengineers.com.au/OfficeV4/authorize_client_id:5g1afb80-7jfq-ask4-t1bx-5zw0d17r	0%	Avira URL Cloud	safe	
http://https://sydneybuildingengineers.com.au/OfficeV4/images/favicon.ico~	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
saisas.com.co	208.91.198.178	true	false	• 0%, Virustotal, Browse	unknown
sydneybuildingengineers.com.au	192.169.157.161	true	false	• 0%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://sydneybuildingengineers.com.au/OfficeV4/authorize_client_id:5g1afb80-7jfq-ask4-t1bx-5zw0d17rfy48_qa32ux85vsrdgt9ncpmw7ebyo4kz10fjilh6hskufelop5ya3m1i0942tcrv8znqxbwj7gd692ez0tj4dmhkufaqbo7pnvyrxl3568cs1iwg?data=dmlzaGFsLmt1bWFyQHNtYXJ0YW5kZmluYWwuY29t	true	• SlashNext: Fake Login Page type: Phishing & Social Engineering	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://sydneybuildingengineers.com.au/OfficeV4/?/dmlzaGFsLmt1bWFyQHNtYXJ0YW5kZmluYWwuY29t	OfficeV4[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://sydneybuildingexrobotosv4/?vishal.kumar	{920BAF37-7557-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false	• Avira URL Cloud: safe	low
http://www.nytimes.com/	msapplication.xml3.1.dr	false		high
http://https://saisas.com.co//Desktop/smartandfinalTicket#51347303511505986.htmexrobotosv4/?vishal.kumar	{920BAF37-7557-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://www.youtube.com/	msapplication.xml7.1.dr	false		high
http://https://saisas.com.co/exrobotosv4/?vishal.kumar	~DF0C840B5320C13C8C.TMP.1.dr, exrobotosv4[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://saisas.com.co/exrobotosv4?vishal.kumar	smartandfinalTicket#5134730351 1505986.htm	false	• Avira URL Cloud: safe	unknown
http://https://sydneybuildingengineers.com.au/OfficeV4?/dmlzaGFsLmt1bWFyQHNtYXJ0YW5kZmluYWwuY29t	exrobotosv4[1].htm0.3.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	unknown
http://www.amazon.com/	msapplication.xml.1.dr	false		high
http://www.live.com/	msapplication.xml2.1.dr	false		high
http://https://sydneybuildingengineers.com.au/OfficeV4/authorize_client_id:5g1afb80-7jfq-ask4-t1bx-5zw0d17r	~DF0C840B5320C13C8C.TMP.1.dr	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

Name	Source	Malicious	Antivirus Detection	Reputation
http:// https://sydneybuildingengineers.com.au/OfficeV4/images/favicon.ico~	imagestore.dat.3.dr	false	• Avira URL Cloud: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
208.91.198.178	unknown	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	false
192.169.157.161	unknown	United States		398101	GO-DADDY-COM-LLCUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	356325
Start date:	22.02.2021
Start time:	22:46:52
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 59s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	smartandfinalTicket#51347303511505986.htm
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:	16

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.winHTM@3/31@3/3
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .htm
Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 204.79.197.200, 13.107.21.200, 52.255.188.83, 13.88.21.125, 13.64.90.137, 88.221.62.148, 104.43.139.144, 51.104.139.180, 152.199.19.161, 52.155.217.156, 20.54.26.129, 93.184.221.240, 92.122.213.194, 92.122.213.247 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, a1449.dscg2.akamai.net, arc.msn.com, wu.azureedge.net, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, go.microsoft.com, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, wu.wpc.apr-52dd2.edgecastdns.net, au-bg-shim.trafficmanager.net, www.bing.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, dual-a-0001.a-msedge.net, ie9comview.vo.msecnd.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, wu.ec.azureedge.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, skypedataprdcolwus15.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net, cs9.wpc.v0cdn.net • 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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PUBLIC-DOMAIN-REGISTRYUS	f4b1bde3-706a-40d2-8ace-693803810b6f.exe	Get hash	malicious	Browse	• 103.53.43.36
	LIQUIDACION INTERBANCARIA 02_22_2021.xls	Get hash	malicious	Browse	• 208.91.199.223
	document-550193913.xls	Get hash	malicious	Browse	• 208.91.199.118
	document-550193913.xls	Get hash	malicious	Browse	• 208.91.199.118
	SecuriteInfo.com.Trojan.Packed2.42850.3598.exe	Get hash	malicious	Browse	• 208.91.199.225
	SecuriteInfo.com.Trojan.Inject4.6572.1879.exe	Get hash	malicious	Browse	• 208.91.199.224
	ffkjg5CVrO.exe	Get hash	malicious	Browse	• 208.91.199.223
	7Lf8J7h7os.exe	Get hash	malicious	Browse	• 208.91.199.223
	Shipping Details_PDF.exe	Get hash	malicious	Browse	• 208.91.198.143
	YKRAB010B_KHE_Preminary Packing List.xlsx.exe	Get hash	malicious	Browse	• 208.91.199.225
	RTM DIAS - CTM.exe	Get hash	malicious	Browse	• 208.91.198.143
	AWB & Shipping Doc.exe	Get hash	malicious	Browse	• 208.91.199.223
	AWB & Shipping Doc.exe	Get hash	malicious	Browse	• 208.91.199.223
	PAYMENT INVOICE-9876543456789.exe	Get hash	malicious	Browse	• 208.91.199.224
	SecuriteInfo.com.Artemis249E62CF9BAE.exe	Get hash	malicious	Browse	• 208.91.198.143
	SecuriteInfo.com.Exploit.Siggen3.10204.3307.xls	Get hash	malicious	Browse	• 103.50.162.157
	document-573042818.xls	Get hash	malicious	Browse	• 103.50.162.157
	document-573042818.xls	Get hash	malicious	Browse	• 103.50.162.157
	document-573042818.xls	Get hash	malicious	Browse	• 103.50.162.157
	document-750895311.xls	Get hash	malicious	Browse	• 103.50.162.157
GO-DADDY-COM-LLCUS	IMG_01670_Scanned.doc	Get hash	malicious	Browse	• 184.168.131.241
	IMG_7742_Scanned.doc	Get hash	malicious	Browse	• 184.168.131.241
	PDF.exe	Get hash	malicious	Browse	• 184.168.131.241
	Statement-ID28865611496334.vbs	Get hash	malicious	Browse	• 107.180.91.179
	Statement-ID21488878391791.vbs	Get hash	malicious	Browse	• 107.180.91.179
	Statement-ID72347595684775.vbs	Get hash	malicious	Browse	• 107.180.91.179
	SOA.exe	Get hash	malicious	Browse	• 184.168.131.241
	YSZiV5Oh2E.exe	Get hash	malicious	Browse	• 184.168.131.241
	Confirmation.exe	Get hash	malicious	Browse	• 184.168.131.241
	Purchase order.exe	Get hash	malicious	Browse	• 184.168.131.241
	Request For Quotation.PDF.exe	Get hash	malicious	Browse	• 184.168.131.241
	IMG_7189012.exe	Get hash	malicious	Browse	• 184.168.131.241
	DHL Shipment Notification 7465649870,pdf.exe	Get hash	malicious	Browse	• 184.168.131.241
	urgent specification request.exe	Get hash	malicious	Browse	• 184.168.131.241
	P.O-48452689535945.exe	Get hash	malicious	Browse	• 107.180.48.248
	Shinshin Machinery.exe	Get hash	malicious	Browse	• 184.168.131.241
	CMahQwuvAE.exe	Get hash	malicious	Browse	• 184.168.131.241
	ForeignRemittance_20210219_USD.xlsx	Get hash	malicious	Browse	• 184.168.131.241
	SHED.EXE	Get hash	malicious	Browse	• 184.168.131.241
	c4p1vG05Z8.exe	Get hash	malicious	Browse	• 184.168.131.241

