ID: 441230
Sample Name: Corona als Dank.docx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 14:54:51
Date: 28/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

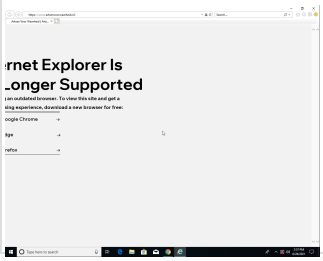
Windows Analysis Report Corona als Dank.docx

Overview

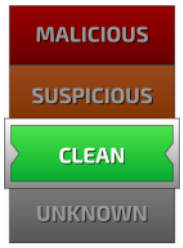
General Information

Sample Name:	Corona als Dank.docx
Analysis ID:	441230
MD5:	a19832a2c9c960..
SHA1:	3f7a955accb1b1a..
SHA256:	44756d412d9244..
Infos:	

Most interesting Screenshot:



Detection

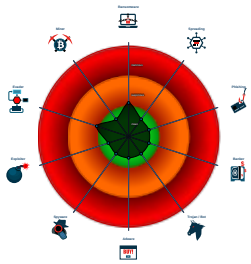


Score:	1
Range:	0 - 100
Whitelisted:	false
Confidence:	60%

Signatures

- IP address seen in connection with o…
- JA3 SSL client fingerprint seen in co…

Classification



Analysis Advice

No malicious behavior found, analyze the document also on other version of Office / Acrobat

Uses HTTPS for network communication, use the 'Proxy HTTPS (port 443) to read its encrypted data' cookbook for further analysis

Process Tree

- **System is w10x64**
- WINWORD.EXE (PID: 7064 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE' /Automation -Embedding MD5: 0B9AB9B9C4DE429473D6450D4297A123)
- iexplore.exe (PID: 984 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6880 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:984 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

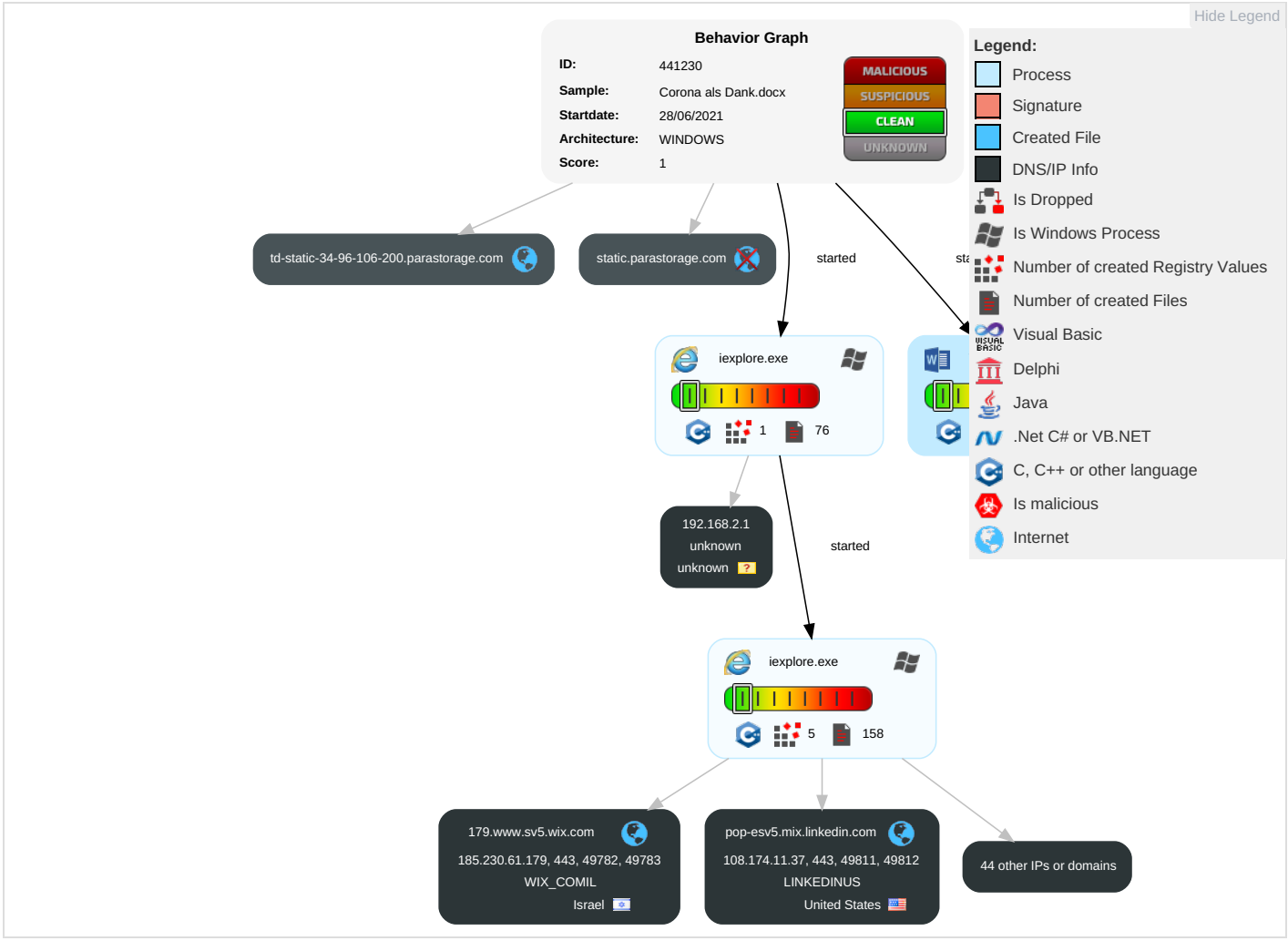
Click to jump to signature section

There are no malicious signatures, click here to show all signatures.

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	Impa
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 Partit
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	System Information Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 2	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Devic Lock
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 3	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delet Devic Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Ingress Tool Transfer 1	SIM Card Swap		Carri Billing Fraud

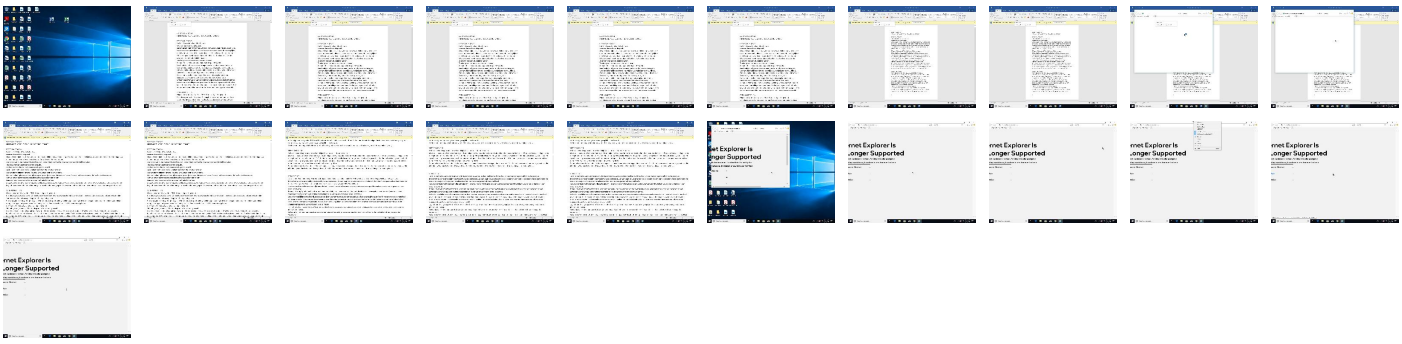
Behavior Graph

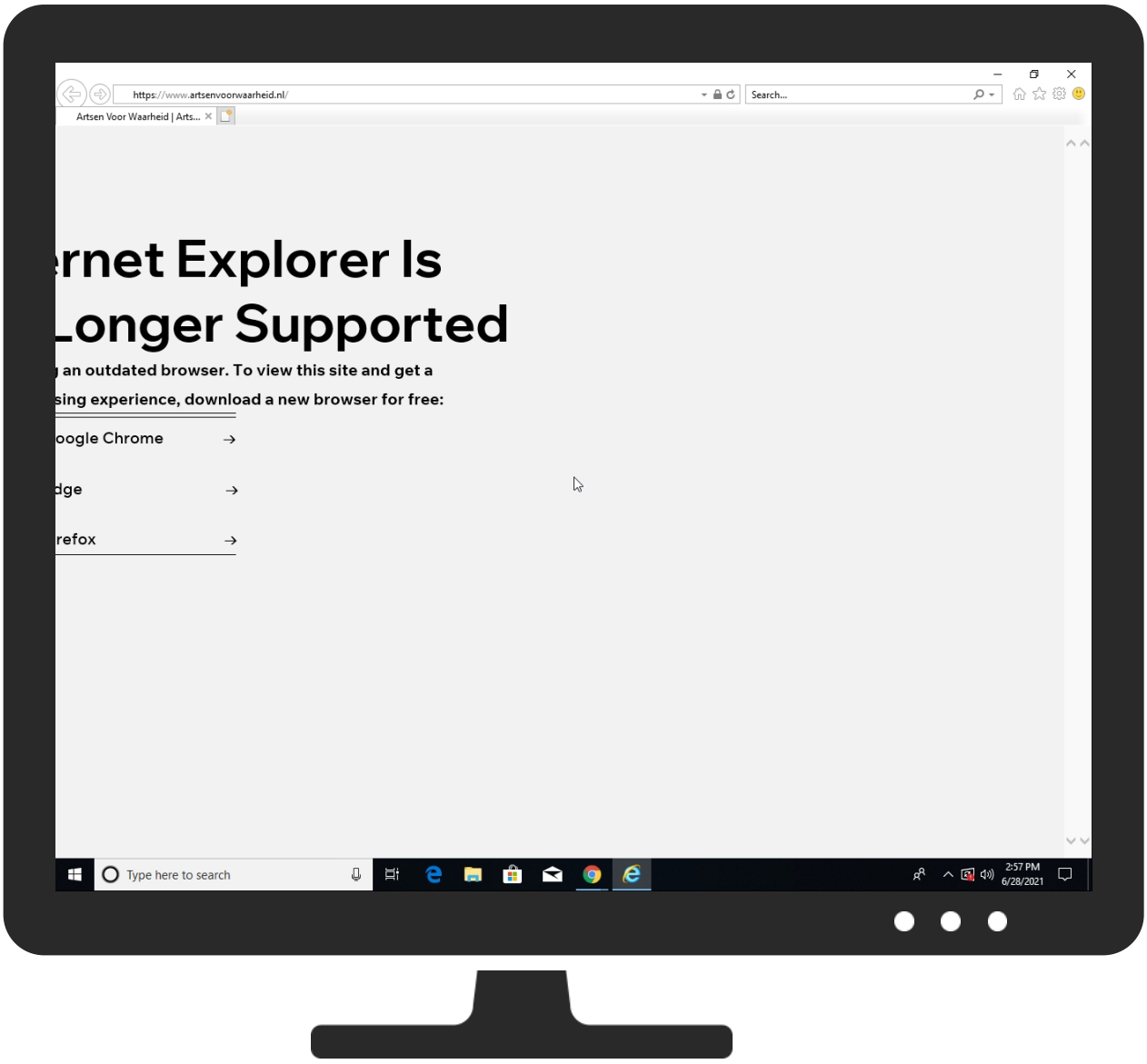


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Corona als Dank.docx	0%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
browser.sentry-cdn.com	0%	Virustotal		Browse
td-balancer-euw2-6-109.wixdns.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://www.deguldenmiddenweg.nl	0%	Avira URL Cloud	safe	
http://polymer.github.io/AUTHORS.txt	0%	Avira URL Cloud	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://www.vaccinvrij.nl	0%	Avira URL Cloud	safe	
http://https://www.artsenvoorwaarheid.nl	0%	Avira URL Cloud	safe	
http://https://openjsf.org/	0%	URL Reputation	safe	
http://https://openjsf.org/	0%	URL Reputation	safe	
http://https://openjsf.org/	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	Avira URL Cloud	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://polymer.github.io/PATENTS.txt	0%	Avira URL Cloud	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://browser.sentry-cdn.com/5.21.4/bundle.min.js	0%	Avira URL Cloud	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://www.artsenvoorwaarheid.nl/Root	0%	Avira URL Cloud	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://www.denieuwewereld.nl	0%	Avira URL Cloud	safe	
http://https://browser.sentry-cdn.com/4.6.2/bundle.min.js	0%	URL Reputation	safe	
http://https://browser.sentry-cdn.com/4.6.2/bundle.min.js	0%	URL Reputation	safe	
http://https://browser.sentry-cdn.com/4.6.2/bundle.min.js	0%	URL Reputation	safe	
http://polymer.github.io/CONTRIBUTORS.txt	0%	Avira URL Cloud	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.google.de	142.250.186.35	true	false		high
star-mini.c10r.facebook.com	157.240.17.35	true	false		high
dart.l.doubleclick.net	142.250.185.198	true	false		high
browser.sentry-cdn.com	151.101.130.217	true	false	• 0%, Virustotal, Browse	unknown
stats.l.doubleclick.net	108.177.15.154	true	false		high
td-balancer-euw2-6-109.wixdns.net	35.246.6.109	true	false	• 0%, Virustotal, Browse	unknown
pop-esv5.mix.linkedin.com	108.174.11.37	true	false		high
gcp.media-router.wixstatic.com	34.102.176.152	true	false		high
179.www.sv5.wix.com	185.230.61.179	true	false		high
fast.fonts.com	104.17.70.188	true	false		high
td-static-34-96-106-200.parastorage.com	34.96.106.200	true	false		high
scontent.xx.fbcdn.net	157.240.17.15	true	false		high
prod.pinterest.global.map.fastly.net	151.101.0.84	true	false		unknown
googleads.g.doubleclick.net	172.217.16.130	true	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
sentry-nlb-e70282e8a06dcc98.elb.us-east-1.amazonaws.com	52.2.188.208	true	false		high
polyfill.io	151.101.1.26	true	false		high
td-username-euw2-6-109.wix.com	35.246.6.109	true	false		high
bi-flogger-alb-ext-343643057.us-east-1.elb.amazonaws.com	54.236.202.140	true	false		high
4382365.fls.doubleclick.net	unknown	unknown	false		high
www.facebook.com	unknown	unknown	false		high
static.wixstatic.com	unknown	unknown	false		high
siteassets.parastorage.com	unknown	unknown	false		high
www.linkedin.com	unknown	unknown	false		high
connect.facebook.net	unknown	unknown	false		high
px.ads.linkedin.com	unknown	unknown	false		high
ct.pinterest.com	unknown	unknown	false		high
en.wix.com	unknown	unknown	false		high
stats.g.doubleclick.net	unknown	unknown	false		high
www.artsenvoorwaarheid.nl	unknown	unknown	false		unknown
frog.wix.com	unknown	unknown	false		high
snap.licdn.com	unknown	unknown	false		high
s.pinimg.com	unknown	unknown	false		high
sentry.wixpress.com	unknown	unknown	false		high
static.parastorage.com	unknown	unknown	false		high
www.wix.com	unknown	unknown	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
108.177.15.154	stats.l.doubleclick.net	United States		15169	GOOGLEUS	false
151.101.0.84	prod.pinterest.global.map.fastly.net	United States		54113	FASTLYUS	false
34.96.106.200	td-static-34-96-106-200.parastorage.com	United States		15169	GOOGLEUS	false
151.101.130.217	browser.sentry-cdn.com	United States		54113	FASTLYUS	false
157.240.17.35	star-mini.c10r.facebook.com	United States		32934	FACEBOOKUS	false
157.240.17.15	scontent.xx.fbcdn.net	United States		32934	FACEBOOKUS	false
35.246.6.109	td-balancer-euw2-6-109.wixdns.net	United States		15169	GOOGLEUS	false
54.236.202.140	bi-flogger-alb-ext-343643057.us-east-1.elb.amazonaws.com	United States		14618	AMAZON-AESUS	false
104.17.70.188	fast.fonts.com	United States		13335	CLOUDFLARENETUS	false
142.250.186.35	www.google.de	United States		15169	GOOGLEUS	false
185.230.61.179	179.www.sv5.wix.com	Israel		58182	WIX_COMIL	false
142.250.185.198	dart.l.doubleclick.net	United States		15169	GOOGLEUS	false
151.101.1.26	polyfill.io	United States		54113	FASTLYUS	false
52.2.188.208	sentry-nlb-e70282e8a06dcc98.elb.us-east-1.amazonaws.com	United States		14618	AMAZON-AESUS	false
34.102.176.152	gcp.media-router.wixstatic.com	United States		15169	GOOGLEUS	false
172.217.16.130	googleads.g.doubleclick.net	United States		15169	GOOGLEUS	false
108.174.11.37	pop-esv5.mix.linkedin.com	United States		14413	LINKEDINUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	441230
Start date:	28.06.2021
Start time:	14:54:51
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 18s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Corona als Dank.docx
Cookbook file name:	defaultwindowsofficecookbook.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
Run name:	Potential for more IOCs and behavior
Number of analysed new started processes analysed:	14
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:	CLEAN
Classification:	clean1.winDOCX@4/142@23/18
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .docx • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Browse link: http://www.artsenvoorwaarheid.nl/ • Scroll down • Close Viewer
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
151.101.0.84	http://marciaconner.com	Get hash	malicious	Browse	• widgets.pinterest.com/v1/urls/count.json?url=http%3A%2F%2Fmarciaconner.com%2F&callback=window._ate.cbs.rcb_fg7e0