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
9e10692f1b7f78228b2d4e424db3a98c	rieuro.dll	Get hash	malicious	Browse	• 208.91.198.178 • 192.169.15 7.161
	receipt145.htm	Get hash	malicious	Browse	• 208.91.198.178 • 192.169.15 7.161
	One Note shergott@vivaldicap.com.html	Get hash	malicious	Browse	• 208.91.198.178 • 192.169.15 7.161
	FAX-MESSAGE201636576736375362.hTMl	Get hash	malicious	Browse	• 208.91.198.178 • 192.169.15 7.161
	message_zdm (2).html	Get hash	malicious	Browse	• 208.91.198.178 • 192.169.15 7.161
	Small Charities.xlsx	Get hash	malicious	Browse	• 208.91.198.178 • 192.169.15 7.161
	leaseplan-invoice-831008_xls2.HtMl	Get hash	malicious	Browse	• 208.91.198.178 • 192.169.15 7.161
	7lM8HxwfAm.dll	Get hash	malicious	Browse	• 208.91.198.178 • 192.169.15 7.161
	LcA7GaqAXC.dll	Get hash	malicious	Browse	• 208.91.198.178 • 192.169.15 7.161
	4FHOFKHnX8.dll	Get hash	malicious	Browse	• 208.91.198.178 • 192.169.15 7.161
	5N5yxttthP.dll	Get hash	malicious	Browse	• 208.91.198.178 • 192.169.15 7.161
	vBKmtJ58Eo.dll	Get hash	malicious	Browse	• 208.91.198.178 • 192.169.15 7.161
	5293ea9467ea45e928620a5ed74440f5.exe	Get hash	malicious	Browse	• 208.91.198.178 • 192.169.15 7.161
	f1a14e6352036833f1c109e1bb2934f2.exe	Get hash	malicious	Browse	• 208.91.198.178 • 192.169.15 7.161
	Njs4kjnD5X.dll	Get hash	malicious	Browse	• 208.91.198.178 • 192.169.15 7.161
	Uiha1GUS7S.dll	Get hash	malicious	Browse	• 208.91.198.178 • 192.169.15 7.161
	SecuriteInfo.com.Mal.EncPk-APW.20360.dll	Get hash	malicious	Browse	• 208.91.198.178 • 192.169.15 7.161
	10.dll	Get hash	malicious	Browse	• 208.91.198.178 • 192.169.15 7.161
	iopjvdf.dll	Get hash	malicious	Browse	• 208.91.198.178 • 192.169.15 7.161
	d88e07467ddcf9e3b19fa972b9f000d1.exe	Get hash	malicious	Browse	• 208.91.198.178 • 192.169.15 7.161
37f463bf4616ecd445d4a1937da06e19	f4b1bde3-706a-40d2-8ace-693803810b6f.exe	Get hash	malicious	Browse	• 192.169.15 7.161
	LIQUIDACION INTERBANCARIA 02_22_2021.xls	Get hash	malicious	Browse	• 192.169.15 7.161
	document-550193913.xls	Get hash	malicious	Browse	• 192.169.15 7.161
	GUEROLA INDUSTRIES N#U00ba de cuenta.exe	Get hash	malicious	Browse	• 192.169.15 7.161
	receipt145.htm	Get hash	malicious	Browse	• 192.169.15 7.161
	xerox for hycite.htm	Get hash	malicious	Browse	• 192.169.15 7.161
	SecuriteInfo.com.Heur.15528.xls	Get hash	malicious	Browse	• 192.169.15 7.161

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Muligheds.exe	Get hash	malicious	Browse	• 192.169.157.161
	DHL_6368638172 documento de recibo,pdf.exe	Get hash	malicious	Browse	• 192.169.157.161
	PDF.exe	Get hash	malicious	Browse	• 192.169.157.161
	pagamento.exe	Get hash	malicious	Browse	• 192.169.157.161
	message_zdm (2).html	Get hash	malicious	Browse	• 192.169.157.161
	Statement-ID28865611496334.vbs	Get hash	malicious	Browse	• 192.169.157.161
	Statement-ID21488878391791.vbs	Get hash	malicious	Browse	• 192.169.157.161
	frank_2021-02-22_02-03.exe	Get hash	malicious	Browse	• 192.169.157.161
	Statement-ID72347595684775.vbs	Get hash	malicious	Browse	• 192.169.157.161
	MR52.vbs	Get hash	malicious	Browse	• 192.169.157.161
	Scan_medcal equipment sample_pdf.exe	Get hash	malicious	Browse	• 192.169.157.161
	rfq02212021.exe	Get hash	malicious	Browse	• 192.169.157.161
	RE ICA 40 Sdn Bhd- Purchase Order#6769704.exe	Get hash	malicious	Browse	• 192.169.157.161

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{920BAF35-7557-11EB-90EB-ECF4BBEA1588}.dat

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.84856656463155
Encrypted:	false
SSDEEP:	192:r3ZoZ12xWKtDifNRfzMe3BydD8sf4RujX:rposACkg2mrh
MD5:	CC0839461BF3524F53495B614F900C1E
SHA1:	ED510A27010418870F36443495B871535085B250
SHA-256:	F7B62B91A8DB59B574E9EFAAE8320B7CCEDC3EF8320784A6A9B7957FF29C4667
SHA-512:	630FBE4E7310E89F37E38E4FD37834DB7C79F287A415188EC398EA0270FF4FDE76FD1DB6410906054E763F91D4A6D204FF6D7C532C989FC422B54BF6194DF10E
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\{920BAF37-7557-11EB-90EB-ECF4BBEA1588}.dat