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://www.kbpharmacyassociates.com	Get hash	malicious	Browse	• widgets.pinterest.com/v1/urls/count.json?url=https%3A%2F%2Fwww.proweaver.com%2Fcustom-web-design&callback=window._ate.cbs.rcb_m060
	http://www.kbpharmacyassociates.com	Get hash	malicious	Browse	• widgets.pinterest.com/v1/urls/count.json?url=https%3A%2F%2Fwww.proweaver.com%2Fcustom-web-design&callback=window._ate.cbs.rcb_eonr0
	http://https://bit.ly/2KpTKPM	Get hash	malicious	Browse	• pinterest.com/pin/create/button/?url=http://gr8.com/r/N7vJY/E/ySg0m?p=
	http://www.eduwhiz.in/zzz.php	Get hash	malicious	Browse	• www.pinterest.com/
	http://edi-notepad.findmysoft.com/	Get hash	malicious	Browse	• widgets.pinterest.com/v1/urls/count.json?callback=jQuery110207100684983967259_1578981735233&source=6&url=http%3A%2F%2Fmultiple-search-and-replace.findmysoft.com%2Fscreenshot%2F&_=1578981735234
151.101.130.217	Rx_r8wAQ.apk	Get hash	malicious	Browse	
	http://https://xmailexpact.wixsite.com/mysite	Get hash	malicious	Browse	
	http://https://f7569252.sibforms.com/serve/MUIEAB6gs9TNgUd1uwv2_sFLHXTD9tkqU98CT0mNZuxiWHy1lSU0ZPYiM0MrswZnKlAbgxAatWpNamgnfb9geYTOQyQZw6aP5ZrTTUSKm0Es7pBZf6H1qFgWY3rfEmPIgbO-3kDBU7Ea4LCQZzSEz9NQv9b2-pahZUmZVfsWiO-NKmJiUnbihXVcFn4DjCpW7NMbDDDBeWiz9fK	Get hash	malicious	Browse	
	http://https://t.yesware.com/tt/ae9851ab7b578dad1289f08bbf450624f7ae3a45/2ee42987f58d2f32bb36ff11a00dd921/2f4e7e35c28c3b7f4958904f5584a915/joom.ag/2VFC	Get hash	malicious	Browse	
	http://https://infozapyt.wixsite.com/mysite	Get hash	malicious	Browse	
	MOI Support ship V2.docx	Get hash	malicious	Browse	
	http://https://joom.ag/yGUC	Get hash	malicious	Browse	
	http://https://joom.ag/uZDC	Get hash	malicious	Browse	
	http://https://urldefense.com/v3/__https://www.swapcard.com/fr/support/?entity=Attendee__;!!ORetoJg!cvFBCSJtUQP4SxbgyWoSvc6xFbn2Yxso1-ZyBfSCejSXmPOASW6xeeoHHlcA0bUqeo8I$	Get hash	malicious	Browse	
	http://https://view.joomag.com/my-first-publication-voice-message-1/0119891001599758522	Get hash	malicious	Browse	
	New-Fax Gmz1d-0n25sqsw.pdf	Get hash	malicious	Browse	
	http://https://storage.googleapis.com/uir/onee.html	Get hash	malicious	Browse	
	http://www.trumpcarehealthfn.solutions	Get hash	malicious	Browse	
	http://duniamelekitku.blogspot.com	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
pop-esv5.mix.linkedin.com	#U260e#Ufe0fAUDIO-2020-05-26-18-51-m4a_MP4messages_2202-434.htm	Get hash	malicious	Browse	• 108.174.11.37
	ACH WIRE INF0RMATION.xlsx	Get hash	malicious	Browse	• 108.174.11.37
	ACH WIRE INF0RMATION.xlsx	Get hash	malicious	Browse	• 108.174.11.37
	SecuriteInfo.com.XLSX.Onephish.B.genCamelot.17169.xlsx	Get hash	malicious	Browse	• 108.174.11.37
	SecuriteInfo.com.XLSX.Onephish.B.genCamelot.17169.xlsx	Get hash	malicious	Browse	• 108.174.11.37
	551UmZ61Ts.exe	Get hash	malicious	Browse	• 108.174.11.37
	X1(1).xlsm	Get hash	malicious	Browse	• 108.174.11.37
	X1(1).xlsm	Get hash	malicious	Browse	• 108.174.11.37
	CX2 RFQ.xlsm	Get hash	malicious	Browse	• 108.174.11.37
	CX2 RFQ.xlsm	Get hash	malicious	Browse	• 108.174.11.37
	C1.Qoute-Purequest Air Filtration Technologies (Pty) Ltd.xlsm	Get hash	malicious	Browse	• 108.174.11.37
	http://https://drive.google.com/file/d/1RuErynB-YG-0sRvW69ZTOX6Evw4WBZ-U/view	Get hash	malicious	Browse	• 108.174.11.37
browser.sentry-cdn.com	Sleek_Free.exe	Get hash	malicious	Browse	• 151.101.2.217
	http://https://xmailexpact.wixsite.com/mysite	Get hash	malicious	Browse	• 151.101.130.217
	http://catalog.amsz.ua/1.php	Get hash	malicious	Browse	• 151.101.194.217
	http://https://f7569252.sibforms.com/serve/MUIEAB6gs9TNgUd1uwv2_sFLHXTD9tkqU98CT0mNZuxiWHy1lSU0ZPYiM0MrsywZnKlAbgxAatWpNamgnfb9geYTOQyQZw6aP5ZrTTUSKm0Es7pBZf6H1qFgWY3rfEmPIgbO-3kDBU7Ea4LCQZzSEz9NQv9b2-pahZUmZVfsWiO-NKmJiUnbihXVcFn4DjCpW7NMbDDDBeWiz9fK	Get hash	malicious	Browse	• 151.101.130.217
	http://https://t.yesware.com/tt/ae9851ab7b578dad1289f08bbf450624f7ae3a45/2ee42987f58d2f32bb36ff11a00dd921/2f4e7e35c28c3b7f4958904f5584a915/joom.ag/2VFC	Get hash	malicious	Browse	• 151.101.130.217
	http://https://joom.ag/eoFC	Get hash	malicious	Browse	• 151.101.2.217
	http://vcomdesign.com	Get hash	malicious	Browse	• 151.101.194.217
	http://https://joom.ag/3wFC	Get hash	malicious	Browse	• 151.101.2.217
	http://https://joom.ag/qJFC	Get hash	malicious	Browse	• 151.101.2.217
	http://https://joom.ag/BRFC	Get hash	malicious	Browse	• 151.101.2.217
	http://https://samson442.wixsite.com/outlook-web	Get hash	malicious	Browse	• 151.101.2.217
	http://https://infozapyt.wixsite.com/mysite	Get hash	malicious	Browse	• 151.101.130.217
	http://https://brechi5.wixsite.com/owa-webmail-updates	Get hash	malicious	Browse	• 151.101.194.217
	http://https://www.eloi-podiafrance.com/	Get hash	malicious	Browse	• 151.101.2.217
	http://https://www.eloi-podiafrance.com/	Get hash	malicious	Browse	• 151.101.2.217
	http://45.95.168.116	Get hash	malicious	Browse	• 151.101.2.217
	MOI Support ship V2.docx	Get hash	malicious	Browse	• 151.101.2.217
	MOI Support ship V2.docx	Get hash	malicious	Browse	• 151.101.2.217
	MOI Support ship V2.docx	Get hash	malicious	Browse	• 151.101.130.217
	MOI Support ship V2.docx	Get hash	malicious	Browse	• 151.101.66.217

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
FASTLYUS	Test.dll	Get hash	malicious	Browse	• 151.101.1.44
	Spotify_v8.6.26.897_v7a_mod.apk	Get hash	malicious	Browse	• 199.232.138.249
	shippingnote (docs).jar	Get hash	malicious	Browse	• 185.199.110.154
	shippingnote (docs).jar	Get hash	malicious	Browse	• 185.199.108.154
	eex86.dll	Get hash	malicious	Browse	• 151.101.1.44
	8f9b032ff6f56a685f4c6f9eb57784811d6c98aa83b0c.dll	Get hash	malicious	Browse	• 151.101.1.44
	file.dll	Get hash	malicious	Browse	• 151.101.1.44
	CCF06242021_0004.pdf.jar	Get hash	malicious	Browse	• 185.199.111.154
	DC Viet Nam Order list 6-25-21.exe	Get hash	malicious	Browse	• 185.199.108.153

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	1.exe	Get hash	malicious	Browse	• 185.199.110.133
	Ln11IgJVUM.dll	Get hash	malicious	Browse	• 151.101.1.44
	6c710694d270db91b550daf3177622514d2444e7484fb.dll	Get hash	malicious	Browse	• 151.101.1.44
	OQgRyt6hCF.exe	Get hash	malicious	Browse	• 185.199.110.133
	microA.exe	Get hash	malicious	Browse	• 185.199.109.133
	Invoice_634000.html	Get hash	malicious	Browse	• 151.101.129.49
	Trackingdetails202106168387483.jar	Get hash	malicious	Browse	• 185.199.110.154
	Nueva orden de env#U00edo .exe	Get hash	malicious	Browse	• 185.199.111.133
	PurchaseOrderDetails1.jar	Get hash	malicious	Browse	• 185.199.110.154
	kT5DnSYEI2.dll	Get hash	malicious	Browse	• 151.101.1.44
	9TW5TjqwON.dll	Get hash	malicious	Browse	• 151.101.1.44
FASTLYUS	Test.dll	Get hash	malicious	Browse	• 151.101.1.44
	Spotify_v8.6.26.897_v7a_mod.apk	Get hash	malicious	Browse	• 199.232.138.249
	shippingnote (docs).jar	Get hash	malicious	Browse	• 185.199.110.154
	shippingnote (docs).jar	Get hash	malicious	Browse	• 185.199.108.154
	eex86.dll	Get hash	malicious	Browse	• 151.101.1.44
	8f9b032ff6f56a685f4c6f9eb57784811d6c98aa83b0c.dll	Get hash	malicious	Browse	• 151.101.1.44
	file.dll	Get hash	malicious	Browse	• 151.101.1.44
	CCF06242021_0004.pdf.jar	Get hash	malicious	Browse	• 185.199.111.154
	DC Viet Nam Order list 6-25-21.exe	Get hash	malicious	Browse	• 185.199.108.153
	1.exe	Get hash	malicious	Browse	• 185.199.110.133
	Ln11IgJVUM.dll	Get hash	malicious	Browse	• 151.101.1.44
	6c710694d270db91b550daf3177622514d2444e7484fb.dll	Get hash	malicious	Browse	• 151.101.1.44
	OQgRyt6hCF.exe	Get hash	malicious	Browse	• 185.199.110.133
	microA.exe	Get hash	malicious	Browse	• 185.199.109.133
	Invoice_634000.html	Get hash	malicious	Browse	• 151.101.129.49
	Trackingdetails202106168387483.jar	Get hash	malicious	Browse	• 185.199.110.154
	Nueva orden de env#U00edo .exe	Get hash	malicious	Browse	• 185.199.111.133
	PurchaseOrderDetails1.jar	Get hash	malicious	Browse	• 185.199.110.154
	kT5DnSYEI2.dll	Get hash	malicious	Browse	• 151.101.1.44
	9TW5TjqwON.dll	Get hash	malicious	Browse	• 151.101.1.44

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
9e10692f1b7f78228b2d4e424db3a98c	sample_payment.html	Get hash	malicious	Browse	• 108.177.15.154 • 142.250.186.35 • 151.101.0.84 • 185.230.61.179 • 34.96.106.200 • 142.250.185.198 • 151.101.1.26 • 151.101.130.217 • 157.240.17.35 • 157.240.17.15 • 52.2.188.208 • 35.246.6.109 • 54.236.202.140 • 34.102.176.152 • 104.17.70.188 • 172.217.16.130 • 108.174.11.37

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	hy2x7ex1Ny.exe	Get hash	malicious	Browse	• 108.177.15.154 • 142.250.186.35 • 151.101.0.84 • 185.230.61.179 • 34.96.106.200 • 142.250.185.198 • 151.101.1.26 • 151.101.130.217 • 157.240.17.35 • 157.240.17.15 • 52.2.188.208 • 35.246.6.109 • 54.236.202.140 • 34.102.176.152 • 104.17.70.188 • 172.217.16.130 • 108.174.11.37
	6nNxvZ2syK.exe	Get hash	malicious	Browse	• 108.177.15.154 • 142.250.186.35 • 151.101.0.84 • 185.230.61.179 • 34.96.106.200 • 142.250.185.198 • 151.101.1.26 • 151.101.130.217 • 157.240.17.35 • 157.240.17.15 • 52.2.188.208 • 35.246.6.109 • 54.236.202.140 • 34.102.176.152 • 104.17.70.188 • 172.217.16.130 • 108.174.11.37
	nO928Cerv8.exe	Get hash	malicious	Browse	• 108.177.15.154 • 142.250.186.35 • 151.101.0.84 • 185.230.61.179 • 34.96.106.200 • 142.250.185.198 • 151.101.1.26 • 151.101.130.217 • 157.240.17.35 • 157.240.17.15 • 52.2.188.208 • 35.246.6.109 • 54.236.202.140 • 34.102.176.152 • 104.17.70.188 • 172.217.16.130 • 108.174.11.37
	ILQyJ80qCs.exe	Get hash	malicious	Browse	• 108.177.15.154 • 142.250.186.35 • 151.101.0.84 • 185.230.61.179 • 34.96.106.200 • 142.250.185.198 • 151.101.1.26 • 151.101.130.217 • 157.240.17.35 • 157.240.17.15 • 52.2.188.208 • 35.246.6.109 • 54.236.202.140 • 34.102.176.152 • 104.17.70.188 • 172.217.16.130 • 108.174.11.37

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	eex86.dll	Get hash	malicious	Browse	• 108.177.15.154 • 142.250.186.35 • 151.101.0.84 • 185.230.61.179 • 34.96.106.200 • 142.250.18 5.198 • 151.101.1.26 • 151.101.13 0.217 • 157.240.17.35 • 157.240.17.15 • 52.2.188.208 • 35.246.6.109 • 54.236.202.140 • 34.102.176.152 • 104.17.70.188 • 172.217.16.130 • 108.174.11.37
	Wilson-McShane Corporation ACH.xlsx	Get hash	malicious	Browse	• 108.177.15.154 • 142.250.186.35 • 151.101.0.84 • 185.230.61.179 • 34.96.106.200 • 142.250.18 5.198 • 151.101.1.26 • 151.101.13 0.217 • 157.240.17.35 • 157.240.17.15 • 52.2.188.208 • 35.246.6.109 • 54.236.202.140 • 34.102.176.152 • 104.17.70.188 • 172.217.16.130 • 108.174.11.37
	8f9b032ff6f56a685f4c6f9eb57784811d6c98aa83b0c.dll	Get hash	malicious	Browse	• 108.177.15.154 • 142.250.186.35 • 151.101.0.84 • 185.230.61.179 • 34.96.106.200 • 142.250.18 5.198 • 151.101.1.26 • 151.101.13 0.217 • 157.240.17.35 • 157.240.17.15 • 52.2.188.208 • 35.246.6.109 • 54.236.202.140 • 34.102.176.152 • 104.17.70.188 • 172.217.16.130 • 108.174.11.37
	file.dll	Get hash	malicious	Browse	• 108.177.15.154 • 142.250.186.35 • 151.101.0.84 • 185.230.61.179 • 34.96.106.200 • 142.250.18 5.198 • 151.101.1.26 • 151.101.13 0.217 • 157.240.17.35 • 157.240.17.15 • 52.2.188.208 • 35.246.6.109 • 54.236.202.140 • 34.102.176.152 • 104.17.70.188 • 172.217.16.130 • 108.174.11.37

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	ATT96412.html	Get hash	malicious	Browse	• 108.177.15.154 • 142.250.186.35 • 151.101.0.84 • 185.230.61.179 • 34.96.106.200 • 142.250.185.198 • 151.101.1.26 • 151.101.130.217 • 157.240.17.35 • 157.240.17.15 • 52.2.188.208 • 35.246.6.109 • 54.236.202.140 • 34.102.176.152 • 104.17.70.188 • 172.217.16.130 • 108.174.11.37
	sf0X1hMF0g.doc	Get hash	malicious	Browse	• 108.177.15.154 • 142.250.186.35 • 151.101.0.84 • 185.230.61.179 • 34.96.106.200 • 142.250.185.198 • 151.101.1.26 • 151.101.130.217 • 157.240.17.35 • 157.240.17.15 • 52.2.188.208 • 35.246.6.109 • 54.236.202.140 • 34.102.176.152 • 104.17.70.188 • 172.217.16.130 • 108.174.11.37
	Wilson-McShane Corporation ACH.xlsx	Get hash	malicious	Browse	• 108.177.15.154 • 142.250.186.35 • 151.101.0.84 • 185.230.61.179 • 34.96.106.200 • 142.250.185.198 • 151.101.1.26 • 151.101.130.217 • 157.240.17.35 • 157.240.17.15 • 52.2.188.208 • 35.246.6.109 • 54.236.202.140 • 34.102.176.152 • 104.17.70.188 • 172.217.16.130 • 108.174.11.37
	1.exe	Get hash	malicious	Browse	• 108.177.15.154 • 142.250.186.35 • 151.101.0.84 • 185.230.61.179 • 34.96.106.200 • 142.250.185.198 • 151.101.1.26 • 151.101.130.217 • 157.240.17.35 • 157.240.17.15 • 52.2.188.208 • 35.246.6.109 • 54.236.202.140 • 34.102.176.152 • 104.17.70.188 • 172.217.16.130 • 108.174.11.37

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Ln11IgJVUM.dll	Get hash	malicious	Browse	• 108.177.15.154 • 142.250.186.35 • 151.101.0.84 • 185.230.61.179 • 34.96.106.200 • 142.250.185.198 • 151.101.1.26 • 151.101.130.217 • 157.240.17.35 • 157.240.17.15 • 52.2.188.208 • 35.246.6.109 • 54.236.202.140 • 34.102.176.152 • 104.17.70.188 • 172.217.16.130 • 108.174.11.37
	6c710694d270db91b550daf3177622514d2444e7484fb.dll	Get hash	malicious	Browse	• 108.177.15.154 • 142.250.186.35 • 151.101.0.84 • 185.230.61.179 • 34.96.106.200 • 142.250.185.198 • 151.101.1.26 • 151.101.130.217 • 157.240.17.35 • 157.240.17.15 • 52.2.188.208 • 35.246.6.109 • 54.236.202.140 • 34.102.176.152 • 104.17.70.188 • 172.217.16.130 • 108.174.11.37
	OQgRyt6hCF.exe	Get hash	malicious	Browse	• 108.177.15.154 • 142.250.186.35 • 151.101.0.84 • 185.230.61.179 • 34.96.106.200 • 142.250.185.198 • 151.101.1.26 • 151.101.130.217 • 157.240.17.35 • 157.240.17.15 • 52.2.188.208 • 35.246.6.109 • 54.236.202.140 • 34.102.176.152 • 104.17.70.188 • 172.217.16.130 • 108.174.11.37
	DocuSign-June-SOA-Dues.261.htm	Get hash	malicious	Browse	• 108.177.15.154 • 142.250.186.35 • 151.101.0.84 • 185.230.61.179 • 34.96.106.200 • 142.250.185.198 • 151.101.1.26 • 151.101.130.217 • 157.240.17.35 • 157.240.17.15 • 52.2.188.208 • 35.246.6.109 • 54.236.202.140 • 34.102.176.152 • 104.17.70.188 • 172.217.16.130 • 108.174.11.37

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Invoice 715320 paul@forthebiome.com.html	Get hash	malicious	Browse	• 108.177.15.154 • 142.250.186.35 • 151.101.0.84 • 185.230.61.179 • 34.96.106.200 • 142.250.185.198 • 151.101.1.26 • 151.101.130.217 • 157.240.17.35 • 157.240.17.15 • 52.2.188.208 • 35.246.6.109 • 54.236.202.140 • 34.102.176.152 • 104.17.70.188 • 172.217.16.130 • 108.174.11.37
	HSBC_Payment_slip_for Outstanding 001005l.htm	Get hash	malicious	Browse	• 108.177.15.154 • 142.250.186.35 • 151.101.0.84 • 185.230.61.179 • 34.96.106.200 • 142.250.185.198 • 151.101.1.26 • 151.101.130.217 • 157.240.17.35 • 157.240.17.15 • 52.2.188.208 • 35.246.6.109 • 54.236.202.140 • 34.102.176.152 • 104.17.70.188 • 172.217.16.130 • 108.174.11.37
	microA.exe	Get hash	malicious	Browse	• 108.177.15.154 • 142.250.186.35 • 151.101.0.84 • 185.230.61.179 • 34.96.106.200 • 142.250.185.198 • 151.101.1.26 • 151.101.130.217 • 157.240.17.35 • 157.240.17.15 • 52.2.188.208 • 35.246.6.109 • 54.236.202.140 • 34.102.176.152 • 104.17.70.188 • 172.217.16.130 • 108.174.11.37
37f463bf4616ecd445d4a1937da06e19	Dfdvfczl_Signed_.exe	Get hash	malicious	Browse	• 34.96.106.200
	9irkb5Rbn8.exe	Get hash	malicious	Browse	• 34.96.106.200
	kgx2fkTmpa.exe	Get hash	malicious	Browse	• 34.96.106.200
	6DFppWx7eK.exe	Get hash	malicious	Browse	• 34.96.106.200
	5EHqnAyk4E.exe	Get hash	malicious	Browse	• 34.96.106.200
	IZNzZi2xvv.exe	Get hash	malicious	Browse	• 34.96.106.200
	6xlaisUIXn.exe	Get hash	malicious	Browse	• 34.96.106.200
	LnsathwafhvylbbptobwoppapjxmujmvteSigned.exe	Get hash	malicious	Browse	• 34.96.106.200
	2dd214b7750c889a14bb6c1be4ff3b32e1bce2fba8d27.exe	Get hash	malicious	Browse	• 34.96.106.200
	GGOz8MeRsD.exe	Get hash	malicious	Browse	• 34.96.106.200
	wUObTX8Yfm.exe	Get hash	malicious	Browse	• 34.96.106.200
	6nNxvZ2syK.exe	Get hash	malicious	Browse	• 34.96.106.200
	nO928Cerv8.exe	Get hash	malicious	Browse	• 34.96.106.200
	1wXELgiTgk.exe	Get hash	malicious	Browse	• 34.96.106.200
	0Xm0BoIbqZ.exe	Get hash	malicious	Browse	• 34.96.106.200
	sjZr8Zavm6.exe	Get hash	malicious	Browse	• 34.96.106.200
	ILQyJ80qCs.exe	Get hash	malicious	Browse	• 34.96.106.200
	Gnqavfhmcsecxlwdiltkkverstraextmrm.exe	Get hash	malicious	Browse	• 34.96.106.200
	Hard.Disk.Sentinel.Pro.5.61.14.Beta.Portable_Downloadly.ir.exe	Get hash	malicious	Browse	• 34.96.106.200
	Wilson-McShane Corporation ACH.xlsx	Get hash	malicious	Browse	• 34.96.106.200

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\E5F0NRSV\www.wix[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1948
Entropy (8bit):	5.0958906788683676
Encrypted:	false
SSDEEP:	48:Ldsdsdsdcsdcp3sdcp3LKhsdcp3LKhu+XF:ZMMMcMcp3Mcp34Mcp34ugF
MD5:	471698C1EC6DE4E721C41E66CD192C7F
SHA1:	4210A0F8A4FFAB5255B2C70CE55F73C7118171A4
SHA-256:	B703FA116B2EE4CB497644200ADB1FF6DFBD59F7031E75CCFA4C04EE192B5B91
SHA-512:	28A0E0C39609E7A71B103720E6B18640F28E74199DEB9646DB270F8E5463A06B224B05853FF919D77FBE44FE9A5D01F0659B373A4F87237BC9EEA9FF5936B3E3
Malicious:	false
Reputation:	low
Preview:	<root></root><root><item name="fedops.logger.sessionId" value="bcedb989-b024-478e-8604-7a7ec277dfe1" ltime="4196656928" htime="30895132" /></root><root><item name="fedops.logger.sessionId" value="bcedb989-b024-478e-8604-7a7ec277dfe1" ltime="4196656928" htime="30895132" /></root><root><item name="fedops.logger.sessionId" value="bcedb989-b024-478e-8604-7a7ec277dfe1" ltime="4196656928" htime="30895132" /></root><root><item name="fedops.logger.sessionId" value="bcedb989-b024-478e-8604-7a7ec277dfe1" ltime="4196656928" htime="30895132" /><item name="_uetsid" value="3c59f9b0d81011eb9d35df070fd534af" ltime="4263076928" htime="30895132" /></root><root><item name="fedops.logger.sessionId" value="bcedb989-b024-478e-8604-7a7ec277dfe1" ltime="4196656928" htime="30895132" /><item name="_uetsid" value="3c59f9b0d81011eb9d35df070fd534af" ltime="4263076928" htime="30895132" /><item name="_uetsid_exp" value="Tue, 29 Jun 2021 12:56:20 GMT" ltime="4263076928" htime="30895132" /></root><root><item name="fed

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{33226EEC-D810-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	33368
Entropy (8bit):	1.8689526945979371
Encrypted:	false
SSDEEP:	192:rprZjOTZfv2UsWEdtSif29jzMmLB0xD8LB3yta90j3:rza1Wws7XK4U6F
MD5:	D59C02ACFA40AE0DB78A72464271DB82
SHA1:	ECB7C7786588DC5D5369F0185D7026ED651A4E66
SHA-256:	9F2D7ACE3A7D1BD9D4B686F00D2A13A659864030DD4804BBF2CD7EBAD5E4CBC7
SHA-512:	1A1D0EBADD007837246003E63004568C729F49FA3CD8FE790E8CFDD755FF81F2EFD73D0DC4CA65143B747EA209463EF4A7B3FFBC67DFEB99764F594D5DBDB63
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\{33226EEE-D810-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	26256
Entropy (8bit):	1.6607215936484394
Encrypted:	false
SSDEEP:	48:IwiGcprtZGwpafG4pQLGrapbSXGQpBKGHHpcH7TGUp8+GzYpm8VGopCOJLPUXGWd:rWZtTQx6/BShjR21WyMCIC47fWA
MD5:	FC899A48F9568D8F592FD3C3A7CC1AED
SHA1:	BD06638A4683DE208A10B8D55568FC07BDF46DE3
SHA-256:	6743923F241D4A4CD749C01CDE70343D812AB928F479D390E7276142CEC1CA0A
SHA-512:	634D0D4F3AD770D5BB44D87E1731C66B4A72AED01FC5835B9E6E321DD72F03EE16809A09862D3D4C277285B2C5723D74ADA0AE70F0DB42221D7B4B21585EC8A
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{33226EEE-D810-11EB-90EB-ECF4BBEA1588}.dat	
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{4AA920AE-D810-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5632639740180536
Encrypted:	false
SSDEEP:	48:Iw+Gcpr9ZGwpamG4pQmGrapbS8GQpK+G7HpR7TGIpG:riZ9TQW6oBSUA5TxA
MD5:	9E913029FB66178F521489BAF83B0DA8
SHA1:	1E9468AADC215FC405EF3B9BF5BE6BBD11118F6D
SHA-256:	9AF529EF5143C5AD249F285CBC76F9EC29ADBB3D9FFEDD0E890B0D74C84A3C3B
SHA-512:	6B47DF0FA4339584069FF136722C7AD82E3EF2A0F52656C940AF371A93E33979569BC35FF289DBDA1A67E9536AF1189B4B28CB9B64490E49DAEBE982D3037176
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):	5.073933070498012
Encrypted:	false
SSDEEP:	12:TMHdNMNxOEBs2nWimI002EtM3MHdNMNxOEB5l4nWimI00OYGVbkEtMb:2d6NxOMs2SZHKd6NxOM74SZ7YLb
MD5:	2AD4B7AD53E7A715D6E9516A7E1DBE0B
SHA1:	83FB2016D8FC230156BE819D10DD77A205B9829B
SHA-256:	858751B63F395808593250383E750213DFAE68F650D6193A3490C3E4938322DC
SHA-512:	040ED6EBDBC4AA61039DC8B8318FD55018A27DEE2D4BCE65D35FE6EEE473AE34DD7217EA92D1F1B01848D77941A8CF6227A0C97BBF5065637D5D7BE628463E CF
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x0b07e4a2,0x01d76c1d</date>< accdate>0x0b07e4a2,0x01d76c1d</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>0x0b07e4a2,0x01d76c1d</date><accdate>0 x0b0f0b93,0x01d76c1d</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):	5.094293582827584
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kBs2nWimI002EtM3MHdNMNxe2kBs2nWimI00OYGkak6EtMb:2d6Nxrss2SZHKd6Nxrss2SZ7Yza7b
MD5:	064F4F2C41FBCA747A494865BBB3AA97
SHA1:	544534C26B670094B68A76D21C8165A3E18E519F
SHA-256:	44A1BF9C877E271D0BD69CB5A124C7FEBF401E2D037C0FD576E6461180943591
SHA-512:	2DFFD64D74DB82BDED2E4C59145402DB2B1FBB5E404710245622D367AB765FA0DBC7406AC4341B965399FFBEB6778BBD915D214BDB240CB12BD30A7986FAC0 04
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x0b07e4a2,0x01d76c1d</date><a ccdate>0x0b07e4a2,0x01d76c1d</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>0x0b07e4a2,0x01d76c1d</date><a ccdate>0x0b07e4a2,0x01d76c1d</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Am azon.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):	5.078875372258253
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLWlnl4nWimI002EtM3MHdNMNxvLWlnl4nWimI00OYGmZEtMb:2d6Nxvul4SZHKd6Nxvul4SZ7Yjb
MD5:	5B324B788829882667D593B3D1F54EB9
SHA1:	7B12C7D762E52C204C0C7F7882C0825488252B51
SHA-256:	775CB618D97069F71E0E6002BF9402029740CBF65F8F5A5680B318415F9B707E
SHA-512:	5EDC0571E3E3330900F89025C502AE37BBA1B5F60046A32E2D36247D42006CF9E9D0443868129829F877ACE281A2721291460D49FA85770BDE76A2F376A408E1
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x0b0f0b93,0x01d76c1d</date><accdate>0x0b0f0b93,0x01d76c1d</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>0x0b0f0b93,0x01d76c1d</date><accdate>0x0b0f0b93,0x01d76c1d</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):	5.082466655821792
Encrypted:	false
SSDEEP:	12:TMHdNMNxiBs2nWimI002EtM3MHdNMNxiBs2nWimI00OYGd5EtMb:2d6NxSs2SZHKd6NxSs2SZ7YEjb
MD5:	5079A2347A53C744808C42BEE6BDC9D6
SHA1:	2328D7DBA4BC463556D447ADBF43287406E1FD1C
SHA-256:	5BB865DBC699595D96CA62A03D6785A88DB8C63ADF001BCD846E4C05ECF6F19C
SHA-512:	7E25E437FB83EBBF78599E0240D1413BDCDA02469F5B14376C401B23DC714B3454E882966BF42065BFCC006901F35C3486E8A9A95DF04A9F1CA1BB19CF978D1
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x0b07e4a2,0x01d76c1d</date><accdate>0x0b07e4a2,0x01d76c1d</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>0x0b07e4a2,0x01d76c1d</date><accdate>0x0b07e4a2,0x01d76c1d</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):	5.08789821895142
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwWlnl4nWimI002EtM3MHdNMNxhGwWlnl4nWimI00OYG8K075EtMb:2d6NxQnl4SZHKd6NxQnl4SZ7YrKajb
MD5:	9767F070CA5D8671F87AA3D81D808278
SHA1:	A953C8C95C60A5A6BE3775B7E8DCCA2F07B12BF6
SHA-256:	DEE55A24ABA08B6D15141D678D69AB2D1422BA017BA1C813128C6713587CCF32
SHA-512:	4294FF535E6075050B984F11B54BEBC931C40A4B937C75B90061D546C726871885226FC41193488D44990D64AD49C6C467AE566AA8CBB4D6FED8E9585503BB72
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x0b0f0b93,0x01d76c1d</date><accdate>0x0b0f0b93,0x01d76c1d</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>0x0b0f0b93,0x01d76c1d</date><accdate>0x0b0f0b93,0x01d76c1d</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):	5.068463911353802
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml	
SSDEEP:	12:TMHdNMNx0nBs2nWimI002EtM3MHdNMNx0nBs2nWimI00OYGxEtMb:2d6Nx0Bs2SZHKd6Nx0Bs2SZ7Ygb
MD5:	41552A5402340A74FF77A52EB67F71FB
SHA1:	0C6F2563D56A12F6321F2DBFDF51B33DC53482F3
SHA-256:	6CF7BD275839A7749D1D7DDAD54C037513A7F08F9A86C7210966C5E3B41D6594
SHA-512:	4FEB4CFE5EF2F475F330C849F4C5DAC09E886547CB6E5787642954C6E9A9963F64A61887D32F0C6565BC16B2002D3F5606CE708085A8519C585E761A4AB45A80
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x0b07e4a2,0x01d76c1d</date><accdate>0x0b07e4a2,0x01d76c1d</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>0x0b07e4a2,0x01d76c1d</date><accdate>0x0b07e4a2,0x01d76c1d</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):	5.10700930778864
Encrypted:	false
SSDEEP:	12:TMHdNMNxxBs2nWimI002EtM3MHdNMNxxBs2nWimI00OYG6Kq5EtMb:2d6NxTs2SZHKd6NxTs2SZ7Yhb
MD5:	1013D1E56EDA4E9F880D0F3FFAD65342
SHA1:	AF800D3776AD12EC81B5DBAE886E1CC931BC7290
SHA-256:	596234CDB02C1DFA1B3AE4C143C0B2D16CE59274E6E2EB0A734D854DE468E350
SHA-512:	820F01CD9580522163FC1C1656ED70EF3CC83393D16852174E02B83E0105447390EEAEC9BA4AAADF7502F7AF365AAF0E8F3283EDCA3E5BF75CFE65A31C6C79A1
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x0b07e4a2,0x01d76c1d</date><accdate>0x0b07e4a2,0x01d76c1d</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>0x0b07e4a2,0x01d76c1d</date><accdate>0x0b07e4a2,0x01d76c1d</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):	5.083339404467366
Encrypted:	false
SSDEEP:	12:TMHdNMNxcBs2nWimI002EtM3MHdNMNxcBs2nWimI00OYGVEtMb:2d6Nx0s2SZHKd6Nx0s2SZ7Ykb
MD5:	E77437E614E243A42EBF6075DCB508D8
SHA1:	D95FF0BEBD0E14932EE7A8AEF5CEA5DB59AD69A2
SHA-256:	34DBBD963392E9918E792D652538344AA26CBB5A9A314061C73BB6758724A4F6
SHA-512:	4CA9C491C5F1EE0BED1DCA415979FB3F626356B036B2A8A18F0E55AD100AB4C6C20497991C3A2759C6431FD5612E7FE7954F95C7E8A99AD32347A1F5947A448
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x0b07e4a2,0x01d76c1d</date><accdate>0x0b07e4a2,0x01d76c1d</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>0x0b07e4a2,0x01d76c1d</date><accdate>0x0b07e4a2,0x01d76c1d</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):	5.068057272370217
Encrypted:	false
SSDEEP:	12:TMHdNMNxfnBs2nWimI002EtM3MHdNMNxfnBs2nWimI00OYGe5EtMb:2d6NxJs2SZHKd6NxJs2SZ7YLjb
MD5:	03FB829AFF9543EBBD9D118CEC38430D
SHA1:	1807B7FDD09E72C8705349B6EF6324D6B16FDCF5
SHA-256:	83FC0E77EDDC657E2638DF3DBB72545F828A138BAA089BB5BA604490D7B12701

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml	
SHA-512:	059E8A644FDFBD906A5FDBBFFCC533C62BE8F594A234290DB12D1BF99EC253958FA98B617ED7582E14E13932D34B4197120F9FCFB9AFECE46153B243A18C7E5 5
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x0b07e4a2,0x01d76c1d</date><a ccdate>0x0b07e4a2,0x01d76c1d</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>0x0b07e4a2,0x01d76c1d</date><a ccdate>0x0b07e4a2,0x01d76c1d</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Go ogle.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):	1286
Entropy (8bit):	1.7635904022975755
Encrypted:	false
SSDEEP:	6:tYmRMhZTMic8ReJq55555555555555pllRS/:amEtg8ReJq55555555555555pl+
MD5:	FB953C9F39863E219A3068FF8B1F53AB
SHA1:	5536811E211DE796B8748F3EF59B7E89878FC7AC
SHA-256:	50E1911BA225A06E2B09BF2C5F0AF45BAEBC73F988D66E94CD1AA8FA4304CA3F
SHA-512:	DCB31B5E4B89B1F8E96FB6262CBFD9E359BEBB03884A85CE70A443F2EB6CCAF28937417C7D54FBE74BDE259FF13F1041F765AD33B97DE653E34536FB8F8444 A
Malicious:	false
Preview:	1.h.t.t.p.s.:./.s.t.a.t.i.c...p.a.r.a.s.t.o.r.a.g.e...c.o.m./.c.l.i.e.n.t./.p.f.a.v.i.c.o...i.c.o.~..... .h.....(..... ....@..... ....