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	29444
Entropy (8bit):	1.794725427239966
Encrypted:	false
SSDEEP:	96:r3ZsQE6CBSyjF25WbMDbMQa1pzX2BlO70EH5h:r3ZsQE6CkyjF25WbMDbMQqpSBlOZH5h
MD5:	05C7154E35AB6A2A8F7DC63F4E289274
SHA1:	3DF842FAE87B7D0333779E67DD02206A10CAE68D
SHA-256:	AA2BE18E8E34CA217B8F5F1925C4AD974F7B58F34030B479C9757202CE2408C8
SHA-512:	D1405AC093DB21232B979D0D451FF5F8C63F5B3079F2AB5551948A00C69247C20D0455BB7112CD5F318DA806A3589A6E30C020D7F9BE94D74C0D362D67472AE
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{920BAF37-7557-11EB-90EB-ECF4BBEA1588}.dat	
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{99B83FD3-7557-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5628787296546043
Encrypted:	false
SSDEEP:	48:IwiGcprbGwpaDG4pQDGrapbSQGQpKCG7HpRVTGIpG:rWZ1Q16nBSYAtTDA
MD5:	E67013FA0FABB1BEAD4BED5951E7B836
SHA1:	830F3173699D9ECFA9EBE7264C154CB8CE63E4FE
SHA-256:	27633182774D0D0714849DAE741BB2AE60DF5DD3D627C1B70AB9EA2F361BB161
SHA-512:	6DC9F0B4B2B5A04876F14BCA253733CAA8B0BCCC29D4AC9639CC380126C65B0EA93BD4C6D26760B498B96849927D501EDB6EDF8511ACC2DC34CB8004E9CC4BA
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):	5.114417751291332
Encrypted:	false
SSDEEP:	12:TMHdNMNxOE0kCekC1nWimI002EtM3MHdNMNxOE0kCekC1nWimI00OYGVbkEtMb:2d6NxOB6RSZHKd6NxOB6RSZ7YLb
MD5:	0D082AF07F390BE14E01DF31C5E60DA9
SHA1:	39045AA5551DA28B35CCE55585A59903CEB60E00
SHA-256:	D66311C9E09CBFACCF84EAA121DEA78045825185D4FBCE3F7546F3EDC60C8347
SHA-512:	012057A16663C80295DF66FB414BE51CD51DC3D664B428DF2A0FFBFA48F9E50CE791CD1D7ABD0A0226208F1C3968E064DF3B20CCED79C34086EAF4A58D6E086
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x6ab20340,0x01d70964</date><accdate>0x6ab20340,0x01d70964</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>0x6ab20340,0x01d70964</date><accdate>0x6ab20340,0x01d70964</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):	5.093375475748663
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kiSCcSC1nWimI002EtM3MHdNMNxe2kiSCcSC1nWimI00OYGkak6Ety:2d6NxrISZHKd6NxrISZ7Yza7b
MD5:	E01331A6EB1343F508DA169504CEB422
SHA1:	E39AA20353A9B5F5399B488610494C8B8AA00F1F
SHA-256:	60E926C69C992C0A1B23D09118021D3CDF4EE4959BA5357E07C60FC56C2A2366
SHA-512:	F1ACE378536E174F7D3FF0802618367D0340619D8BDEE87DCAADCD3EFC10894CEAFA2F6B4FA90191B6AA36A8E09CADA8D9AD91F78D0C1BBB47304AE0D57D1E87
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x6aaadc5c,0x01d70964</date><accdate>0x6aaadc5c,0x01d70964</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>0x6aaadc5c,0x01d70964</date><accdate>0x6aaadc5c,0x01d70964</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):	5.133664965116651
Encrypted:	false
SSDEEP:	12:TMHdNMNxvL0kCekC1nWimI002EtM3MHdNMNxvL0kCekC1nWimI00OYGmZEtMb:2d6Nxvg6RSZHKd6Nxvg6RSZ7Yjb
MD5:	90C17E549181CFDF88BC408E181AD19C
SHA1:	39470F72E77D650AD6009BCC5803FEDCC50F2663
SHA-256:	6BCF727C5C6A044FD1D7C2ECAD7FEC76A3D4E41BBEA889B7A17FF5752A18E0A3
SHA-512:	B18E180E23F391A2EF84B88A83A5DC22D6135FA645E20420200D5E7FDBCAE2D9638CB58C645AE676E898BC5DD7F1D6A51EC90A232F15487A17C8A28CB37EB56
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x6ab20340,0x01d70964</date><accdate>0x6ab20340,0x01d70964</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>0x6ab20340,0x01d70964</date><accdate>0x6ab20340,0x01d70964</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):	5.081922262182561
Encrypted:	false
SSDEEP:	12:TMHdNMNxioCaC1nWimI002EtM3MHdNMNxioCaC1nWimI00OYGd5EtMb:2d6NxESZHKd6NxESZ7YEjb
MD5:	29BE80C87E97121C213CB3D34327E385
SHA1:	80AA8DA5E6751E11848E3244620E117C790D3542
SHA-256:	24691562C62340B2BA95A94742E3F6B545B32ADABC46F500360648DEC10D8425
SHA-512:	9155DA36DC69BEE74FF7E87DEA4B79692CE7786EF13B442E615C49AE83FCE5B64D0E11983CC11EA79DA1BD1832150902D242DF7A2204265E26AEE4D9AA95F73
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x6aafa0e9,0x01d70964</date><accdate>0x6aafa0e9,0x01d70964</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>0x6aafa0e9,0x01d70964</date><accdate>0x6aafa0e9,0x01d70964</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):	5.145057217640643
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGw0kCekC1nWimI002EtM3MHdNMNxhGw0kCekC1nWimI00OYG8K075Es:2d6NxQl6RSZHKd6NxQl6RSZ7YrKajb
MD5:	2C9F501DA18158DCA76A8FF7DA4F29CE
SHA1:	6B97A5EAD015D84EA709C81C4C90E862156D6DD5
SHA-256:	8266CEE2AC9ABC4A35E58DE8A7AF318D2222F35A3FA927998CD6B73B8E71F35E
SHA-512:	E05D76187B42335C1104334DA09BD347D9D205D0431D1839A20F529E64ECE2940C2FE83A903E038E860E6DD58889421DD62DED3310907913F3E9BF453AA81F44
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x6ab20340,0x01d70964</date><accdate>0x6ab20340,0x01d70964</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>0x6ab20340,0x01d70964</date><accdate>0x6ab20340,0x01d70964</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):	5.088468942202851
Encrypted:	false
SSDEEP:	12:TMHdNMNx0noCaC1nWimI002EtM3MHdNMNx0noCekC1nWimI00OYGxEtMb:2d6Nx0/SZHKd6Nx0eRSZ7Ygb
MD5:	6FD9BBD0AE034CE87D8A53D91420C3CE
SHA1:	E92964FE90C2B07EC8216A6688EAE1F236D4516C
SHA-256:	A198B08AD5A452352E7DC23989B3DD8093ABBD30DC95E0A3A145D481F01C00A0
SHA-512:	185A14DBAE8CD44D3DE5D5E67D3AE7EF148FF19D6BC3036D9D388E62CCAA606BCAD7737D9C69454E5469D8556D72A178E66BB61A04C95A45CC8611212768A8 3
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x6aafa0e9,0x01d70964</date><a ccdate>0x6aafa0e9,0x01d70964</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>0x6aafa0e9,0x01d70964</date><accdate>0x6 ab20340,0x01d70964</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):	5.106472382964582
Encrypted:	false
SSDEEP:	12:TMHdNMNxxoCaC1nWimI002EtM3MHdNMNxxoCaC1nWimI00OYG6Kq5EtMb:2d6NxxSZHKd6NxxSZ7Yhb
MD5:	52D0BECF21B145CD666A40B605025EE9
SHA1:	C3C3CFADDE941BF6D3190549487AC88E2933C48C
SHA-256:	12368EAE89D2A863C281446F62EEB1F741CEE6DE04EF8EFD7C9CF2CC8F9B6A9C
SHA-512:	449D441E553A6890C98CB91F052A5F17CB5517E5859E3CE9E01A3F94DB00BE33A5BA12839B2F53DB61A5F74D521BAF195DB7EDFEEE2725108FE90D64ABBF803 4
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x6aafa0e9,0x01d70964</date>< accdate>0x6aafa0e9,0x01d70964</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>0x6aafa0e9,0x01d70964</date><accdate>0 x6aafa0e9,0x01d70964</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):	5.098527241326319
Encrypted:	false
SSDEEP:	12:TMHdNMNxcQtCetC1nWimI002EtM3MHdNMNxcQtCetC1nWimI00OYGVEtMb:2d6NxSSZHKd6NxSSZ7Ykb
MD5:	399EF1928730BF78593B16DEAC7D6E5B
SHA1:	12DEEE1FC18CEB67EA7A6A1AD4523F23D3A74C22
SHA-256:	8DA5512F1CE5B50803EF119E838D0D4B1F5BBABAD70CF4F5C53DA64B7045E4A3
SHA-512:	1521E47BBB5E1536603EA836DF525B8DA8B3D9D991291AC54280DFC81B3589AD8131D8905314C763A8EAFE1970794C7A4499851E8E48967485B1808F8F14DCF6
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x6aad3e8e,0x01d70964</date> <accdate>0x6aad3e8e,0x01d70964</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>0x6aad3e8e,0x01d70964</date><accdate >0x6aad3e8e,0x01d70964</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