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\EEDCAF9D-BC91-4C9F-8B50-94E1F85D3771	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	135189
Entropy (8bit):	5.363312697455771
Encrypted:	false
SSDEEP:	1536:mcQIKNgeBTA3gBwlpQ9DQW+z7Y34ZliKWXboOidX5E6LWME9:AEQ9DQW+zvXO1
MD5:	AF6FDF0BC10F32E5CC619B6F0D741570
SHA1:	A81F09549CF784FA9163ABA70D4314B494CDDB62
SHA-256:	E63976393808D13B2B4EB7643B6DAB9797AFF55BBE063B6A221644DA76A98A32
SHA-512:	F39C5EE99C54A8A09AD5EFA1B5F780D9EF357E56FE3FD6C838EBD23A5CC7FC31184F7E7A18CC78BE2A815E9F5211BE27D6040A414473B88759040848D754C71
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2021-06-28T12:55:37">.. Build: 16.0.14223.30528-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:u rl>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{D684EC2D-73DF-439F-B61F-60005178369F}.tmp	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	1.3655810646434015
Encrypted:	false
SSDEEP:	6:Iiiiiiiiii8l+4V/Nc8++ldL61DX6tD6pV2E6ll:23dNG+PmBqZ6pV2p3
MD5:	2A611A2E2E412FC73785E4048501F65B
SHA1:	7720D6FB86B9B943EA9C6E690BA6F2394B0D084C
SHA-256:	2314AB1A0D3242E36B6A0352EF5FE8318D395A818EA1A947F010C7A63E1819AE
SHA-512:	471C33543229793CF990C51CE945A6395A4B8F213DD75936F4800CC46CC1968000F9C22DE2040CA28ACDB3A5135D63F2557D6D40F1BE389DCDCE71B541A3362
Malicious:	false
Preview:	..(...(...(...(...(...(...(...(...(...(...p.r.a.t.e.s.h...p..... ...."...&...*.....>...B..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{E3818052-BF02-4A3F-98E6-061521D6460F}.tmp	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	273726
Entropy (8bit):	3.9493878587902347
Encrypted:	false
SSDEEP:	3072:Hiw5cNPQWp0zsno7vJsHQV4LCjDhzUc8dKHAv3fbYmfEiY7sW0XPECh3YaGDaj3Y:5Z
MD5:	88ED780A37B17DFB1A0AFB601CA08579
SHA1:	EE28D68357B4B02FDA017B455C86A2F9A35033C9
SHA-256:	637EC231B766204FCD6AE73DF4C646B507387561B2440D756110D66DD60A5B7B
SHA-512:	3968E193B4984135C791EF70A915D3DF4B7A263114CEB360938020F38A0C529F3095CC9E81D3C9987349100145B8BF567DB3195018E156EAB1912AC80A50FE5D
Malicious:	false
Preview:	..... .!."#.$.%.&.'.(.).*.+.,.-.../.0.1.2.3.4.5.6.7.8.9.:.;.<.=.>.....C.O.R.O.N.A. .A.L.S. .D.A.N.K.!...I.N.F.O.R.M.A.T.I.E. . . .V.O.O. R.L.I.C.H.T.I.N.G. . . .H.A.N.D.R.E.I.K.I.N.G. . . .O.P.R.O.E.P....C.O.R.O.N.A. .A.L.S. .D.A.N.K.?. ...D.a.t. .k.l.i.n.k.t. .s.c.h.o.k.k.e.n.d. .e.n. .d.a.t. .i.s. .h.e.t. .o.o.k.....W.a.a. r.o.m. .d.a.n. .t.o.c.h. .d.i.e. .u.i.t.s.p.r.a.a.k.....L.i.e.v.e. .m.e.n.s.e.n. .m.i.j.n. .h.a.r.t. .....:.....|.....P.....*..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{F1638333-2616-4E62-9212-B870D6F1A23B}.tmp	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28BA4
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\67da9da8-4b53-4407-9184-abce69bfc8b5[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 31640, version 1.0
Category:	downloaded
Size (bytes):	31640
Entropy (8bit):	7.987419157519047
Encrypted:	false
SSDEEP:	768:2ksR9I2XrELLNH2szA8XginR2NvWwYinLhmL9sEH+L:2ksR9droLTzjginR2NvpndmJsFL
MD5:	24174D7A19C1C3BDB8863E4D5966C81E
SHA1:	C6D6A0E39D2F1F02875D29645922100ACD5F67CC
SHA-256:	AEB41D763A82AA10BFE8C920F7C7DC92A6F4FD07083AA9272F488C1834F21CBA
SHA-512:	02E3B54765CDD14C2B6DD5AABEA75FA80CD72620D8BD376B06A61EA4D10F339C8E762F0319A8A64E184D5ED684783066B33CA075F6C9556DA7DC83F40CE3AE75
Malicious:	false
IE Cache URL:	http://https://static.parastorage.com/services/santa-resources/resources/viewer/user-site-fonts/fonts/Helvetica/v2/67da9da8-4b53-4407-9184-abce69bfc8b5.woff
Preview:	wOFF.....{.....v.....GPOS.....x..GSUB.....OS/2...X...S...`f.|.VDMX.....\....p.xlcmap.....&cvt .....X.....:..fpgm...,.....,...gasp.....glyf.. ....R^...|v...head..h ...6...6..~.hhea..hX...!...$.E.ihmtx..h\|.....$=\3.loca..k,.....(.j..maxp..o(... ... .u.Tname..oH.....post..u..... ...2prep..u,.....x..TMKTQ.~.w.... G...u.).@PD.....HqSf_..h..?..j.A."..m..E.&\....>6..9.....z.....e.C.x{.>....>.....4..we.>x.L..A.....Z.Z.....S.fpDd...".D...D:Z..._c....yhY..N.?.Z=....C.O.G.....f....h..Qfa. J..W.uT...5...?{2.<.;...,....r|."V$o....9j5.}..I.....Y49b.....M.?.G.J..9.g.sv..)o>..n./.L.W.A4;c2..d..jF....a.J.z...~.Q...c..{....I&.{....]..=....x..9[.p.)}.N.gQ..e.....6.bLu..7%+ 2>.z4...hG..1.;.<.+..k.....=.....O..%,..V.....T..P.U%.kw0.....B1.f..... ..9."\..1..~.1Hx.6....Ba..@$.....$};x.....$.....5..+... ...7)u...U...Q5<.y.l...6r.B8....DL"....d.^}.....y/.j.Y.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\HOSOIXRG.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	594698
Entropy (8bit):	5.6334438519929595
Encrypted:	false
SSDEEP:	6144:WcRj9C5cxjTW8gTwf13m2pnzLcrHEXeHmYWHVHw:Xd13EreimTdw

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\HOSOIXRG.htm	
MD5:	612F638153331AFEBAEBBD3342A1113F
SHA1:	DFA74B975063102F7C6F4DC35E811722697655F3
SHA-256:	A5A2C8167B9F85AD1C47C9F89337CA2F179EBCC642303963E17E22A029F8E8AA
SHA-512:	3D3A01CA75B21DDE0ABECC7BB6C9492E291F31D71657176D1D2DE8E396CD6CE819EC532628C838E6E2F2AB282E318E004CF32ACBE24510160EDA87BC34B79F4
Malicious:	false
IE Cache URL:	http://https://www.artsenvoorwaarheid.nl/
Preview:	<!DOCTYPE html>.<html lang="en">.<head>. . <meta charset='utf-8'>. <meta name="viewport" content="width=device-width, initial-scale=1" id="wixDesktopViewport" />. <meta http-equiv="X-UA-Compatible" content="IE=edge">. <base href="https://www.artsenvoorwaarheid.nl/">. <meta name="generator" content="Wix.com Website Builder"/>.. <link rel="icon" sizes="192x192" href="https://static.parastorage.com/client/pfavico.ico">. <link rel="shortcut icon" href="https://static.parastorage.com/client/pfavico.ico" type="image/x-icon"/>. <link rel="apple-touch-icon" href="https://static.parastorage.com/client/pfavico.ico" type="image/x-icon"/>. Safari Pinned Tab Icon -->. <link rel="mask-icon" href="https://static.parastorage.com/client/pfavico.ico"> -->.. Legacy Polyfills -->. <script src="https://static.parastorage.com/unpkg/core-js-bundle@3.2.1/minified.js" nomodule=""></script>. <script src="https://static.parastorage.com/unpkg/focus-within-polyfill@5.0.9/dist/focus-wit

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\WixMadeforDisplay_W_Bd[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 27080, version 1.13107
Category:	downloaded
Size (bytes):	27080
Entropy (8bit):	7.984576267611114
Encrypted:	false
SSDEEP:	384:YGJNjRUmxJdaYP4ekBDEggz90TzZWzjlru54l0AkjRrk31JNbGpN6MDfcWG:9rUmxJYYP43FY7qWv1JZEzFG
MD5:	19D333269CAABD296357B1A7E72FBB5D
SHA1:	FBE6AB746415B8713FFFE51DFFFDC3C9D59BC40C
SHA-256:	8A6A9A30D97D0C3591326A34B222515BA5A5B7D16E68F4FF49DDBE0FA13EB541
SHA-512:	00861456CC778E5150AB1F1498F3BCBF1A3770580DE621927560D3DC4D448D7CC01BE21C426C7F06A5BEFE9335456A03798C8EA65E10DC66FCFD394CCDDA23A
Malicious:	false
IE Cache URL:	http://https://static.parastorage.com/services/santa-resources/resources/viewer/user-site-fonts/fonts/WixMadefor/v2/WixMadeforDisplay_W_Bd.woff
Preview:	wOFF.....i.....33.....GDEF..W0.....".."!GPOS..W.....E.&.{EGSUB..e.....fOS/2.....X...`....cmap.....X..:.cvt ...h.....$^.%fpgm.....0.6gasp..W$..... ..glyf.....CO..s.v>..head.....6...6.mI.hhea..... ...$...ehmtx...P...Z...h.3bloca...$...t.....maxp..... ... .D..name..U....%....@BlVpost..W..... ...>prep...h....._$i.....33v.w+_. .....+/.....x.c`d``.....X..EP..-.....P...X...../.a.....x.%...B1../..4H...i....2H6`.T..'w..%. Iv.....zYE....b.T.....f.@. ....4....Zx....tG....[.6>/>...m.m#.m..j.. ..t&o...;.8w..4J....j...l.|..s.0[X(\.....b^.=.....-...P.'.~..`o)..q.xWK.U.7n.Y.j...E.55,...K.p..ak...Y.q.!\.>.p..NW.p.{gcOW.....L..k.b.f.....*xB3P.HX.....`..Kj.v...6Jl.....7.....R.}.q.#.2. ....q..s..Q.a9...^..a.+|.5.h<.....hNt.....B....I..37k....P.r.ST.+..E.cT...%,.E.A.?.az..i@|.;..'k..-v=..O.>.n%.....We..>.)..p.om.5.#NP.....i.}.!...j\

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\WixMadeforText_W_It[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 27412, version 1.13107
Category:	downloaded
Size (bytes):	27412
Entropy (8bit):	7.982891923389201
Encrypted:	false
SSDEEP:	768:ap6knzmw/hRKu7qDk7lddf2H7jE/MnEzqD2NSXTiheFG:aYJw/Hlxf7Mn5SNi4z
MD5:	8E17780BCDC9E29BFDF2B5EC643E7B3B
SHA1:	CFBB4904DAF466D0AD0864DC43249C30866E7285
SHA-256:	507BC6DAB5FCF62276BFEE3155DDF6083AE9EBB54729FB56040A60DEE9C705B3
SHA-512:	ABA09CC85AAC3F2096A98FEFBDCA5DF572D718A553AC2F2918945E788901D87D0244A15E01CA417945A2E02BB10D6813CF390A83168662747FEB701B39C9222
Malicious:	false
IE Cache URL:	http://https://static.parastorage.com/services/santa-resources/resources/viewer/user-site-fonts/fonts/WixMadefor/v2/WixMadeforText_W_It.woff
Preview:	wOFF.....k.....33.....GDEF..Z.....".."!GPOS..[d.....Dn....GSUB..g.....fOS/2.....[...`....cmap...H.....X..:.cvt ...0.....+...fpgm...X.....0.6gasp..Z..... ...glyf...h..F+..u.....head.....6...6.}..hhea.....#...$...+hmtx...X.....h.jGRloca.....z....''S..maxp..... ... ....name..Y.....?.k.post..Z..... ...@prep.....,.....33.[.._.<..... .....x.c`d``.....,{._0\f@.....O...R...../.a...1.....x.%.....@...'.H.$xc..:..... l.(h....Z...../.:RL.f.T-.....@..U....e..]....9..(....1...x.....J..oW~.m.m.m.m.mc...d.y .s.SIW.z.'d...wx.p>.C..EW.A..@...Cc....3..YF.b.....~...t3.....'.QN..0.....+.Hj...''.Vj %.[.yH..3v..S].5.!Tg....7..F ...q..x.f\^.`\~..1.0myR.qQ...z.U..RM.Tg...@..~.F..|....[B...D.:.F_[.. mB.`....!.%(.h JXk.....~.iH'.P...ul4..3)J.N.#3.{...e.....#M.....z.DFh.M..H./..6....v....P..Z...9.+.N..... .....''.:...a.J..... .P..cU..8*.....^..O(.C

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\WixMadeforText_W_Rg[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 26104, version 1.13107
Category:	downloaded
Size (bytes):	26104
Entropy (8bit):	7.98125788470629
Encrypted:	false
SSDEEP:	768:AAPFnTujLBLXY1QeKq5X253Cbs/y3/yspaw+oPjO09FG:A920T3C4y3/ys+mRe
MD5:	1A0CA11ADF2C74087410EC6D02B86AA7
SHA1:	E8B0C1A2D023E989D0270898F8C863AB5F9DF11F
SHA-256:	F2E3AE2666C03A75C5A9DF7073540DE7E55E168327AEA24BDFE1F9D7796C6F0C

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\WixMadeforText_W_Rg[1].woff	
SHA-512:	438C38767BDB263C8B9F5DCE11A87B785B76426E1838C9EF4346830E64D0608CCDCD69719D977A760ECFA18FFE9A55CD8A4FF49384059A9AE3E045C839EA94F
Malicious:	false
IE Cache URL:	http://https://static.parastorage.com/services/santa-resources/resources/viewer/user-site-fonts/fonts/WixMadefor/v2/WixMadeforText_W_Rg.woff
Preview:	wOFF.....e.....33.....GDEF..Vx.....".."!GPOS..W.....A...V.GSUB..a.....fOS/2.....[..`....cmap.....X..:.cvt .....'..ofpgm.....0.6gasp..Vl.....glyf... ...B...s.B?..head.....6...6.il.hhea..... ...$...dhmtx...T...Q...h.RSnloca...<...y.....N..maxp..... ... .~..name..U8.....@.lGpost..VX..... ...@prep...d.....H6.....33$..._.<.....+ /.....9...r.....x.c`d``....e.....X.."(.....X.....P...X...../.a...#.....x.%...Aa.....Y....rg....F...bo...y.p.l)Lp....v...)....oK.B..R..J...^o.....(.....L.3.x....l....~.=.m.g.m.m.m.7..DU o/...."...z.{....|.).qN..Q>..t.?Ui{.2{_..k.....v._.")..~.a.C./.y..V.]4*.....)....0...j<.iv.&..Zl'k..^v....c.h..Qv..1.....f-....8;..Q/j.....h.m....>a{.....8...]`W...'.....&.o8P#..V.k.....k|Av....p....9I.Y.. }.1jrFi..F.#..q.M.....^#..../...v.:..~...Nw?.N.x...)M._a..6a.6.1.V.ZO....\...C.?c'....7.v..ke../j.p..d.....X[A.....X!...=L.h[..|.H+..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\activityi;src=4382365;type=count;cat=websi0;ord=1;num=6375209772439;gtm=2wg6n0;auiddc=288779517.1624884980;u1=0014774d-e86e-4006-895c-197a7e3747e8;~oref=https___www.wix[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	492
Entropy (8bit):	5.516853633619749
Encrypted:	false
SSDEEP:	12:hnMQbwuOaxyCkv4AEH7BV7ec8VjYEO/nQTw3AEIAgKWw1vf:hMiRO9yB0rVjXOvQTKqAgKvvf
MD5:	0ABAF3C96B7F1E6A19CD60067C5D4585
SHA1:	1FE68951383348022FC5A9FD6DA648B3114111AA
SHA-256:	8DE15C89B172581B5417B0C7800765F2458F21C45FF03AB4FEF6A185C4EF9F2E
SHA-512:	398E21D22CBE6E6FE0A001E095153DFA705A125F4CDCB74575198FC7F88E0A087A92D7D3DB1B458B1AD93CC75D3E9BBD5C363F5903C3423ADFA264C385BED(93
Malicious:	false
IE Cache URL:	http://https://4382365.fls.doubleclick.net/activityi;src=4382365;type=count;cat=websi0;ord=1;num=6375209772439;gtm=2wg6n0;auiddc=288779517.1624884980;u1=0014774d-e86e-4006-895c-197a7e3747e8;~oref=https%3A%2F%2Fwww.wix.com%2Foutdated-browser%2Finternet-explorer%3FforceBolt%3D%26ssrIndicator%3Dfalse%26suppressbi%3Dtrue?
Preview:	<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd"><html><head><title></title></head><body style="b ackground-color: transparent"></body></html>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\analytics-event-adapter.bundle.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	25954
Entropy (8bit):	5.2333144705571435
Encrypted:	false
SSDEEP:	384:B4zFRNtNCYoc7cWMxE5kkWC5H+pu6UJ9OZp2VkpQ5pKmoVhRRJHf8zJQM:ON/7cWMxEhWCMpu/vF6pwKm2NYJz
MD5:	B52699D1ECC78BA53EEB09387232F122
SHA1:	216F19C6339FB0DDD4AB634500F1A14BF3A31C34
SHA-256:	B13F6BD317BB3A04B14262D8F535E4F5C8773352513DC698CF7A3305F4AC9E71
SHA-512:	29D61DEA50E8D5175DB587C7CAE7AC703BA114C04161870C9BE5A175232252E44C7E1AF07BDA66D80851BBFB1DCB45A71EF307F14AFFD3796EE24F7A4E1AB6 6F
Malicious:	false
IE Cache URL:	http://https://static.parastorage.com/services/promote-analytics-adapter/2.759.0/analytics-event-adapter.bundle.min.js
Preview:	!function(e,n){"object"==typeof exports&&"object"==typeof module?module.exports=n():"function"==typeof define&&define.amd?define("promote-analytics-adapter",[], n):"object"==typeof exports?exports["promote-analytics-adapter"]=n():e["promote-analytics-adapter"]=n()}("undefined"!=typeof self?self:this,function(){return function(e){var n={};function t(r){if(n[r])return n[r].exports;var o=n[r]={i:r,l:!1,exports:{}};return e[r].call(o.exports,o,o.exports,t),o.l=!0,o.exports}return t.m=e,t.c=n,t.d=function(e,n,r){t.o(e,n) ||Object.defineProperty(e,n,{enumerable:!0,get:r})},t.r=function(e){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(e,Symbol.toStringTag,{ value:"Module"}),Object.defineProperty(e,"__esModule",{value:!0})},t.t=function(e,n){if(1&n&&(e=t(e)),8&n)return e;if(4&n&&"object"==typeof e&&e&&e.__esModule)return e;var r=Object.create(null);if(t.r(r),Object.defineProperty(r,"default",{enumerable:!0,value:e}),2&n&&"string"!=typeof e)for(var o in e)t.d(r,o,function(n