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml	
Entropy (8bit):	5.067517880816491
Encrypted:	false
SSDEEP:	12:TMHdNMNxfnoCaC1nWimI002EtM3MHdNMNxfnoCaC1nWimI00OYGe5EtMb:2d6NxHSZHKd6NxHSZ7YLjb
MD5:	6357EE3D77268A8D600CEB67605E98D5
SHA1:	E3DB30439696F58DF0F42585975851511D364702
SHA-256:	E4B037D9150B24D7D217D77488AEBBB157D62A36951A1C853059811F7F495D95
SHA-512:	18B1B1638F641DA5053B173D893F098896446B4B83EE430A6F941D2671077349553B19928E1C3A810478EDFE0D701BB74393FD526AA4992C7EC9523D1B6F9B8D
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x6aafa0e9,0x01d70964</date><accdate>0x6aafa0e9,0x01d70964</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>0x6aafa0e9,0x01d70964</date><accdate>0x6aafa0e9,0x01d70964</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:	dropped
Size (bytes):	1320
Entropy (8bit):	4.976173540641026
Encrypted:	false
SSDEEP:	24:RsWfImyQOyrQZ9FjFjFjFAZ4qCYORlzi+fzi+fzi+fziAVR9u:RsWQm5OyoBBB6ZvORlzi0zi0ziGRI
MD5:	E6E35AB1BEEB430776892C9C1CECB5E6
SHA1:	AD73F61752F8757E5B5A1B7F908C550455232763
SHA-256:	A491F1D67AE301A620C6943F2CB1DCE28159E9C131AF286030026DB49A51A929
SHA-512:	C4999D28AFA37188FA6BBA9F3AE5E1D5399E53383688A30AD53DA62C4FA104123005B5576A0A52A609319C30DCAF475058D72D6C2E7A4898341EE570F8E97F37
Malicious:	false
Reputation:	low
Preview:	B.h.t.t.p.s.:././.s.y.d.n.e.y.b.u.i.l.d.i.n.g.e.n.g.i.n.e.e.r.s...c.o.m...a.u./.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...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...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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/UVlb+J3+MqU4
MD5:	BD6E291A9A3CC17ED37605E4FF0010CC
SHA1:	6C1EFD74231E3D253E0F51E4656ECED2F3335D71
SHA-256:	706DE242E7C3CFC4B16BA8174723F26FB80566C3171E9E795F057476011A5DE1
SHA-512:	D940D950167404FE53BD6A7AABAAA8C57AC58878AAD045B9F09B1FA331743A8DB5ECA2568F7E1C3D92EDA4C3AC8F1BE112409171028 62F65BB0372EE1D82B33
Malicious:	false
Reputation:	moderate, very likely benign file
IE Cache URL:	http://https://sydneybuildingengineers.com.au/OfficeV4/images/enterpass.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\2WF3MMUU\exrobotosv4[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	273
Entropy (8bit):	5.179917685373619
Encrypted:	false
SSDEEP:	6:pn0+Dy9xwol6hEr6VX16hu9nPHTLiRAdIEB+s7U+KqD:J0+ox0RJWWPzQAfIsfT
MD5:	2B9C6FB3BF190B5120DB7A101A6423A1

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\exrobotosv4[1].htm	
SHA1:	036A29B9FD863690D0E9B587F23AC8AD7FF43318
SHA-256:	A8B64AD32CC041DBA431BDB513F7B32D9A0136B946098C41316DA8FE6910AABA
SHA-512:	8CB66B78068E3A70ED0AA09A1D7D1B7267FC5ACFCB9C4245FE9A732C6EA44929F561ED3E6C1767D3203FE6ACF9C7C2B235461FCC21187A6E4E7A138FCCC0B79
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">.<html><head>.<title>301 Moved Permanently</title>.</head><body>. Moved Permanently . The document has moved here. .</body></html>.

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
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://sydneybuildingengineers.com.au/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.$...%F..%@....K..l[.Z#.cN.jZY:hg.Z.E.aYk..RvZ.....{...*.LH.[..bK.|... ..}..Z..G.*.|j.t.k.....ON..a.1..D.....$..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\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://sydneybuildingengineers.com.au/OfficeV4/images/sigin.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\9026IKNJ\OfficeV4[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	298
Entropy (8bit):	5.424574859702785
Encrypted:	false
SSDEEP:	6:pn0+Dy9xwol6hEr6VX16hu9nPL0ebWBK2fECtgUF6vAr+KqD:J0+ox0RJWWPLFb32fEWFiXT
MD5:	1F050ABD9871AB7BC253372B20676707
SHA1:	FAF361AABE24FB11BF6E138AAE938309D2C8846B
SHA-256:	390FB9037C5F93F9C6FBEDA176512667FBF586A11C1A61677C9A94F2A1A03639
SHA-512:	474CA538FC0843A1BA5207F57300F927DAB546F300ECC456510A743420C4EAA388A03D4533496E4EDA94901D5844E02359F137364A506B8B0AC4DC2220723600
Malicious:	false
Preview:	<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">.<html><head>.<title>301 Moved Permanently</title>.</head><body>. Moved Permanently . The document has moved here. .</body></html>.

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:NoBBB6ZvORlzi0zi0ziGR9
MD5:	7CDD5A7E87E82D145E7F82358F9EBD04
SHA1:	265104CAD00300E4094F8CE6A9EDC86E54812EAD
SHA-256:	5D91563B6ACD54468AE282083CF9EE3D2C9B2DAA45A8DE9CB661C2195B9F6CBF
SHA-512:	407919CB23D24FD8EA7646C941F4DCEE922B9B4021B6975DD30C738E61E1A147E10A473956A8FBB2DDF7559695E540F2CDF8535DB2C66FA6C7DECDA38BB1B12
Malicious:	false
IE Cache URL:	http://https://sydneybuildingengineers.com.au/OfficeV4/images/favicon.ico
Preview:	..... .h.....(..... ....P..$..%..%..%..%..''...}.....9e..<h..<h..<h..<h..;f..c....2.....f.w....K...N...N...N...N...L..lq...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....l...L...L...L...L...K..Gp.....g...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....}.....~.8..0.....k...f....}.....~.8../.....j...e....|...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\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://sydneybuildingengineers.com.au/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\Microsoft\Windows\INetCache\IE\CS6IXJW6\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
IE Cache URL:	http://https://sydneybuildingengineers.com.au/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\CS6IXJW6\authorize_client_id_5g1afb80-7jfq-ask4-t1bx-5zw0d17rfy48_qa32ux85vsrdgt9ncpmw7ebyo4kz10fjilh6hskufelop5ya3m1i0942tcrv8znqxbwj7gd692ez0tj4dmhkufaqbo7pnvyrxl3568cs1iwg[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12530

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\authorize_client_id_5g1afb80-7jfq-ask4-t1bx-5zw0d17rfy48_qa32ux85vsrdgt9ncpmw7ebyo4kz10fjilh6hskufelop5ya3m1i0942tcrv8znqxbwj7gd692ez0tj4dmhkufaqbo7pnvyrxl3568cs1iwg[1].htm	
Entropy (8bit):	5.61435194414764
Encrypted:	false
SSDEEP:	384:Qx4dYLrFhld6UTyv6R0+nQKrlibQmYMH/pMa1E:Kb/yvCndhi8yfpH1E
MD5:	09C38B34378DC77C039A763ABDC79BFC
SHA1:	FC8E6EAC6934571B6770EF0385EE0F90090E9E4D
SHA-256:	7DD245A1505B111C1DF02CB04687FE51FCE3ABDD8F1E39A8B9C26997FD5C7791
SHA-512:	7770006632B1C5106FB31FFAED8F6A4F6A445267DA4462D25B7F8522F4FE45CFDD7AE3D83359A7592A251CA8DB25C3D8F2387089A600B67EE0B802E54522F603
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_10, Description: Yara detected HtmlPhish_10, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\authorize_client_id_5g1afb80-7jfq-ask4-t1bx-5zw0d17rfy48_qa32ux85vsrdgt9ncpmw7ebyo4kz10fjilh6hskufelop5ya3m1i0942tcrv8znqxbwj7gd692ez0tj4dmhkufaqbo7pnvyrxl3568cs1iwg[1].htm, Author: Joe Security
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>confirm your email</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="t7m8xsn" class="nd s8lqyrcv" style="display: block;">. .. <div style="background-image: url("images/inv-small-background.