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\bolt-components[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	29642
Entropy (8bit):	5.309386095525225
Encrypted:	false
SSDEEP:	768:ksXWi1cgUt7e8RojAviT/d3A2F0GbM2GOQb:H8RojAvI/d3A2Fzu
MD5:	4AAA5B353FC13CC4D663255ED0CEE7C7
SHA1:	B377411DCD8DAE53A57636620CED628EC716263F
SHA-256:	61665413ECBD4B293E42FFB74DF9D777FEE7B88ED79F56E7738786B131E1E254

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\bolt-components[1].js	
SHA-512:	EEC062E9FC74CC2AAED9A8FC9F38F763E63255676F3DB43F7FF663932A2F6492DFCDA9F6D414F93F2AF3FA5DE90F6388E5D6BECC6A443374C440BC4FB3A5CE E6
Malicious:	false
IE Cache URL:	http://https://static.parastorage.com/services/wix-bolt/1.7264.0/node_modules/bolt-components/dist/bolt-components.js
Preview:	!function(e,t){"object"==typeof exports&&"object"==typeof module?module.exports=t(require("react"),require("prop-types"),require("santa-components"),require("lo dash"),require("santa-core-utils")):"function"==typeof define&&define.amd?define(["react","prop-types","santa-components","lodash","santa-core-utils"],t):"object"==typeof exports?exports["bolt-components"]=t(require("react"),require("prop-types"),require("santa-components"),require("lodash"),require("santa-core-utils")):e["bolt-components "]=t(e.react,e["prop-types"],e["santa-components"],e.lodash,e["santa-core-utils"])}(this,function(e,t,r,o,n){return function(e){var t={};function r(o){if(t[o])return t[o].exports;var n=t[o]={i:o,l:!1,exports:{}};return e[o].call(n.exports,n,n.exports,r),n.l=!0,n.exports}return r.m=e,r.c=t,r.d=function(e,t,o){r.o(e,t)||Object.defineProperty(e,t,{enumerable:!0 ,get:o})},r.r=function(e){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(e,Symbol.toStringTag,{value:"Module"}),Objec

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\bolt-main-r.animations[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	15274
Entropy (8bit):	5.0786591960830565
Encrypted:	false
SSDEEP:	192:SJIpIaNFtNpIGNaCYz8omesMK3Z5Ub1FCFZ7c+TmdKq52wUOdZZUj20KAH5KFe68:rXpFU3zjsMKp5U+boOmd1lgH8eWuNV
MD5:	5112E2448CDFCD600FD8AE8CEA4F2E18
SHA1:	81EB20408588FBF6773DA8870DC81B2CDC2EEAD9
SHA-256:	5F64A46FE3986511A45732CE9A888E738131FD614CE1B06E565CD589AABB25C8
SHA-512:	ACBD35CEC4A85D10A2E9AC497DAAC2DF2AA2085D554973CCFD1303EEBD7F85DCBF614E00C83415461C5850DD93E36F80E33E290D29AB5DC246982D07829D8 27
Malicious:	false
IE Cache URL:	http://https://static.parastorage.com/services/wix-bolt/1.7264.0/bolt-main/app/bolt-main-r.animations.js
Preview:	(this.webpackJsonp=this.webpackJsonp||[]).push([[1],{1e3:function(e,t,n){"use strict";function i(e,t){if(null==e)return{};var n,i,a=function(e,t){if(null==e)return{};var n,i,a={},r =Object.keys(e);for(i=0;i<r.length;i++)n=r[i],t.indexOf(n)>=0||(a[n]=e[n]);return a}(e,t);if(Object.getOwnPropertySymbols){var r=Object.getOwnPropertySymbols(e);for(i=0;i <r.length;i++)n=r[i],t.indexOf(n)>=0||Object.prototype.propertyIsEnumerable.call(e,n)&&(a[n]=e[n])}return a}function a(e,t){for(var n=0;n<t.length;n++){var i=t[n];i.enume rable=i.enumerable||!1,i.configurable=!0,"value"in i&&(i.writable=!0),Object.defineProperty(e,i.key,i)}}function r(e,t){return function(e){if(Array.isArray(e))return e}(e)||functio n(e,t){var n=[],i=!0,a=!1,r=void 0;try{for(var o,s=e[Symbol.iterator]();!(i=(o=s.next()).done)&&(n.push(o.value),!t||n.length!==t);i=!0);}catch(e){a=!0,r=e}finally{try{i||null==s.r eturn||s.return()}finally{if(a)throw r}}return n}(e,t)||function(){throw new TypeError("Invalid attempt to destructure n

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\bolt-main-r.init[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	339474
Entropy (8bit):	5.446448385592585
Encrypted:	false
SSDEEP:	3072:f+w3wlrHaLiQjiLhMaZdJxkF5Njt/4i4Q44z4FhvJrWvpQ2rNXK8HOwPH9L3fPj5:2wSLhf4LZI8hDPj5
MD5:	25A63C0AE966BD76C3C5765B7D3BEACD
SHA1:	2A6E2E3B7959C14A554477AFE15B6ABC0B4854B6
SHA-256:	9D24704FA0C1018EF8660960C12B1DF87796883E2318FE731C70AF1AC8F3E553
SHA-512:	F891623C763F6009D2BFCF97ED03EDD5BD1CB9DF6C517AD732C05CF07E30E5EBB9355763453676FE817AF42616AFB5D1E33B327F254E30830D79A1127AF3AF4
Malicious:	false
IE Cache URL:	http://https://static.parastorage.com/services/wix-bolt/1.7264.0/bolt-main/app/bolt-main-r.init.js
Preview:	(this.webpackJsonp=this.webpackJsonp||[]).push([[4],{22:function(e,n,r){"use strict";function t(e){for(var n=1;n<arguments.length;n++){var r=null!=arguments[n]?arguments[n]:{},t=Object.keys(r);"function"==typeof Object.getOwnPropertySymbols&&(t=t.concat(Object.getOwnPropertySymbols(r).filter(function(e){return Object.getOwnPrope rtyDescriptor(r,e).enumerable}))),t.forEach(function(n){o(e,n,r[n])})}return e}function o(e,n,r){return n in e?Object.defineProperty(e,n,{value:r,enumerable:!0,configurab le:!0,writable:!0}):e[n]=r,e}var a=r(50),i=r(461),s=r(462).getLanguageCode,u=r(55).webBiLoggerFactory,l=r(463),c=r(464).createFunctionLibrary,p=r(513),d=r(514), m=d.getRuntimeStoreDefaultValue,g=d.getRuntimeEventsStoreDefaultValue,f=r(515),v=f.applyGradualRolloutOverrides,w=f.overrideClientSpecMapScriptsFromQu ery,y=f.removeApps,M=r(296).updateHistory,h=r(517).initSeoWrapper,b=function(){},P=function(e,n,r){var a=n.components,i=e||function(e){return o({},e.MasterPage. compType,e.MasterPage)}(a),s=t

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\bolt-main-r.vendors~init[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	54888
Entropy (8bit):	5.418605348178299
Encrypted:	false
SSDEEP:	768:2RByuyYT+yDVLn044tuNzID1tDvj7Z8e1E4qNuTOY7gIxd58nVn6:2/lbL0bwIDfvxYNuTO+XD
MD5:	D6474CD7BFB01E1CEC10034FF8E78D9F
SHA1:	14BC582F100995F0C280FEC721B1EE393FE520F7
SHA-256:	01B6CEF8BAA50E5A8180621C6496301EDB7E1C835F195031323725463D2B59E7
SHA-512:	111CFAB505ED239C848BFE47EF8054DD0D1818FCBDFEB8DE6BF98EC8E17649962A10ADE0564369E3A607B5B18B7F18B49795B9B4AD27828F256650929D4E645 A

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\bolt-main-r.vendors~init[1].js

Malicious:	false
IE Cache URL:	http://https://static.parastorage.com/services/wix-bolt/1.7264.0/bolt-main/app/bolt-main-r.vendors~init.js
Preview:	(this.webpackJsonp=this.webpackJsonp||[]).push([[8],{191:function(e,l,a){"use strict";Object.defineProperty(l,"__esModule",{value:!0});var o=a(50);l.top=function(e){return e.top},l.left=function(e){return e.left},l.bottom=function(e){return e.top+e.height},l.height=function(e){return e.height},l.fitToContentHeight=function(e){return Boolean(e.fitToContentHeight)},l.getContainerHeight=function(e){return o.max([e.height||0,e.minHeight||0])},l.isRotated=function(e){return o.isNumber(e.rotationInDegrees)&&0!==e.rotationInDegrees}},297:function(e,l,a){"use strict";Object.defineProperty(l,"__esModule",{value:!0});var o=a(501);l.isPolicyAllowsBsi=function(e){return!e||!e.policy||e.policy[o.ConsentPolicyCategories.Analytics]&&e.policy[o.ConsentPolicyCategories.Functional]}},298:function(e,l,a){"use strict";Object.defineProperty(l,"__esModule",{value:!0}),l.validateExternalApi=function(e){for(var l=[],a=1;a<arguments.length;a++)l[a-1]=arguments[a];return l.forEach(function(l){if(!e||"function"!

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\bootstrap-features.53639d1b.bundle.min[1].js

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	134185
Entropy (8bit):	5.315880830816571
Encrypted:	false
SSDEEP:	1536:MCaUTGBWDVRNNRviithocvTUV2yd2z/hhM2a:+WtxLUV5dCX2
MD5:	16EF54B37117FB41D86C1FF75EA6E79E
SHA1:	A812A5EB71AB8F1F3534E8CACC56685DBAA217EF
SHA-256:	8AC1BCBAF1AE78F7E6BB52DEEDCEBF9FE7DCA269C1E3476CB1AFFFDE2809AFF9
SHA-512:	C8EDBD0A49FE9EF432FAC459030EE4F7CF8B2CB418D65DC21C74A5CAA5DE820290312F1C161624DE9FEA816347F74B9CF653DC52ACB7C8640E257F2CC16DA41
Malicious:	false
IE Cache URL:	http://https://static.parastorage.com/services/wix-thunderbolt/dist/bootstrap-features.53639d1b.bundle.min.js
Preview:	/*! For license information please see bootstrap-features.53639d1b.bundle.min.js.LICENSE.txt */.(self.webpackJsonp__wix_thunderbolt_app=self.webpackJsonp__wix_thunderbolt_app||[]).push([[4767],{55049:function(){!function(n){var t={};function e(r){if(t[r])return t[r].exports;var o=t[r]={i:r,l:!1,exports:{}};return n[r].call(o.exports,o,o.exports,e),o.l=!0,o.exports}e.m=n,e.c=t,e.d=function(n,t,r){e.o(n,t)||Object.defineProperty(n,t,{enumerable:!0,get:r})},e.r=function(n){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(n,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(n,"__esModule",{value:!0})},e.t=function(n,t){if(1&t&&(n=e(n)),8&t)return n;if(4&t&&"object"==typeof n&&n&&n.__esModule)return n;var r=Object.create(null);if(e.r(r),Object.defineProperty(r,"default",{enumerable:!0,value:n}),2&t&&"string"!=typeof n)for(var o in n)e.d(r,o,function(t){return n[t]}.bind(null,o));return r},e.n=function(n){var t=n&&n.__esModule?function(){return n.default}:functio

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\bundle.min[1].js

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	58325
Entropy (8bit):	5.209892608777627
Encrypted:	false
SSDEEP:	768:/FKwvfGLx+0gGQyyIYo9vNAf4E2QIVMs2EUq80zniR6PaLyC/3O5kki/gXBKtgK:/FKsh0gGQyynoITsfW0UkVXwtb
MD5:	6167461CDB31A9A37C6CB908EE20F437
SHA1:	2351DAECD6BBEE25A9790FF7887AA2D995A5EB81
SHA-256:	010C6C3D69720442EB181274E95F61FBBB3486DA6338E3BA129287B7077627FE
SHA-512:	385D34C4BD3CAC9AF4AD1B513066B816B56DC5AC877A6A522566B1B52B635D4433B3F12DA3E9BF9C982374D1A05A5A37C11B3B37F99F086D1D99E0DFA33E11F
Malicious:	false
IE Cache URL:	http://https://browser.sentry-cdn.com/5.21.4/bundle.min.js
Preview:	/*! @sentry/browser 5.21.4 (0228d1f) | https://github.com/getsentry/sentry-javascript */.var Sentry=function(t){var n=function(t,r){return(n=Object.setPrototypeOf||{__proto__:[]}instanceof Array&&function(t,n){t.__proto__=n}||function(t,n){for(var r in n)n.hasOwnProperty(r)&&(t[r]=n[r])})(t,r)};function r(t,r){function e(){this.constructor=t}n(t,r),t.prototype=null===r?Object.create(r):(e.prototype=r.prototype,new e)}var e,i,o,u=function(){return(u=Object.assign||function(t){for(var n,r=1,e=arguments.length;r<e;r++)for(var i in n=arguments[r])Object.prototype.hasOwnProperty.call(n,i)&&(t[i]=n[i]);return t}).apply(this,arguments)};function c(t,n){var r="function"==typeof Symbol&&t[Symbol.iterator];if(!r)return t;var e,i,o=r.call(t),u=[];try{for(;(void 0===n||n-- >0)&&!(e=o.next()).done;)u.push(e.value)}catch(t){i={error:t}}finally{try{e&&!e.done&&(r=o.return)&&r.call(o)}finally{if(i)throw i.error}}return u}function a(){for(var t=[],n=0;n<arguments.length;n++)t=t.concat(c(arguments[n]));}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\color.min[1].js

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	18954
Entropy (8bit):	5.462041906644879
Encrypted:	false
SSDEEP:	384:DmUI8qSy0vgJON6aAPXVhuR7DOegpSnoVTX6W9FDW6+I65nFuM9:DTFHN6vPX+7DOegpSnoVT7FDW6bM9
MD5:	7F8F0363808B72AE76DE192F51689D33
SHA1:	212EEE29A63222FD2B558CC5F432347EE31407D8
SHA-256:	CE88CFE2A86DD05C6ED0B3A876C0FD93C3B5CCCAE146D2FB9CF0BA2E2EC729F6
SHA-512:	4846DB41108A0BE652B183C0081746FC0180AC7233B9977254270B3C0073EB09200ABC62A6F8BCD5ADAF3D1F5B56FA746FE495E63316113D486DF22E60E9C697

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\color.min[1].js	
Malicious:	false
IE Cache URL:	http://https://static.parastorage.com/unpkg/@wix/santa-external-modules@1.644.0/color-convert/0.2.0/color.min.js
Preview:	(function e(t,n,r){function s(o,u){if(!n[o]){if(!t[o]){var a=typeof require=="function"&&require;if(!u&&a)return a(o,!0);if(i)return i(o,!0);throw new Error("Cannot find module '"+o+"'")}var f=n[o]={exports:{}};t[o][0].call(f.exports,function(e){var n=t[o][1][e];return s(n?n:e)},f,f.exports,e,t,n,r)}return n[o].exports}var i=typeof require=="function"&&require;for(var o=0;o<r.length;o++)s(r[o]);return s})({1:[function(require,module,exports){Color=require("./color")},{"./color":2}],2:[function(require,module,exports){var convert=require("color-convert"),string=require("color-string");module.exports=function(cssString){return new Color(cssString)};var Color=function(cssString){this.values={rgb:[0,0,0],hsl:[0,0,0],hsv:[0,0,0],cmyk:[0,0,0,0],alpha:1};if(typeof cssString=="string"){var vals=string.getRgba(cssString);if(vals){this.setValues("rgb",vals)}else if(vals=string.getHsla(cssString)){this.setValues("hsl",vals)}}else if(typeof cssString=="object"){var vals=cssString;if(vals["r"]!==un