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://sydneybuildingengineers.com.au/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://sydneybuildingengineers.com.au/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..x..|.....Z=..z....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\style[1].css	
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://sydneybuildingengineers.com.au/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\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://sydneybuildingengineers.com.au/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,.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-.893,0,1.164,1.164,0,0,1-.607-.607,1.161,1.161,0,0,1,0-.893,1.164,1.164,0,0,1,.607-.607A1.107,1.107,0,0,1,8,6.857m6.857,0a1.107,1.107,0,0,1,.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-.893,0,1.164,1.164,0,0,1-.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://sydneybuildingengineers.com.au/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,.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-.893,0,1.164,1.164,0,0,1-.607-.607,1.161,1.161,0,0,1,0-.893,1.164,1.164,0,0,1,.607-.607A1.107,1.107,0,0,1,8,6.857m6.857,0a1.107,1.107,0,0,1,.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-.893,0,1.164,1.164,0,0,1-.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\exrobotosv4[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	downloaded
Size (bytes):	230
Entropy (8bit):	5.389463555930212
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\exrobotosv4[1].htm	
SSDEEP:	6:hjQL/sGcQ2WF4ZXR0AqJm7+mmHr0ebWB4ECtgUF6vApOL:hjxbjPqJm7+xHrFbcWFioOL
MD5:	8811C2BED058D34E67AAB7C4E57B0223
SHA1:	004F00A5154F6D0A3D14F2CAA409DA9521CDB550
SHA-256:	B231234616F9B76794F2AEDC3038DFBEB5DFA37E2D924D1A55DDC679608AE288
SHA-512:	4F50687D279B138FC7A77375F455A442333A01A14C25F562712305FDE34C8227A15F4E383358CB88F9E7F1B361DA300B1494AC4D7B226C86C8D4B3260DF45E8C
Malicious:	false
IE Cache URL:	http://https://saisas.com.co/exrobotosv4/?vishal.kumar@smartandfinal.com
Preview:	<!DOCTYPE html">.<html>. <head>. <title>Review: 0ffice365</title>. <script type="text/javascript">window.location.href = "https://sydneybuildingengineers.com.au/OfficeV4?/dmlzaGFsLmt1bWFyQHNtYXJ0YW5kZmluYWwuY29t"</script>.

C:\Users\user\AppData\Local\Temp\~DF0C840B5320C13C8C.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	43373
Entropy (8bit):	0.46171655188967237
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+V75or8r414UzWBlO70EHL:kBqoxKAuqR+V75or8rKPiBlOZHL
MD5:	39EBA000C28E4BAE67BDFED43BAA54A2
SHA1:	4FEBC8D5E77845E177C0B53D3C56D48FD552F203
SHA-256:	7B73DF045AB6A2F7B0BCA3C8EBB202096A9157D511567BEAAED5C3927E10D3B3
SHA-512:	C7EFEEE50A0E7E697DADCD736DC9AB2CD1390274C9BFF0EA727B013173B66C50DA86D4AEA82C0B2ED9F61B0F0A5BB15388A51A41A5E7A984EEB2A98B97606A2F
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF837C423F64999335.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.47599519052501754
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lokA9lokQ9lWkO2xdeh2xt5dxtEzhzB:kBqoI8CsFfG
MD5:	9794E786A7D9719EDA29406BBCDDFB7C
SHA1:	F0136E6D96B2141675DA4664450320759C1A9C41
SHA-256:	499C84543D837C8D76E7DE67A525B29DD83AE227ADFBE5ABF290ED429645B73D
SHA-512:	49C11DC8F5F83A3BA937D21185CF7BB84F9FDBF2B0DCE3BC51A702094A1D749DA50F59F439280AF10CF4AF8D670185B9D67786F8D152D6B8AB46D00E322B574A
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFC6F44CA59B7DB5F9.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	1.0267500105381397
Encrypted:	false
SSDEEP:	96:kBqoxDhHWSVSE+M+Q5CK7VC2s7iDFgQ9ki3D1:kBqoxDhHjgE+M+Q5CK1QiR3D1
MD5:	A55B6CDE2DA92BC4E46420F0691E946B
SHA1:	B35878C65074EC1D692D6486FCCFC1ED77B38321
SHA-256:	C530022B78638EC2CF3695EC132B28855CC2DCCC07D57754AD065D8A8ECA3F05
SHA-512:	1AFB5E7062AAB661C2097BCE17A4ACDB7B5EAFD113F3458962FF2E0F386E73FA7F2D3558F20BC060B2036DCE2B90F727CAB62132BAEAE2AB1A343BF41A016C56
Malicious:	false

C:\Users\user\AppData\Local\Temp\~DFC6F44CA59B7DB5F9.TMP	
Preview:	............................*%..H..M..{y..+.0...(................... ....*%..H..M..{y..+.0...(.................. ....

Static File Info

General

File type:	HTML document, ASCII text, with no line terminators
Entropy (8bit):	4.692825608716909
TrID:	• HyperText Markup Language (31031/1) 100.00%
File name:	smartandfinalTicket#51347303511505986.htm
File size:	128
MD5:	5f42d465e7e680e051a74bb797bc6535
SHA1:	843faae5f7d10488aed129367e8ea7ada3396942
SHA256:	e4b97c79b4c90cb26a1c518bc1a6d821444436d4420d1e579b781b1c3704bb57
SHA512:	bbae0a97261cfc12cc203e7cf038a3f453da86388e1b76cface56dc4a6c0e1fdefb5a5d603f65c6acf641108da6c15d440fa180b6c7f3655e95bc640aff1a467
SSDEEP:	3:gnkAqRAdu6/GY7voOkADYnWPyTLiBXkAaWIEBi1J2+x7b:7AqJm7+mYnHTLi9kAdIEB+sgb
File Content Preview:	<script type="text/javascript">window.location.href="https://saisas.com.co/exrobotosv4?vishal.kumar@smartandfinal.com";</script>