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\comboBoxInput.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	32298
Entropy (8bit):	5.413232241801773
Encrypted:	false
SSDEEP:	768:BC2C7ZTfX1017qTqNX3017qTofHTk17qT0kye:uJfX1017qTqNX3017qTofHTk17qT0kye
MD5:	00F241AA303942FD276951555595909C
SHA1:	FEF3B3743F9C1CDCD0C721257ECD2518A56159C2
SHA-256:	3601506B77DB5387EBA5B37EE822469B053D30233B9B9CCF0A94BDA50DEC0400
SHA-512:	35E7F47CE8CEE461B269E575A771DB9EA199D6943F216B786C177543B4D57A709266AC00DDB1D3A72CF1C8DA4425865F93B20960548BA18D506923FD224F0742
Malicious:	false
IE Cache URL:	http://https://static.parastorage.com/services/wix-bolt/1.7264.0/node_modules/wix-santa/dist/packages-bin/comboBoxInput/comboBoxInput.min.js
Preview:	define("comboBoxInput",["lodash","santa-components","componentsCore","prop-types","skins","textCommon"],(function(e,t,o,r,i,l){return function(e){var t={};function o(r){if(t[r])return t[r].exports;var i=t[r]={i:r,l:!1,exports:{}};return e[r].call(i.exports,i,i.exports,o),i.l=!0,i.exports}return o.m=e,o.c=t,o.d=function(e,t,r){o.o(e,t)||Object.defineProperty(e,t,{enumerable:!0,get:r})},o.r=function(e){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(e,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(e,"__esModule",{value:!0})},o.t=function(e,t){if(1&t&&(e=o(e)),8&t)return e;if(4&t&&"object"==typeof e&&e&&e.__esModule)return e;var r=Object.create(null);if(o.r(r),Object.defineProperty(r,"default",{enumerable:!0,value:e}),2&t&&"string"!=typeof e)for(var i in e)o.d(r,i,function(t){return e[t]}.bind(null,i));return r},o.n=function(e){var t=e&&e.__esModule?function(){return e.default}:function(){return e};return o.d(t,"a",t),t},o.o=function(e,t){return Object.pr

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\components.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	107563
Entropy (8bit):	5.178655246258952
Encrypted:	false
SSDEEP:	1536:k4EbwKaraPyj+TxNWfpgnFBho62BmKF9C8tT1IG54m6CaEbNZ+:a2CrWf+NcdDauO
MD5:	09CE194FFCE597D89F2925A3064ADB14
SHA1:	9BCA6646FEB35112AA9300364D43E7753A863739
SHA-256:	5647256A5B2A82B190036331306BBC74D447456DC95BCF0270579FCF573122A9
SHA-512:	5DF21A378372ABDC425FA2E62FACA0DCF02F664C08C1B7F2D894836E7ADE6E4723289C95FC9A610CE896523366B6F6DA339ED2590385081504724261DC8C015
Malicious:	false
IE Cache URL:	http://https://static.parastorage.com/services/wix-bolt/1.7264.0/node_modules/wix-santa/dist/packages-bin/components/components.min.js
Preview:	define("components",["lodash","coreUtils","santa-components","componentsCore","prop-types","skins","reactDOM","zepto","santa-core-utils","create-react-class","image-client-api","textCommon","backgroundCommon","santa-animations","galleriesCommon","displayer","imageZoom","comboBoxInput"],(function(e,t,i,n,s,a,o,r,p,l,c,d,u,h,m,g,y,f){return function(e){var t={};function i(n){if(t[n])return t[n].exports;var s=t[n]={i:n,l:!1,exports:{}};return e[n].call(s.exports,s,s.exports,i),s.l=!0,s.exports}return i.m=e,i.c=t,i.d=function(e,t,n){i.o(e,t)||Object.defineProperty(e,t,{enumerable:!0,get:n})},i.r=function(e){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(e,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(e,"__esModule",{value:!0})},i.t=function(e,t){if(1&t&&(e=i(e)),8&t)return e;if(4&t&&"object"==typeof e&&e&&e.__esModule)return e;var n=Object.create(null);if(i.r(n),Object.defineProperty(n,"default",{enumerable:!0,value:e}),2&t&&"string"!=typeof e)for(var s

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\componentsCore.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	34991
Entropy (8bit):	5.1759691573185655
Encrypted:	false
SSDEEP:	384:k6g680OvgHweHduehEIOXRJlb3ZL+mZJqDnG2ZKbVsjz83CTK1/jLwhq40zZ:X8m5Hx+BJlb3ZLZaja
MD5:	D6CF1EBA6C70BECBEF2E84177BE65EF7
SHA1:	D496CF49D9EFBFA8622950A9353A9AEB959D5C35
SHA-256:	151A1E3A41FD50F31D96EB76EE9C3F2160387B8DF4E751C2DD92584BF18665BD
SHA-512:	095E1435C59385BC80C110DF035C356B93998B5509B1A088E03DE087B81C680DFC6DDF21D66E15CE86B83B00DD8E7A38218B442F5ED5A401C38DA636E66F49A
Malicious:	false
IE Cache URL:	http://https://static.parastorage.com/services/wix-bolt/1.7264.0/node_modules/wix-santa/dist/packages-bin/componentsCore/componentsCore.min.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\componentsCore.min[1].js	
Preview:	define("componentsCore",["lodash","coreUtils","santa-components","prop-types","skins","reactDOM","zepto","santa-core-utils","warmupUtilsLib","create-react-class","react"],(function(e,t,n,i,r,o,s,a,c,l,u){return function(e){var t={};function n(i){if(t[i])return t[i].exports;var r=t[i]={i:i,l:!1,exports:{}};return e[i].call(r.exports,r,r.exports,n),r.l=!0,r.exports}return n.m=e,n.c=t,n.d=function(e,t,i){n.o(e,t)||Object.defineProperty(e,t,{enumerable:!0,get:i})},n.r=function(e){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(e,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(e,"__esModule",{value:!0})},n.t=function(e,t){if(1&t&&(e=n(e)),8&t)return e;if(4&t&&"object"==typeof e&&e&&e.__esModule)return e;var i=Object.create(null);if(n.r(i),Object.defineProperty(i,"default",{enumerable:!0,value:e}),2&t&&"string"!=typeof e)for(var r in e)n.d(i,r,function(t){return e[t]}.bind(null,r));return i},n.n=function(e){var t=e&&e.__esModule?function(){return e.default}:f

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\coreUtils[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	108711
Entropy (8bit):	5.507484905571302
Encrypted:	false
SSDEEP:	1536:/kuG5CvhaFfvbms/fMYhMlWKKSSpNPakN0IF/U2yCSE3N78Ly+BQ5:NZher5bPFN5U2yCSlQ5
MD5:	FEFA989A1F936A1372036154B69DCA6A
SHA1:	B09FA1B7AA091DE9D946887DA05F8B0978989298
SHA-256:	4C200060AB0507A801B7BE75C1DC313213AE0F97BAD1B8A8F30E8A6E7502A4C0
SHA-512:	D1736E46849F4CE0B806D00957EE3B79706AB90BB62BE78E7BDA71D972E771A34D7A64E53BD82D6DDCFA7AA00EA9A93FF7BE504D3E9018747A29E34ECEB28ABF
Malicious:	false
IE Cache URL:	http://https://static.parastorage.com/unpkg/@wix/santa-core-utils@1.2706.0/dist/coreUtils.js
Preview:	!function(e,t){"object"==typeof exports&&"object"==typeof module?module.exports=t(require("lodash"),require("zepto"),require("warmupUtilsLib")):"function"==typeof define&&define.amd?define(["lodash","zepto","warmupUtilsLib"],t):"object"==typeof exports?exports.coreUtils=t(require("lodash"),require("zepto"),require("warmupUtilsLib")):e.coreUtils=t(e.lodash,e.zepto,e.warmupUtilsLib)}(this,(function(e,t,n){return function(e){var t={};function n(r){if(t[r])return t[r].exports;var o=t[r]={i:r,l:!1,exports:{}};return e[r].call(o.exports,o,o.exports,n),o.l=!0,o.exports}return n.m=e,n.c=t,n.d=function(e,t,r){n.o(e,t)||Object.defineProperty(e,t,{enumerable:!0,get:r})},n.r=function(e){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(e,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(e,"__esModule",{value:!0})},n.t=function(e,t){if(1&t&&(e=n(e)),8&t)return e;if(4&t&&"object"==typeof e&&e&&e.__esModule)return e;var r=Object.create(null);if(n.r(r),Object.defineProperty

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\core[1].js	
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):	1142
Entropy (8bit):	5.056209222218177
Encrypted:	false
SSDEEP:	24:Xcw6BmAVFGa94c6o/dmSdHlc4/1zJ96I6ak5TSVHZgRWZorpL:MdVie/dVdZg/akQ4wgl
MD5:	57947439B864E017FEED0D94316D5A8C
SHA1:	BB614192B65263446730B24D157A7DE812344394
SHA-256:	503F17F1EAD39E733BBF304E686D367D5C7051A5DF079F15B7E251B479959B13
SHA-512:	A92DEBE35193C72A490299C476E1EF20B2F072F735C20382892B0A008080C98CC087AB8623B3D7294D2105FA389C54E14A8CE04E8B060C7069AAC01C55F99330
Malicious:	false
IE Cache URL:	http://https://s.pinimg.com/ct/core.js
Preview:	!function(e){var r={};function u(n){if(r[n])return r[n].exports;var t=r[n]={i:n,l:!1,exports:{}};return e[n].call(t.exports,t,t.exports,u),t.l=!0,t.exports}u.m=e,u.c=r,u.d=function(n,t,e){u.o(n,t)||Object.defineProperty(n,t,{enumerable:!0,get:e})},u.r=function(n){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(n,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(n,"e",{value:!0})},u.t=function(t,n){if(1&n&&(t=u(t)),8&n)return t;if(4&n&&"object"==typeof t&&t&&t.e)return t;var e=Object.create(null);if(u.r(e),Object.defineProperty(e,"default",{enumerable:!0,value:t}),2&n&&"string"!=typeof t)for(var r in t)u.d(e,r,function(n){return t[n]}.bind(null,r));return e},u.n=function(n){var t=n&&n.e?function(){return n.default}:function(){return n};return u.d(t,"a",t),t},u.o=function(n,t){return Object.prototype.hasOwnProperty.call(n,t)},u.p="",u(u.s=0)}([function(n,t){!function(n,t){var e=n.createElement("script");e.async=!0,e.src="https://s.pinimg.com/ct/lib/main.c6c

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\f[1].txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	36812
Entropy (8bit):	5.495963300284302
Encrypted:	false
SSDEEP:	384:KEnScJ72pCWmKFnpMfG2X2G3LLa8L5BGQEHAkLTokXpjs4rECsNSDA7ojtgSJ1N3:x7ZWOHaQqLTok5hIijYe4O1csd
MD5:	5EF22C21B317FD3D68435F65D5D32C25
SHA1:	5BDF3EDE274481C5FA9DC71169719A6329D7F609
SHA-256:	92BD24374FB205C765A133D522ACB2772693D2CCD486B7855E2447918DE296A1
SHA-512:	F9FCE558D7900852C757872F8A707385FD274706AE5ACE9AC1610CD9F068FDD2045F8C64EE64C5C97EB762D7F0FE6557DCA32B94B9E6D853CD1B0979BEB2FB9
Malicious:	false
IE Cache URL:	http://https://www.googleadservices.com/pagead/conversion_async.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\f[1].txt	
Preview:	(function(){/* . . Copyright The Closure Library Authors. . SPDX-License-Identifier: Apache-2.0 .*/ .function aa(a){var b=0;return function(){return b<a.length?{done:!1,value:a[b++]}:{done:!0}}}var ba="function"==typeof Object.defineProperties?Object.defineProperty:function(a,b,c){if(a==Array.prototype||a==Object.prototype)return a;a[b]=c.value;return a}; .function ca(a){a=["object"==typeof globalThis&&globalThis,a,"object"==typeof window&&window,"object"==typeof self&&self,"object"==typeof global&&global];for(var b=0;b<a.length;++b){var c=a[b];if(c&&c.Math==Math)return c}throw Error("Cannot find global object");}var da=ca(this),ea="function"===typeof Symbol&&"symbol"===typeof Symbol("x"),l={},fa={};function t(a,b){var c=fa[b];if(null==c)return a[b];c=a[c];return void 0!==c?c:a[b]} .function v(a,b,c){if(b)a:{var d=a.split(".");a=1===d.length;var e=d[0],f;!a&&e in l?f=l:f=da;for(e=0;e<d.length-1;e++){var g=d[e];if(!(g in f))break a;f=f[g]}d=d[d.length-1];c=ea&&"es6"===c?f[d]:null;b=b(c)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\fbevents[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	96704
Entropy (8bit):	5.393965237573589
Encrypted:	false
SSDEEP:	1536:/M+OWtl6ay9Xes12KqQqfUThe7Kdv0a9slOs1jaV7vu5Dm20C+QNSMngySZYSIIa:/zOW5jSVnYDGeI
MD5:	7D0176E2E41E8C19FEBAD043A44369D2
SHA1:	74717141EE34016163D0625497697AEDB618E7EE
SHA-256:	F35FD99C15DE392199C3C5B116FAB65BB8AAAAA74BCF1C1729E9E01BB26780E7
SHA-512:	74C39F93E7638828E4E3C810B1B8BAA764048CCE4001E4A4677C66CF5BEE61C543C7C588BBE39D3D7B9E56233F4F3C2871B37CD0B2421F3EADEC8BC3FCB574AE
Malicious:	false
IE Cache URL:	http://https://connect.facebook.net/en_US/fbevents.js
Preview:	/**.* Copyright (c) 2017-present, Facebook, Inc. All rights reserved..*.* You are hereby granted a non-exclusive, worldwide, royalty-free license to use,.* copy, modify, and distribute this software in source code or binary form for use.* in connection with the web services and APIs provided by Facebook..*.* As with any software that integrates with the Facebook platform, your use of.* this software is subject to the Facebook Platform Policy.* [http://developers.facebook.com/policy/]. This copyright notice shall be.* included in all copies or substantial portions of the software..*.* THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR.* IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS.* FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR.* COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER.* IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN.* CONNECTION WI

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\frame-listener.bundle.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	12492
Entropy (8bit):	5.160419543755334
Encrypted:	false
SSDEEP:	192:3yEiy5RPrtX3wF++ATgkStaO3umwutHnvlAg6fyvumWUpx2PO+lAg68JD2kD63:3yQQFVQmwckf9mJQPe852T3
MD5:	D829108208F1EB9B9BC884C5E6C43A54
SHA1:	05A79B7F0738CFD2F2FE3C6CEBDBD0A7702EB44C
SHA-256:	22EE05C11B27143CF6474926408154A2723EC321249FAF6684BACA657F64B723
SHA-512:	51646E8E2B5557949EB5A77B10092ABA6E8575C17E696477CDEFF012687E857E9D01B5BD33E511892EFCB8292DB3781323C1CD7440CB9E41C82F8B298A849A1E
Malicious:	false
IE Cache URL:	http://https://static.parastorage.com/unpkg/data-capsule@1.0.83/dist/statics/frame-listener.bundle.min.js
Preview:	!function(e,t){"object"==typeof exports&&"object"==typeof module?module.exports=t():"function"==typeof define&&define.amd?define("data-capsule",[],t):"object"==typeof exports?exports["data-capsule"]=t():e["data-capsule"]=t()}("undefined"!=typeof self?self:this,function(){return function(e){function t(n){if(r[n])return r[n].exports;var o=r[n]={i:n,l:!1,exports:{}};return e[n].call(o.exports,o,o.exports,t),o.l=!0,o.exports}var r={};return t.m=e,t.c=r,t.d=function(e,r,n){t.o(e,r)||Object.defineProperty(e,r,{configurable:!1,enumerable:!0,get:n})},t.n=function(e){var r=e&&e.__esModule?function(){return e.default}:function(){return e};return t.d(r,"a",r),r},t.o=function(e,t){return Object.prototype.hasOwnProperty.call(e,t)},t.p="",t.p="undefined"!=typeof window&&window.__STATICS_BASE_URL__||t.p,t(t.s=54)}({0:function(e,t,r){"use strict";function n(e,t){if(!(e instanceof t))throw new TypeError("Cannot call a class as a function")}var o=function(){function e(e,t){for(var r=0;r<t.length;r++){va

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\gtm[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	251200
Entropy (8bit):	5.545139917818821
Encrypted:	false
SSDEEP:	6144:Sfv5PvoEJYGTZpIBHOPA3z/NSPBMUJwe/iuq9AUBNMMz5cMsohL:Sf4r96wR
MD5:	6BD8220EA6C33A8139F3FB541BFE9429
SHA1:	754986B0EC503A1C2828BBA557F55D0F73C71BCE
SHA-256:	FD06C6FF53E698E9F8EEC82E7BF66BD33A373F85721B8D0CF1D12F538D4C1784
SHA-512:	687AA194707C0FA04561BBF4C138F238E077A32393D5896685421CB891B172FFCC2006D7F91E3F47A86B0692454BC0A736111EF3B13B9164C174B19D8F9ADEED
Malicious:	false
IE Cache URL:	http://https://www.googletagmanager.com/gtm.js?id=GTM-MDD5C4