Network Behavior

Network Port Distribution

Total Packets: 80

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 22:47:36.740900993 CET	49733	443	192.168.2.4	208.91.198.178
Feb 22, 2021 22:47:36.741144896 CET	49734	443	192.168.2.4	208.91.198.178
Feb 22, 2021 22:47:36.917944908 CET	443	49733	208.91.198.178	192.168.2.4
Feb 22, 2021 22:47:36.918159008 CET	49733	443	192.168.2.4	208.91.198.178
Feb 22, 2021 22:47:36.918370008 CET	443	49734	208.91.198.178	192.168.2.4
Feb 22, 2021 22:47:36.918577909 CET	49734	443	192.168.2.4	208.91.198.178
Feb 22, 2021 22:47:36.927895069 CET	49733	443	192.168.2.4	208.91.198.178
Feb 22, 2021 22:47:36.928350925 CET	49734	443	192.168.2.4	208.91.198.178
Feb 22, 2021 22:47:37.105814934 CET	443	49733	208.91.198.178	192.168.2.4
Feb 22, 2021 22:47:37.105865955 CET	443	49734	208.91.198.178	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 22:47:37.107625008 CET	443	49734	208.91.198.178	192.168.2.4
Feb 22, 2021 22:47:37.107676983 CET	443	49734	208.91.198.178	192.168.2.4
Feb 22, 2021 22:47:37.107716084 CET	443	49734	208.91.198.178	192.168.2.4
Feb 22, 2021 22:47:37.107738018 CET	49734	443	192.168.2.4	208.91.198.178
Feb 22, 2021 22:47:37.107788086 CET	49734	443	192.168.2.4	208.91.198.178
Feb 22, 2021 22:47:37.107798100 CET	49734	443	192.168.2.4	208.91.198.178
Feb 22, 2021 22:47:37.107846022 CET	443	49733	208.91.198.178	192.168.2.4
Feb 22, 2021 22:47:37.107898951 CET	443	49733	208.91.198.178	192.168.2.4
Feb 22, 2021 22:47:37.107917070 CET	49733	443	192.168.2.4	208.91.198.178
Feb 22, 2021 22:47:37.107953072 CET	443	49733	208.91.198.178	192.168.2.4
Feb 22, 2021 22:47:37.107959032 CET	49733	443	192.168.2.4	208.91.198.178
Feb 22, 2021 22:47:37.108021021 CET	49733	443	192.168.2.4	208.91.198.178
Feb 22, 2021 22:47:37.142250061 CET	49734	443	192.168.2.4	208.91.198.178
Feb 22, 2021 22:47:37.142251015 CET	49733	443	192.168.2.4	208.91.198.178
Feb 22, 2021 22:47:37.147919893 CET	49734	443	192.168.2.4	208.91.198.178
Feb 22, 2021 22:47:37.148458958 CET	49734	443	192.168.2.4	208.91.198.178
Feb 22, 2021 22:47:37.148679972 CET	49733	443	192.168.2.4	208.91.198.178
Feb 22, 2021 22:47:37.319236040 CET	443	49733	208.91.198.178	192.168.2.4
Feb 22, 2021 22:47:37.319295883 CET	443	49733	208.91.198.178	192.168.2.4
Feb 22, 2021 22:47:37.319405079 CET	49733	443	192.168.2.4	208.91.198.178
Feb 22, 2021 22:47:37.319461107 CET	49733	443	192.168.2.4	208.91.198.178
Feb 22, 2021 22:47:37.320167065 CET	443	49734	208.91.198.178	192.168.2.4
Feb 22, 2021 22:47:37.320219040 CET	443	49734	208.91.198.178	192.168.2.4
Feb 22, 2021 22:47:37.320305109 CET	49734	443	192.168.2.4	208.91.198.178
Feb 22, 2021 22:47:37.320354939 CET	49734	443	192.168.2.4	208.91.198.178
Feb 22, 2021 22:47:37.321033955 CET	49733	443	192.168.2.4	208.91.198.178
Feb 22, 2021 22:47:37.322359085 CET	49734	443	192.168.2.4	208.91.198.178
Feb 22, 2021 22:47:37.325217962 CET	443	49734	208.91.198.178	192.168.2.4
Feb 22, 2021 22:47:37.325340033 CET	49734	443	192.168.2.4	208.91.198.178
Feb 22, 2021 22:47:37.326481104 CET	443	49733	208.91.198.178	192.168.2.4
Feb 22, 2021 22:47:37.326643944 CET	49733	443	192.168.2.4	208.91.198.178
Feb 22, 2021 22:47:37.366476059 CET	443	49734	208.91.198.178	192.168.2.4
Feb 22, 2021 22:47:37.497961044 CET	443	49734	208.91.198.178	192.168.2.4
Feb 22, 2021 22:47:37.537406921 CET	443	49733	208.91.198.178	192.168.2.4
Feb 22, 2021 22:47:37.608355999 CET	443	49734	208.91.198.178	192.168.2.4
Feb 22, 2021 22:47:37.608467102 CET	49734	443	192.168.2.4	208.91.198.178
Feb 22, 2021 22:47:37.612776041 CET	49734	443	192.168.2.4	208.91.198.178
Feb 22, 2021 22:47:37.779253960 CET	443	49734	208.91.198.178	192.168.2.4
Feb 22, 2021 22:47:37.983474970 CET	443	49734	208.91.198.178	192.168.2.4
Feb 22, 2021 22:47:37.983551025 CET	49734	443	192.168.2.4	208.91.198.178
Feb 22, 2021 22:47:38.822577953 CET	49736	443	192.168.2.4	192.169.157.161
Feb 22, 2021 22:47:38.823863983 CET	49737	443	192.168.2.4	192.169.157.161
Feb 22, 2021 22:47:39.006057978 CET	443	49736	192.169.157.161	192.168.2.4
Feb 22, 2021 22:47:39.006191015 CET	49736	443	192.168.2.4	192.169.157.161
Feb 22, 2021 22:47:39.006827116 CET	49736	443	192.168.2.4	192.169.157.161
Feb 22, 2021 22:47:39.007209063 CET	443	49737	192.169.157.161	192.168.2.4
Feb 22, 2021 22:47:39.007353067 CET	49737	443	192.168.2.4	192.169.157.161
Feb 22, 2021 22:47:39.007885933 CET	49737	443	192.168.2.4	192.169.157.161
Feb 22, 2021 22:47:39.190157890 CET	443	49736	192.169.157.161	192.168.2.4
Feb 22, 2021 22:47:39.190320015 CET	443	49736	192.169.157.161	192.168.2.4
Feb 22, 2021 22:47:39.190347910 CET	443	49736	192.169.157.161	192.168.2.4
Feb 22, 2021 22:47:39.190365076 CET	443	49736	192.169.157.161	192.168.2.4
Feb 22, 2021 22:47:39.190376043 CET	443	49736	192.169.157.161	192.168.2.4
Feb 22, 2021 22:47:39.190521002 CET	49736	443	192.168.2.4	192.169.157.161
Feb 22, 2021 22:47:39.190577984 CET	49736	443	192.168.2.4	192.169.157.161
Feb 22, 2021 22:47:39.190897942 CET	443	49737	192.169.157.161	192.168.2.4
Feb 22, 2021 22:47:39.191116095 CET	443	49737	192.169.157.161	192.168.2.4
Feb 22, 2021 22:47:39.191198111 CET	49737	443	192.168.2.4	192.169.157.161
Feb 22, 2021 22:47:39.191200972 CET	443	49737	192.169.157.161	192.168.2.4
Feb 22, 2021 22:47:39.191224098 CET	443	49737	192.169.157.161	192.168.2.4
Feb 22, 2021 22:47:39.191236973 CET	443	49737	192.169.157.161	192.168.2.4
Feb 22, 2021 22:47:39.191258907 CET	49737	443	192.168.2.4	192.169.157.161
Feb 22, 2021 22:47:39.191294909 CET	49737	443	192.168.2.4	192.169.157.161
Feb 22, 2021 22:47:39.191466093 CET	443	49736	192.169.157.161	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 22:47:39.191545010 CET	49736	443	192.168.2.4	192.169.157.161
Feb 22, 2021 22:47:39.192704916 CET	443	49737	192.169.157.161	192.168.2.4
Feb 22, 2021 22:47:39.192770958 CET	49737	443	192.168.2.4	192.169.157.161