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\gtm[1].js	
Preview:	.// Copyright 2012 Google Inc. All rights reserved..(function(w,g){w[g]=w[g]||{};w[g].e=function(s){return eval(s);};})(window,'google_tag_manager');(function(){..var data = {."resource": {. "version":"579",. . "macros":[{. "function":"__e". },{. "function":"__u",. "vtp_component":"PATH",. "vtp_enableMultiQueryKeys":false,. "vtp_enableIgnoreEmptyQueryParam":false. },{. "function":"__j",. "vtp_name":"rendererModel.documentType". },{. "function":"__u",. "vtp_component":" HOST",. "vtp_enableMultiQueryKeys":false,. "vtp_enableIgnoreEmptyQueryParam":false. },{. "function":"__c",. "vtp_value":"wixed.wixeducation.com, signup.wixeducation.com, wixeducation.com". },{. "function":"__v",. "vtp_name":"postCategory",. "vtp_dataLayerVersion":1. },{. "function":"__k",. "vtp_name":"userType". },{. "function":"__u",. "vtp_enableMultiQueryKeys":false,. "vtp_enableIgnoreEmptyQue

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\insight.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	4774
Entropy (8bit):	5.518986103890679
Encrypted:	false
SSDEEP:	96:yvc+dEEqOmEM0fUBpL5CN6jKaYmd97KHijQcAoyvXe/J2Gnzr8D/e:x1EOEgzAK7N+oyvIJhv2e
MD5:	C4440888B2ED74F2A104115FC1D3C737
SHA1:	81359FD8D29CF6AFFD5B27317C379E53DDAEF00F
SHA-256:	6E6E6A03E72A528C28884B50BF296425667F38DD0AAF1DD17CE89199FFC85271
SHA-512:	5BE97F4FB111C4BBF32543B7581796AEBB3277585B5F7AF909E4E99765523ECCAFF300DA81533F6F0FE2A27D4A775DE3F3731E6B4E837B5070CC988A7A699C09
Malicious:	false
IE Cache URL:	http://https://snap.licdn.com/li.lms-analytics/insight.min.js
Preview:	!function(){"use strict";function n(){return(new Date).getTime()}function c(n,e){var i=n.cookie.match(new RegExp("(?:^|;)"+encodeURIComponent(e).replace(/([\.$?*|{}\(\)\[\]\\\/\+^])/g,"\\$1")+"=([^;]*)"));return i?decodeURIComponent(i[1]):""}function l(n,e,i,r){var o=r.days_until_expiration,t=void 0===o?1:o,a=r.path,d=void 0===a?"/":a,_=r.domain,c=void 0===_?null:_,l=function(n){var e=(new Date).getTime()+n,i=new Date;return i.setTime(e),i.toUTCString()}(864e5*t),s=encodeURIComponent(e)+"="+encodeURIComponent(i);s=s+";expires="+l,c&&(s=s+";domain="+c),s=s+";path="+d,n.cookie=s}function r(n){return n.webkit&&n.webkit.messageHandlers&&n.webkit.messageHandlers.LIPixli||!1}function e(n,e){var i="https://px.ads.linkedin.com/collect?"+e;r(n)?n.webkit.messageHandlers.LIPixli.postMessage(i):(new n.Image).src=i}function i(n,e){var i="https://px.ads.linkedin.com/insight_tag_errors.gif?"+e;r(n)?n.webkit.messageHandlers.LIPixli.postMessage(i):(new n.Image).src=i}function s(n){return n.map(functio

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\main.a9ba068a.bundle.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	175028
Entropy (8bit):	5.222342396636392
Encrypted:	false
SSDEEP:	1536:l4pmErcLf7p6gJL38jsD29HruZqr7+H9XvaLNr1ttlkLj7llHhBPAdk:pVVJL3L3oi9XyIoje
MD5:	8C73CAA238BB7708721AF6FD22CD5BCC
SHA1:	ECEB37269E2D0126EF65F1D5D492869365FDDBD4
SHA-256:	4828215E368CDDB0EBDAF5D047C35C70E172C6125B0F5CEB5775D70B8BEA8CB9
SHA-512:	29FCCC10409BA6278D9C5DB62F642FCA87600C52D9BAFA01BC82326BE6046366FBFCC03ED03016885844C60982326BF23F32475B8CD30D7C1738376E1499FDA
Malicious:	false
IE Cache URL:	http://https://static.parastorage.com/services/wix-thunderbolt/dist/main.a9ba068a.bundle.min.js
Preview:	(self.webpackJsonp__wix_thunderbolt_app=self.webpackJsonp__wix_thunderbolt_app||[]).push([[179,2892],{1721:function(e,t,n){"use strict";n.r(t),n.d(t,{ConsentPolicyAccessor:function(){return p}});var r,i={policy:"getCurrentConsentPolicy",header:"_getConsentPolicyHeader",isMethod:!0},o={policy:"consentPolicy",header:"consentPolicyHeader",isMethod:!1},a={essential:!0,dataToThirdParty:!0,advertising:!0,functional:!0,analytics:!0};function s(){return window}function u(){return self}function c(){return n.g}function d(){return globalThis}function l(e){var t;void 0===e&&(e=void 0),e&&(r=e),r||e||([d,c,u,s].forEach((function(e){try{r||(r=e())}catch(e){}})),r=r);try{"object"==typeof r.commonConfig&&r.commonConfig.consentPolicy&&(t=f(r.commonConfig,o)),t||"object"!=typeof r.consentPolicyManager||(t=f(r.consentPolicyManager,i)),t||"object"!=typeof r.Wix||"object"!=typeof r.Wix.Utils||"function"!=typeof r.Wix.Utils.getCurrentConsentPolicy||(t=f(r.Wix.Utils,i))}catch(e){}return t}function f(e,t){ret

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\mobileLayoutUtils.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	21421
Entropy (8bit):	5.165376477490233
Encrypted:	false
SSDEEP:	384:AnDgYzuD8GKit4jLQL3UC1rj5314n9UvjFZ9QjlEkI:C9BYfJZ9I2r
MD5:	F9312036ED8D97FBF474A25E24B3CE64
SHA1:	26198A3647E40E7E22BD58739CE1D497A707A10D
SHA-256:	4B7ED33BC551F23E4CDB54C2A9D05DAEA0A718FFD911049E8D762DFE8E59B2DE
SHA-512:	8029D8FEFB6640EACA822749B7158B04B041BA9FABB11D2CE18428DDE6A5BB752FD08F8DECAD07C6AC1BD915CE4C659FF7386A10CFB28242DAB63A82B63B7963
Malicious:	false
IE Cache URL:	http://https://static.parastorage.com/unpkg/@wix/santa-mobile-core@1.1233.0/dist/mobileLayoutUtils.min.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\mobileLayoutUtils.min[1].js	
Preview:	define(["lodash","coreUtilsLib"],(function(n,t){return function(n){var t={};function e(r){if(t[r])return t[r].exports;var o=t[r]={i:r,l:!1,exports:{}};return n[r].call(o.exports,o,o.exports,e),o.l=!0,o.exports}return e.m=n,e.c=t,e.d=function(n,t,r){e.o(n,t)||Object.defineProperty(n,t,{enumerable:!0,get:r})},e.r=function(n){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(n,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(n,"__esModule",{value:!0})},e.t=function(n,t){if(1&t&&(n=e(n)),8&t)return n;if(4&t&&"object"==typeof n&&n&&n.__esModule)return n;var r=Object.create(null);if(e.r(r),Object.defineProperty(r,"default",{enumerable:!0,value:n}),2&t&&"string"!=typeof n)for(var o in n)e.d(r,o,function(t){return n[t]}.bind(null,o));return r},e.n=function(n){var t=n&&n.__esModule?function(){return n.default}:function(){return n};return e.d(t,"a",t),t},e.o=function(n,t){return Object.prototype.hasOwnProperty.call(n,t)},e.p="",e(e.s=8)}([function(t,e){t.exports=n},

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\polyfill.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	downloaded
Size (bytes):	22629
Entropy (8bit):	5.262393792354482
Encrypted:	false
SSDEEP:	384:x/2ggnPTclMcL65uNlPvgtDj6WnW+Y6/cTxJtlwMHnWazh5vd2uZvOC1:x/hL60NlPkW+F/cTxfXHWazhDXZvOC1
MD5:	42E531D2C282ACC7A2EC77E00CEC1D10
SHA1:	87B8F7A381B07C2771F3CF4B651F304470B5F4D8
SHA-256:	38F84B4BF4D91C67D64FFBEE5CC4B6A39BAA9653E5369532D902F9F06F650A57
SHA-512:	BAC8A94B872E3E196CA45906E2780ED1E546B42DDC2318A9FF4F1B4D14EF7FC49783160C3295AD39B54C1B051DE61F7BCBF2935C5FD368E24B2E5E39FDA00F6
Malicious:	false
IE Cache URL:	http://https://polyfill.io/v3/polyfill.min.js?features=fetch
Preview:	/* Disable minification (remove `.min` from URL path) for more info */..(function(self, undefined) {function Call(t,l){var n=arguments.length>2?arguments[2]:[];if(!1===IsCallable(t))throw new TypeError(Object.prototype.toString.call(t)+"is not a function.");return t.apply(l,n)}function CreateMethodProperty(e,r,t){var a={value:t,writable:!0,enumerable:!1,configurable:!0};Object.defineProperty(e,r,a)}function Get(n,t){return n[t]}function HasOwnProperty(r,t){return Object.prototype.hasOwnProperty.call(r,t)}function IsCallable(n){return"function"==typeof n}function SameValueNonNumber(e,n){return e===n}function ToObject(e){if(null===e||e===undefined)throw TypeError();return Object(e)}function GetV(t,e){return ToObject(t)[e]}function GetMethod(e,n){var r=GetV(e,n);if(null===r||r===undefined)return undefined;if(!1===IsCallable(r))throw new TypeError("Method not callable: "+n);return r}function Type(e){switch(typeof e){case"undefined":return"undefined";case"boolean":return"boolean";case"numbe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\viewerScript.bundle.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	94323
Entropy (8bit):	5.260793419988244
Encrypted:	false
SSDEEP:	768:V97OQJdeLADrR41xhos4FrqRr3DVsIeuGGROnCjCNCxUAuCKsah5CAZ46EhC4tih:V9yQPLDt4BKq3523c2G6KE2nCvPRknw
MD5:	89FF53B24905C33CB74C5831238E80AE
SHA1:	E7971439BF381FD02F6AAFF879BB05726D47A7AD
SHA-256:	F48DE2017182C4BA6F7011A1B6CDBFB3BBB25C4B285393009E9944198EBB4DC8
SHA-512:	E52B69792B95F85C069CD34FA41884EA6430F465307D4C99F45B7C77124976A252C8F6186B54A2985EF2D7BE3773A9BD580DBAE7FB6393E920122EB4219A255B
Malicious:	false
IE Cache URL:	http://https://static.parastorage.com/services/profile-card-tpa-ooi/1.277.0/viewerScript.bundle.min.js
Preview:	!function(e,t){"object"==typeof exports&&"object"==typeof module?module.exports=t():"function"==typeof define&&define.amd?define([],t):"object"==typeof exports?exports.viewerScript=t():e.viewerScript=t()}(self,(function(){return function(e){var t={};function n(r){if(t[r])return t[r].exports;var o=t[r]={i:r,l:!1,exports:{}};return e[r].call(o.exports,o,o.exports,n),o.l=!0,o.exports}return n.m=e,n.c=t,n.d=function(e,t,r){n.o(e,t)||Object.defineProperty(e,t,{enumerable:!0,get:r})},n.r=function(e){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(e,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(e,"__esModule",{value:!0})},n.t=function(e,t){if(1&t&&(e=n(e)),8&t)return e;if(4&t&&"object"==typeof e&&e&&e.__esModule)return e;var r=Object.create(null);if(n.r(r),Object.defineProperty(r,"default",{enumerable:!0,value:e}),2&t&&"string"!=typeof e)for(var o in e)n.d(r,o,function(t){return e[t]}.bind(null,o));return r},n.n=function(e){var t=e&&e.__esModule?function(){r

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\wix-dom-sanitizer[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	19220
Entropy (8bit):	5.284078809599163
Encrypted:	false
SSDEEP:	384:3YyrTijbyGi/LA7A0MpCdzxv8ZlMiIV/iMewjtYC23MiVjfhuYrY9:vTxLsd9v8bMiS/iDGtYC23ZbuYr2
MD5:	BF53692C2D49A9E59E611AF682416BB4
SHA1:	87ED7DA4FD43B66A124D4180CE69596C88672F6D
SHA-256:	76F4A71B7ED39504017336D133F172CECEF1B2505E2557746E44F4647097BE5E
SHA-512:	B7BCA4D406D02950A849709DA913B2B4A0DD4A2F3E9B0CD5A4A9E93301F59F8F5F5C168D3EA80FC4A3BE9541848F806F415157FF07CB604A28D315A3E12A1DD5
Malicious:	false
IE Cache URL:	http://https://static.parastorage.com/unpkg/@wix/wix-dom-sanitizer@1.783.0/dist/wix-dom-sanitizer.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\wix-dom-sanitizer[1].js	
Preview:	!function(e,t){"object"==typeof exports&&"object"==typeof module?module.exports=t():"function"==typeof define&&define.amd?define([],t):"object"==typeof exports?exports["wix-dom-sanitizer"]=t():e["wix-dom-sanitizer"]=t()}(this,(function(){return function(e){var t={};function r(n){if(t[n])return t[n].exports;var o=t[n]={i:n,l:!1,exports:{}};return e[n].call(o.exports,o,o.exports,r),o.l=!0,o.exports}return r.m=e,r.c=t,r.d=function(e,t,n){r.o(e,t)||Object.defineProperty(e,t,{enumerable:!0,get:n})},r.r=function(e){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(e,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(e,"__esModule",{value:!0})},r.t=function(e,t){if(1&t&&(e=r(e)),8&t)return e;if(4&t&&"object"==typeof e&&e&&e.__esModule)return e;var n=Object.create(null);if(r.r(n),Object.defineProperty(n,"default",{enumerable:!0,value:e}),2&t&&"string"!=typeof e)for(var o in e)r.d(n,o,function(t){return e[t]}.bind(null,o));return n},r.n=function(e){var t=e&&e.__esMod

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\1006927621[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped
Size (bytes):	42
Entropy (8bit):	2.9881439641616536
Encrypted:	false
SSDEEP:	3:CUXPQE/xlEy:1QEoy
MD5:	D89746888DA2D9510B64A9F031EAECD5
SHA1:	D5FCEB6532643D0D84FFE09C40C481ECDF59E15A
SHA-256:	EF1955AE757C8B966C83248350331BD3A30F658CED11F387F8EBF05AB3368629
SHA-512:	D5DA26B5D496EDB0221DF1A4057A8B0285D15592A8F8DC7016A294DF37ED335F3FDE6A2252962E0DF38B62847F8B771463A0124EF3F84299F262ED9D9D3CEE4
Malicious:	false
Preview:	GIF89a.............!.......,...........D.;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\36c796_223f054ee81b4205b73998fe4dce1fb2~mv2[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=6, orientation=upper-left, xresolution=86, yresolution=94, resolutionunit=2], progressive, precision 8, 245x98, frames 3
Category:	dropped
Size (bytes):	6445
Entropy (8bit):	7.805944024842776
Encrypted:	false
SSDEEP:	96:0eOwnsafCc7CNYqZNv5ofSWxxDOdJ+uNMhBjJ+GLMZBU/faQ57DbxXkV:PyiCcmNYGgvVdNBjJDx/SQdxXkV
MD5:	639FBF0EAFE4AECDBBBAFCA7A2851D48
SHA1:	D00CD2EA32466878BCF42E555A20387D85886594
SHA-256:	14540CBA108F63B6A17B23C9DA7387F04C19BB75B582DB684719163ADA14297D
SHA-512:	F50893D45622031C270533D52747F435D743182F0E99188029B5A725230B1F0E681F6799F71CE49E34F3EEE35F2BA9D49BE0659864B242AB015AFCB99EA2DDE9
Malicious:	false
Preview:	......JFIF.............Exif..II*..........................V..........^...(......................i.......f.......8c......8c................0210...................0100..............................b..........C.................................... .%...#... , #&')*)..-0-(0%()(...C...........(...((......b...o......x6.[.!6.|.[....b..[..E@P"..i..ZW ...AYwL.r.D...7..,#Y.....BpZR.VYh.=4.H6{T.=.dud.z..LT.o.l;....L.../..%...:w/.-'.&."...sl...m-...v.={L..X..h.f.,7...E.<..vrT:...m.M.I.u.../....{'...U.HqJ..(.iVr.8.........1...M.CH..A..`...,.f .1.............U.........V#-....W..r+.....3hk.T...'y.. .n.^.t.9.E5].A.:..e...%./Z......AW.`..+3:.0.....N3.f0........us....;."0].i(M....[.n..!i....N.]\".x..F.....".ru..-.......o..;.s.....{ol2.F.r...i>..3(..i.Du. [G.x.........:...V.J..O#i9....eT..UW!v[H.x..@z.]....l....B.1U._.V.%.*6..%l..f.x:..:#.j

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\3d84bae5ad4d4d8a96de15e9f4b79a08[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	1385
Entropy (8bit):	4.129066840649089
Encrypted:	false
SSDEEP:	24:tCzcRj04WwUzoJpfM6Ve6KmZYRVILgQqTmXMIIXuK7KLAWF3Ds5YuFQaAE:wijf/M0pf9V5fYOgQqTmXotOLBghFQab
MD5:	4D0FFCA03B31AE92FB3459ACF490DB9A
SHA1:	4D94E2F3BEF0A284997C1D18EAF83514C40F1F72
SHA-256:	C2DC7E0BECDBAB5E9A5C79E527BB95FEC10667645CC6F2F8177F5E0F4F585EA1
SHA-512:	D69CFBFF8A535504DB28F6850A7CD6978364896647BA16821606042BD839AC94D783AC693A14258EED993EC63C314EFDE399BBF1DA11E2C51E001FB311DCE34
Malicious:	false
IE Cache URL:	http://https://static.wixstatic.com/shapes/3d84bae5ad4d4d8a96de15e9f4b79a08.svg
Preview:	<svg data-bbox="0 0 50 50" data-type="shape" xmlns="http://www.w3.org/2000/svg" width="50" height="50" viewBox="0 0 50 50">. <g>. <path d="M25 48.077c-5.924 0-11.31-2.252-15.396-5.921 2.254-5.362 7.492-8.267 15.373-8.267 7.889 0 13.139 3.044 15.408 8.418-4.084 3.659-9.471 5.77-15.385 5.77m.278-35.3c4.927 0 8.611 3.812 8.611 8.878 0 5.21-3.875 9.456-8.611 9.456s-8.611-4.246-8.611-9.456c0-5.066 3.684-8.878 8.611-8.878M25 0C11.193 0 0 11.193 0 25c0 .915.056 1.816.152 2.705.032.295.091.581.133.873.085.589.173 1.176.298 1.751.073.338.169.665.256.997.135.515.273 1.027.439 1.529.114.342.243.675.37 1.01.18.476.369.945.577 1.406.149.331.308.657.472.98.225.446.463.883.714 1.313.182.312.365.619.56.922.272.423.56.832.856 1.237.207.284.41.568.629.841.325.408.671.796 1.02 1 .182.22.244.432.494.662.728.405.415.833.801 1.265 1.186.173.154.329.325.507.475l.004-.011A24.886 24.886 0 0 0 25 50a24.881 24.881 0 0 0 16.069-5.861.126.126 0 0 1 .003.01c.172-.144.324-.309.49-.458.442-.392.88-.787 1.293