Feb 22, 2021 22:47:39.235647917 CET	49736	443	192.168.2.4	192.169.157.161
Feb 22, 2021 22:47:39.236179113 CET	49736	443	192.168.2.4	192.169.157.161
Feb 22, 2021 22:47:39.236318111 CET	49737	443	192.168.2.4	192.169.157.161
Feb 22, 2021 22:47:39.419302940 CET	443	49736	192.169.157.161	192.168.2.4
Feb 22, 2021 22:47:39.419471025 CET	49736	443	192.168.2.4	192.169.157.161
Feb 22, 2021 22:47:39.419964075 CET	443	49737	192.169.157.161	192.168.2.4
Feb 22, 2021 22:47:39.420145035 CET	49737	443	192.168.2.4	192.169.157.161
Feb 22, 2021 22:47:39.459527016 CET	443	49736	192.169.157.161	192.168.2.4
Feb 22, 2021 22:47:39.610702038 CET	443	49736	192.169.157.161	192.168.2.4
Feb 22, 2021 22:47:39.610910892 CET	49736	443	192.168.2.4	192.169.157.161
Feb 22, 2021 22:47:39.615317106 CET	49736	443	192.168.2.4	192.169.157.161
Feb 22, 2021 22:47:39.798717976 CET	443	49736	192.169.157.161	192.168.2.4
Feb 22, 2021 22:47:39.990684986 CET	443	49736	192.169.157.161	192.168.2.4
Feb 22, 2021 22:47:39.990736961 CET	443	49736	192.169.157.161	192.168.2.4
Feb 22, 2021 22:47:39.990761995 CET	443	49736	192.169.157.161	192.168.2.4
Feb 22, 2021 22:47:39.990784883 CET	443	49736	192.169.157.161	192.168.2.4
Feb 22, 2021 22:47:39.990813971 CET	443	49736	192.169.157.161	192.168.2.4
Feb 22, 2021 22:47:39.990842104 CET	443	49736	192.169.157.161	192.168.2.4
Feb 22, 2021 22:47:39.990870953 CET	443	49736	192.169.157.161	192.168.2.4
Feb 22, 2021 22:47:39.990891933 CET	49736	443	192.168.2.4	192.169.157.161
Feb 22, 2021 22:47:39.990900040 CET	443	49736	192.169.157.161	192.168.2.4
Feb 22, 2021 22:47:39.990931034 CET	443	49736	192.169.157.161	192.168.2.4
Feb 22, 2021 22:47:39.990959883 CET	443	49736	192.169.157.161	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 22:47:27.693114996 CET	59123	53	192.168.2.4	8.8.8.8
Feb 22, 2021 22:47:27.741898060 CET	53	59123	8.8.8.8	192.168.2.4
Feb 22, 2021 22:47:28.030894995 CET	54531	53	192.168.2.4	8.8.8.8
Feb 22, 2021 22:47:28.082415104 CET	53	54531	8.8.8.8	192.168.2.4
Feb 22, 2021 22:47:29.031456947 CET	49714	53	192.168.2.4	8.8.8.8
Feb 22, 2021 22:47:29.093513966 CET	53	49714	8.8.8.8	192.168.2.4
Feb 22, 2021 22:47:30.250067949 CET	58028	53	192.168.2.4	8.8.8.8
Feb 22, 2021 22:47:30.298794985 CET	53	58028	8.8.8.8	192.168.2.4
Feb 22, 2021 22:47:31.075625896 CET	53097	53	192.168.2.4	8.8.8.8
Feb 22, 2021 22:47:31.127257109 CET	53	53097	8.8.8.8	192.168.2.4
Feb 22, 2021 22:47:32.313855886 CET	49257	53	192.168.2.4	8.8.8.8
Feb 22, 2021 22:47:32.364195108 CET	53	49257	8.8.8.8	192.168.2.4
Feb 22, 2021 22:47:33.579905987 CET	62389	53	192.168.2.4	8.8.8.8
Feb 22, 2021 22:47:33.641076088 CET	53	62389	8.8.8.8	192.168.2.4
Feb 22, 2021 22:47:34.854129076 CET	49910	53	192.168.2.4	8.8.8.8
Feb 22, 2021 22:47:34.905623913 CET	53	49910	8.8.8.8	192.168.2.4
Feb 22, 2021 22:47:35.352196932 CET	55854	53	192.168.2.4	8.8.8.8
Feb 22, 2021 22:47:35.414113045 CET	53	55854	8.8.8.8	192.168.2.4
Feb 22, 2021 22:47:35.926305056 CET	64549	53	192.168.2.4	8.8.8.8
Feb 22, 2021 22:47:35.977979898 CET	53	64549	8.8.8.8	192.168.2.4
Feb 22, 2021 22:47:36.539923906 CET	63153	53	192.168.2.4	8.8.8.8
Feb 22, 2021 22:47:36.726438046 CET	53	63153	8.8.8.8	192.168.2.4
Feb 22, 2021 22:47:37.086323977 CET	52991	53	192.168.2.4	8.8.8.8
Feb 22, 2021 22:47:37.135219097 CET	53	52991	8.8.8.8	192.168.2.4
Feb 22, 2021 22:47:38.067205906 CET	53700	53	192.168.2.4	8.8.8.8
Feb 22, 2021 22:47:38.488632917 CET	53	53700	8.8.8.8	192.168.2.4
Feb 22, 2021 22:47:39.044003963 CET	51726	53	192.168.2.4	8.8.8.8
Feb 22, 2021 22:47:39.095865965 CET	53	51726	8.8.8.8	192.168.2.4
Feb 22, 2021 22:47:40.298794985 CET	56794	53	192.168.2.4	8.8.8.8
Feb 22, 2021 22:47:40.347461939 CET	53	56794	8.8.8.8	192.168.2.4
Feb 22, 2021 22:47:41.640904903 CET	56534	53	192.168.2.4	8.8.8.8
Feb 22, 2021 22:47:41.689574957 CET	53	56534	8.8.8.8	192.168.2.4
Feb 22, 2021 22:47:43.571768045 CET	56627	53	192.168.2.4	8.8.8.8
Feb 22, 2021 22:47:43.625044107 CET	53	56627	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 22:47:44.360001087 CET	56621	53	192.168.2.4	8.8.8.8
Feb 22, 2021 22:47:44.408653021 CET	53	56621	8.8.8.8	192.168.2.4
Feb 22, 2021 22:47:45.165456057 CET	63116	53	192.168.2.4	8.8.8.8
Feb 22, 2021 22:47:45.214236975 CET	53	63116	8.8.8.8	192.168.2.4
Feb 22, 2021 22:47:45.929384947 CET	64078	53	192.168.2.4	8.8.8.8
Feb 22, 2021 22:47:45.981482983 CET	53	64078	8.8.8.8	192.168.2.4
Feb 22, 2021 22:47:46.783931017 CET	64801	53	192.168.2.4	8.8.8.8
Feb 22, 2021 22:47:46.832925081 CET	53	64801	8.8.8.8	192.168.2.4
Feb 22, 2021 22:47:48.006782055 CET	61721	53	192.168.2.4	8.8.8.8
Feb 22, 2021 22:47:48.057023048 CET	53	61721	8.8.8.8	192.168.2.4
Feb 22, 2021 22:47:49.283747911 CET	51255	53	192.168.2.4	8.8.8.8
Feb 22, 2021 22:47:49.335289955 CET	53	51255	8.8.8.8	192.168.2.4
Feb 22, 2021 22:47:53.675256968 CET	61522	53	192.168.2.4	8.8.8.8
Feb 22, 2021 22:47:54.114592075 CET	53	61522	8.8.8.8	192.168.2.4
Feb 22, 2021 22:47:58.213332891 CET	52337	53	192.168.2.4	8.8.8.8
Feb 22, 2021 22:47:58.265522957 CET	53	52337	8.8.8.8	192.168.2.4
Feb 22, 2021 22:48:05.324827909 CET	55046	53	192.168.2.4	8.8.8.8
Feb 22, 2021 22:48:05.374264002 CET	53	55046	8.8.8.8	192.168.2.4
Feb 22, 2021 22:48:05.941843987 CET	49612	53	192.168.2.4	8.8.8.8
Feb 22, 2021 22:48:05.999068022 CET	53	49612	8.8.8.8	192.168.2.4
Feb 22, 2021 22:48:06.328391075 CET	55046	53	192.168.2.4	8.8.8.8
Feb 22, 2021 22:48:06.385709047 CET	53	55046	8.8.8.8	192.168.2.4
Feb 22, 2021 22:48:06.952367067 CET	49612	53	192.168.2.4	8.8.8.8
Feb 22, 2021 22:48:07.011730909 CET	53	49612	8.8.8.8	192.168.2.4
Feb 22, 2021 22:48:07.327270031 CET	55046	53	192.168.2.4	8.8.8.8
Feb 22, 2021 22:48:07.377815962 CET	53	55046	8.8.8.8	192.168.2.4
Feb 22, 2021 22:48:07.968146086 CET	49612	53	192.168.2.4	8.8.8.8
Feb 22, 2021 22:48:08.017272949 CET	53	49612	8.8.8.8	192.168.2.4
Feb 22, 2021 22:48:09.623935938 CET	55046	53	192.168.2.4	8.8.8.8
Feb 22, 2021 22:48:09.674022913 CET	53	55046	8.8.8.8	192.168.2.4
Feb 22, 2021 22:48:10.046485901 CET	49612	53	192.168.2.4	8.8.8.8
Feb 22, 2021 22:48:10.097933054 CET	53	49612	8.8.8.8	192.168.2.4
Feb 22, 2021 22:48:13.624566078 CET	55046	53	192.168.2.4	8.8.8.8
Feb 22, 2021 22:48:13.673329115 CET	53	55046	8.8.8.8	192.168.2.4
Feb 22, 2021 22:48:14.063208103 CET	49612	53	192.168.2.4	8.8.8.8
Feb 22, 2021 22:48:14.113125086 CET	53	49612	8.8.8.8	192.168.2.4
Feb 22, 2021 22:48:16.314790010 CET	49285	53	192.168.2.4	8.8.8.8
Feb 22, 2021 22:48:16.364679098 CET	53	49285	8.8.8.8	192.168.2.4
Feb 22, 2021 22:48:17.085474968 CET	50601	53	192.168.2.4	8.8.8.8
Feb 22, 2021 22:48:17.147320986 CET	53	50601	8.8.8.8	192.168.2.4
Feb 22, 2021 22:48:17.744492054 CET	60875	53	192.168.2.4	8.8.8.8
Feb 22, 2021 22:48:17.801759958 CET	53	60875	8.8.8.8	192.168.2.4
Feb 22, 2021 22:48:18.235559940 CET	56448	53	192.168.2.4	8.8.8.8
Feb 22, 2021 22:48:18.288713932 CET	59172	53	192.168.2.4	8.8.8.8
Feb 22, 2021 22:48:18.311781883 CET	53	56448	8.8.8.8	192.168.2.4
Feb 22, 2021 22:48:18.377490044 CET	53	59172	8.8.8.8	192.168.2.4
Feb 22, 2021 22:48:18.859749079 CET	62420	53	192.168.2.4	8.8.8.8
Feb 22, 2021 22:48:18.922635078 CET	53	62420	8.8.8.8	192.168.2.4
Feb 22, 2021 22:48:19.454322100 CET	60579	53	192.168.2.4	8.8.8.8
Feb 22, 2021 22:48:19.511662006 CET	53	60579	8.8.8.8	192.168.2.4
Feb 22, 2021 22:48:20.294550896 CET	50183	53	192.168.2.4	8.8.8.8
Feb 22, 2021 22:48:20.351878881 CET	53	50183	8.8.8.8	192.168.2.4
Feb 22, 2021 22:48:21.223568916 CET	61531	53	192.168.2.4	8.8.8.8
Feb 22, 2021 22:48:21.272449017 CET	53	61531	8.8.8.8	192.168.2.4
Feb 22, 2021 22:48:22.460555077 CET	49228	53	192.168.2.4	8.8.8.8
Feb 22, 2021 22:48:22.517735958 CET	53	49228	8.8.8.8	192.168.2.4
Feb 22, 2021 22:48:23.128050089 CET	59794	53	192.168.2.4	8.8.8.8
Feb 22, 2021 22:48:23.184580088 CET	55916	53	192.168.2.4	8.8.8.8
Feb 22, 2021 22:48:23.185147047 CET	53	59794	8.8.8.8	192.168.2.4
Feb 22, 2021 22:48:23.243113995 CET	53	55916	8.8.8.8	192.168.2.4
Feb 22, 2021 22:48:33.051295042 CET	52752	53	192.168.2.4	8.8.8.8
Feb 22, 2021 22:48:33.102930069 CET	53	52752	8.8.8.8	192.168.2.4
Feb 22, 2021 22:48:33.415774107 CET	60542	53	192.168.2.4	8.8.8.8
Feb 22, 2021 22:48:33.489891052 CET	53	60542	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 22:48:38.097318888 CET	60689	53	192.168.2.4	8.8.8.8
Feb 22, 2021 22:48:38.157083988 CET	53	60689	8.8.8.8	192.168.2.4
Feb 22, 2021 22:49:11.027713060 CET	64206	53	192.168.2.4	8.8.8.8
Feb 22, 2021 22:49:11.080614090 CET	53	64206	8.8.8.8	192.168.2.4
Feb 22, 2021 22:49:12.815059900 CET	50904	53	192.168.2.4	8.8.8.8
Feb 22, 2021 22:49:12.872108936 CET	53	50904	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 22, 2021 22:47:36.539923906 CET	192.168.2.4	8.8.8.8	0x773c	Standard query (0)	saisas.com.co	A (IP address)	IN (0x0001)
Feb 22, 2021 22:47:38.067205906 CET	192.168.2.4	8.8.8.8	0xc44c	Standard query (0)	sydneybuildingengineers.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 22:47:53.675256968 CET	192.168.2.4	8.8.8.8	0xe8be	Standard query (0)	sydneybuildingengineers.com.au	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 22, 2021 22:47:36.726438046 CET	8.8.8.8	192.168.2.4	0x773c	No error (0)	saisas.com.co		208.91.198.178	A (IP address)	IN (0x0001)
Feb 22, 2021 22:47:38.488632917 CET	8.8.8.8	192.168.2.4	0xc44c	No error (0)	sydneybuildingengineers.com.au		192.169.157.161	A (IP address)	IN (0x0001)
Feb 22, 2021 22:47:54.114592075 CET	8.8.8.8	192.168.2.4	0xe8be	No error (0)	sydneybuildingengineers.com.au		192.169.157.161	A (IP address)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 22, 2021 22:47:37.107716084 CET	208.91.198.178	443	192.168.2.4	49734	CN=cpcalendars.saisas.com.co 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.	Mon Dec 28 15:44:54 CET 2020 Wed Oct 07 21:21:40 CEST 2020	Sun Mar 28 16:44:54 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		
Feb 22, 2021 22:47:37.107953072 CET	208.91.198.178	443	192.168.2.4	49733	CN=cpcalendars.saisas.com.co 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.	Mon Dec 28 15:44:54 CET 2020 Wed Oct 07 21:21:40 CEST 2020	Sun Mar 28 16:44:54 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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 22, 2021 22:47:39.191466093 CET	192.169.157.161	443	192.168.2.4	49736	CN=sydneybuildingengineers.com.au 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	Thu Dec 31 01:00:00 CET 2020 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Thu Apr 01 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		
Feb 22, 2021 22:47:39.192704916 CET	192.169.157.161	443	192.168.2.4	49737	CN=sydneybuildingengineers.com.au 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	Thu Dec 31 01:00:00 CET 2020 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Thu Apr 01 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		
Feb 22, 2021 22:47:54.489181042 CET	192.169.157.161	443	192.168.2.4	49752	CN=sydneybuildingengineers.com.au 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	Thu Dec 31 01:00:00 CET 2020 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Thu Apr 01 01:59:59 CEST 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					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		

Code Manipulations

Statistics

Behavior

System Behavior

Analysis Process: iexplore.exe PID: 6832 Parent PID: 800

General

Start time:	22:47:34
Start date:	22/02/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff7f01a0000
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: 6924 Parent PID: 6832

General

Start time:	22:47:35
Start date:	22/02/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6832 CREDAT:17410 /prefetch:2
Imagebase:	0x1240000
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