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\642100862[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\642100862[1].gif	
Category:	dropped
Size (bytes):	84
Entropy (8bit):	2.9881439641616536
Encrypted:	false
SSDEEP:	3:CUXPQE/xlEqjdfXPQE/xlEy:1QEoqh3QEoy
MD5:	6A3F2D147842187CD48B1546EDDD5BA0
SHA1:	AB278C31189DF2939428CF81A3850A2C6DBF5E2E
SHA-256:	D4990F907BCA02F02B3D41216EEA5461609D4BCBA07A3CBEE0D7CF28A6D0D864
SHA-512:	998F55BF5C3D4A71CB3C23782B788F71E7625DF83A37FE8A18F915AAA3BDE5420183A3C709816664E262069EE2FE245CA44799E3476B6DE507B5D68FC86F8960
Malicious:	false
Preview:	GIF89a.....!.....,.....D.;GIF89a.....!.....,.....D.;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\819384062[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped
Size (bytes):	84
Entropy (8bit):	2.9881439641616536
Encrypted:	false
SSDEEP:	3:CUXPQE/xlEqjdfXPQE/xlEy:1QEoqh3QEoy
MD5:	6A3F2D147842187CD48B1546EDDD5BA0
SHA1:	AB278C31189DF2939428CF81A3850A2C6DBF5E2E
SHA-256:	D4990F907BCA02F02B3D41216EEA5461609D4BCBA07A3CBEE0D7CF28A6D0D864
SHA-512:	998F55BF5C3D4A71CB3C23782B788F71E7625DF83A37FE8A18F915AAA3BDE5420183A3C709816664E262069EE2FE245CA44799E3476B6DE507B5D68FC86F8960
Malicious:	false
Preview:	GIF89a.....!.....,.....D.;GIF89a.....!.....,.....D.;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\WixMadeforText_W_BdIt[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 28692, version 1.13107
Category:	downloaded
Size (bytes):	28692
Entropy (8bit):	7.984015162753741
Encrypted:	false
SSDEEP:	384:0xmMzIjVGNHUnD6SundIUZ9mIqA3b/zdaijMACAE9MVYlJMp2PXO9T9BVzdcAkQO:PWggdIUZw4na1z/TPXmVSAnZFG
MD5:	9557403059EA8B62EF946E44250971FA
SHA1:	F5D7EA5B2DDE5D291490E7AF03DD72E70114299B
SHA-256:	0871C5BF40DA6C907DFD85E3803AC0A950029E66BA1C970B7F4BD5F713541B59
SHA-512:	AF18FEA8D59897ED48B46477A1A4DC8969280302EC3717C284BC671BBB89BF3C93BC1DB8EBD996254FEC392D86FE8D489D3E32EF8B81B0DE537146E7533713 0
Malicious:	false
IE Cache URL:	http://https://static.parastorage.com/services/santa-resources/resources/viewer/user-site-fonts/fonts/WixMadefor/v2/WixMadeforText_W_BdIt.woff
Preview:	wOFF.....p.....33.....GDEF..]....."."!GPOS..]....x..H.....GSUB..l.....fOS/2.....\...`....cmap...h.....X..:.cvt .....$..Afpgm...x.....0.6gasp..\.....glyf... T..H[..u....Khead.....6...6.D..hhea.....$...$.g..hmtx...X.....h..-*loca.....w....i.K.maxp..... ... .9..name..[....,....DCnEpost..\..... ...@prep...$.....Q.T.....33...._.<..... .....O...X...../.a.....x.%...Q.....Q.t7.....-t.{.....e..S..O.>...s....;.].^..R.\./..0..O.s..F.|.....Zx....4Y..oR.m.m..m.m.m..jjfz..|'y.... o.K....UP%.x&.Gk++...*V...:.....^W.j...#.J.TI?.....J..n*..f.g?iWo.?.....U....Q7...R.3..V.[..y|f[..vL.d[.W....F..%.W..t..i...mMn.h.m.....{#.....:.."z/...z..nhn...^.....q.Do.zS.....7. .....9U..ir..L.PW?R.|+M..U.>...q[.v..I.}.....a.....+..H..Sb.....#.Ym._...29G.a#.....%|..%..w.Z.lU<e?..N.1..<j.....[.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\WixMadeforText_W_Bd[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 26940, version 1.13107
Category:	downloaded
Size (bytes):	26940
Entropy (8bit):	7.983196044654624
Encrypted:	false
SSDEEP:	768:ei+5ISPc4Mq85akb8yCh/uX2Qfvj566p4ruUR2FG:waSPcNq85dzChGGYJKruURb
MD5:	1B77CABA6C9D4D264DD5E101A8326D9D
SHA1:	0AEF11FFF06D2A166705A50E44E545B3D7FE5DF3
SHA-256:	640522494DAF6FB6A791DC1D67AE7A3884D25F87E439A83EC59BAF71D5E39D63
SHA-512:	BA83A6976FB8329D04EBD8897F863289AF694EFC34291D248BE9F9D576E43B61B4B261F2453B89A68BFA8BDC2CB16600B565CED54AFAB47611076A42A6B6EB5 1
Malicious:	false
IE Cache URL:	http://https://static.parastorage.com/services/santa-resources/resources/viewer/user-site-fonts/fonts/WixMadefor/v2/WixMadeforText_W_Bd.woff

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\WixMadeforText_W_Bd[1].woff	
Preview:	wOFF.....i<.....33.....GDEF..WP.....".."!GPOS..W....O..C....qGSUB..e,.....fOS/2.....Y...`....cmap.....X..:.cvt ...d.....$..Afpgm.....0.6gasp..WD..... ...glyf.....Co..s.x..head.....6...6..I.hhea..... ...$...Fhmtx...T...\...h.3<aloca...$...v.....}c.maxp..... ... .9..name..V....!....=tidpost..W0..... ...@prep...l.....Q.T.....33..._.<.... .....+/.....&.....x.c`d``....e.....X..EP..-.....M...X...../.a.....x.%....0../..Q(\....[..{.. .d....wx....d.$.....LC.f...w....@.`<..H.|iy.h..t..I.@....!.[...x.....Y..OU?.m.k.m.. .q..m..._en..\"\M...(.c_k...Z...&.....7:..h...-.r..Z..w.Q.~EW..#\'.....p..??H#.'..c...WW?[C}-..5.W.x.C#X..s.....O..P.....U.;F.mw.ND.Q....'..!.....4'..nS;r..k.t....7L.....+.N....`7..... ..i.o..~..S...nb.^.f.k. .*.ubL-6W.K.^m.....-.].x..`S..TG.....e?i..q\.Av.:..v.....;..z.....F..\m.....m`..;..z.....h.N....w.w.....+Z.....5.....m..>.~.../=;..i...>~(.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\WixMadeforText_W_MdIt[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 29748, version 1.13107
Category:	downloaded
Size (bytes):	29748
Entropy (8bit):	7.985185178927653
Encrypted:	false
SSDEEP:	768:HnkhSzpM44Q3IOYkOyF9afGJ2zeEwILUppcQKRWAUXFSEgFG:Hkh0xwuhbafGJ2dLMUWA2Sy
MD5:	32F3E3707D0AB7F9D86367FB30425ABF
SHA1:	BE74B2636AE55828943F0145479557A1F44FBD8A
SHA-256:	0570726D9B35862B303637EFFD8718EE7E2BE3088EFFD566BEE07D443AEEE6EB
SHA-512:	10639864512919815EC77AFC5EBB457495BCC0B2F8E118AA63236B2354B2D069DF26E295B00ED68C30B0CE43B3A8FF72319CDFC26972112C70B72007F4DE2C5F
Malicious:	false
IE Cache URL:	http://https://static.parastorage.com/services/santa-resources/resources/viewer/user-site-fonts/fonts/WixMadefor/v2/WixMadeforText_W_MdIt.woff
Preview:	wOFF.....t4.....d..33.....GDEF..._.....".."!GPOS..``.....J.D..vGSUB..p$.....fOS/2.....\...`.=..cmap...X.....X..:.cvt .....&...fpgm...h.....0.6gasp.._..... ...glyf...,..JJ..yta...head.....6...6.@..hhea.....#...$....hmtx...X.....h..<tloca.....y....t.U.maxp..... ... .D..name..^x...5...PP.}.post.._..... ...@prep.....B.es.....33.ld._.<.. .....x.c`d``.....,..._0\f@.....P...U...../.a.....x.%..AQ.....2.Jw;k.-T..Z...b..H.{9...:....So..Y.ld.u..M.zj..@8.]..|;..Yn...>$..@.....cx....%A.D.j.m.m.m. m.m....;....Z..._>!....G.!....7....o.sq0[&c.....{.....~.....u.1...?...g...8.....4.BkKd.RH..H3.).'.P\.....|g~G:..2..9.-C...h2.uyn..@..l<WP: ..A9.s.\...R/$.e...~.H&.7.{"C./..P.....ss.W ...^U..^S..S...m..D.6p....h4.8...Y...^d.IH..PI. .vFY.(..+.....Hw.uc.O.j...{..Y.a!Z...b....%Hp9....CI;g!...W$.4..).....'..y.+ ..7... 71S.1f3..i&.l.K.z..1%3}1.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\WixMadeforText_W_Md[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 27876, version 1.13107
Category:	downloaded
Size (bytes):	27876
Entropy (8bit):	7.981912701503317
Encrypted:	false
SSDEEP:	768:4ykhSNOuWMXnoEpsfdZnfNPlNtH5E4dVQFG:zkhsOuPK1zP7tZEGB
MD5:	7EFC62924AA0D697C0FE9592A2DA44A5
SHA1:	27D1436BD7E9C36ECCBD295622584E1332E8DDE5
SHA-256:	158A4B3011AB5707FA5A4AE4FD3858A187A13022E1AA9C98EE5ACDF04AC4C6BF
SHA-512:	5F659A9D77DD36DE3AAD302FE1003E2A14A35E02C861E35F8B0C72D2BE8AB809FBBB0FEE64958BDC5F2399DC2A5C4DEA48AE6805DB36B30B7260151FAA6E6 1F
Malicious:	false
IE Cache URL:	http://https://static.parastorage.com/services/santa-resources/resources/viewer/user-site-fonts/fonts/WixMadefor/v2/WixMadeforText_W_Md.woff
Preview:	wOFF.....l.....33.....GDEF..Zp.....".."!GPOS..Z.....C.I..GSUB..h.....fOS/2.....[...`.=..cmap.....X..:.cvt ...L.....&...fpgm.....0.6gasp..Zd.....glyf.... ..E...v"A7..head.....6...6.sI.hhea..... ...$...Rhmtx...T...i...h..l.loca.....v.....k.maxp..... ... .D..name..Y....3....C.u$post..ZP..... ...@prep...|.....B.es.....332..._.<.....+/ .....1.....x.c`d``....e....WXZ."(.....N...X...../.a.....x.%....P...+^Q.....3L...;.....-....x.....#..l.....,.K.P.*(5.....Pz.cR.....x.....;..W.....m[.m.m...c.m{.6m .U<s./...z.N....Y.....z..=m.m..t.....U..c.xk..N...O.<...k...J.....,@..D.d....r...\.....G.z...ID..h.B.z...Qd.7..u....n.....i....;v.0...C.....d(..a...H..%!$....j..^J...3....y.4[.kj. A..V..HV.Y._$ ..r^[q.....%..U...N.sP..fo.P`.`.r...r.W.T."....N.....H.w9...z...8.N..<....4T....q.T.:.L.w.:.I.KH.a.U..N...../Z;..O..W"A..B..do;.....2..d.x.gI..h...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\bolt-custom-elements.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	151032
Entropy (8bit):	5.418493775650687
Encrypted:	false
SSDEEP:	1536:QlvITGyprshqtSVR+/w4Dd/Td4YzabkBwZFh5KTuECsWufGY:YwJrshRmWQW5B0
MD5:	74617A356F6C89B687D1119B3D2B532C
SHA1:	D24C8CCACE36E06B20D51595A8F0BB9B1F6148AC
SHA-256:	3E5CED91EFBF38CB2FBF01DA33BBDE1B54FFD75C9D4E46C5A1C72928A0501E6E
SHA-512:	D0917569880CAC7FA4522817CA549A3674BE532D8FE33D5B90892C3795CF10947D80367C33D4F2B6991DF747F6B6640C1474C3B7566C416762EE7790E08922D6
Malicious:	false
IE Cache URL:	http://https://static.parastorage.com/services/wix-bolt/1.7264.0/bolt-main/app/bolt-custom-elements.min.js
Preview:	var customElementsPackage=function(e){var t={};function i(r){if(t[r])return t[r].exports;var n=t[r]={i:r,l:!1,exports:{}};return e[r].call(n.exports,n,n.exports,i),n.l=!0,n.exports }return i.m=e,i.c=t,i.d=function(e,t,r){i.o(e,t)||Object.defineProperty(e,t,{enumerable:!0,get:r})},i.r=function(e){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object .defineProperty(e,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(e,"__esModule",{value:!0})},i.t=function(e,t){if(1&t&&(e=i(e)),8&t)return e;if(4&t&&"object"= =typeof e&&e&&e.__esModule)return e;var r=Object.create(null);if(i.r(r),Object.defineProperty(r,"default",{enumerable:!0,value:e}),2&t&&"string"!=typeof e)for(var n in e) i.d(r,n,function(t){return e[t]}.bind(null,n));return r},i.n=function(e){var t=e&&e.__esModule?function(){return e.default}:function(){return e};return i.d(t,"a",t),t},i.o=function(e,t) {return Object.prototype.hasOwnProperty.call(e,t)},i.p="",i(i.s=1)}([function(e,t,i){e.exports=function(e){var t={};function

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\bolt-custom-elements.min[1].js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\clientWorker.0eb5dbb0.bundle.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	460295
Entropy (8bit):	5.376096939854045
Encrypted:	false
SSDEEP:	6144:I2n2cQIY6Um+0pxSTvcLMW2P2Dw5Fj3UG/f6Hr:9Q16UmC0
MD5:	880560D747C808A74D002B46F6694083
SHA1:	0769072C4D4C91321FCCF8E20455F3F93CF692DC
SHA-256:	654B21E72D445BD5010627EBA4639C65A51C8B2B92E83F3F63B2B1ED5EC5A339
SHA-512:	E95EEE511E113A6CE9D03E04B8CABF26CB854CD7D6EE39F7023605E23440526C6A3E76755C7E9FD4CF00121ED97C5EC81F04BCA5CCE31C38BE007971C8B4B D8
Malicious:	false
IE Cache URL:	http://https://www.artsenvoorwaarheid.nl/_partials/wix-thunderbolt/dist/clientWorker.0eb5dbb0.bundle.min.js
Preview:	/*! For license information please see clientWorker.0eb5dbb0.bundle.min.js.LICENSE.txt */.!function(e,t){"object"==typeof exports&&"object"==typeof module?module.exports=t():"function"==typeof define&&define.amd?define([],t):"object"==typeof exports?exports.clientWorker=t():e.clientWorker=t()}(self,(function(){return function(){var __webpack_modules__={7788:function(e,t,n){"use strict";n.d(t,{RR:function(){return u},wM:function(){return c},u_:function(){return f},gk:function(){return h}});var r=n(1683),o=n(5605),i=n(7276),a=function(){return(a=Object.assign||function(e){for(var t,n=1,r=arguments.length;n<r;n++)for(var o in t=arguments[n])Object.prototype.hasOwnProperty.call(t,o)&&(e[o]=t[o]);return e}).apply(this,arguments)},s=function(){for(var e=0,t=0,n=arguments.length;t<n;t++)e+=arguments[t].length;var r=Array(e),o=0;for(t=0;t<n;t++)for(var i=arguments[t],a=0,s=i.length;a<s;a++,o++)r[o]=i[a];return r},u=function(e,t){var n=Object.values(e).reduce((function(e,n){var r;return a(a({},

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\coreUtils.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	116660
Entropy (8bit):	5.3522050762988025
Encrypted:	false
SSDEEP:	3072:3Svggjht6Jf0Cd6SKB3YFZn7Svu6NtDYRWq:EBoINtMP
MD5:	0FE10139CBFED012C055D8A44B10641A
SHA1:	65199F4D007FB04D255A7C97A7C5A369D61810DB
SHA-256:	F61C07CF695B3F699393F9BF4024F36D221D57B90B58D9BA90A301B3F502876F
SHA-512:	F7A88FFC38B9A89D60647F9F784064380C7901C5F08C32C9A19C6D95EB2D1A4618BB9E14EDD72C23DAAFE15FCA9D6293690DE0359BAC3DD0CB2D702E253D52 E
Malicious:	false
IE Cache URL:	http://https://static.parastorage.com/services/wix-bolt/1.7264.0/node_modules/wix-santa/dist/packages-bin/coreUtils/coreUtils.min.js
Preview:	define("coreUtils",["lodash","warmupUtils","santa-core-utils","warmupUtilsLib","color","thirdPartyAnalytics","xss","data-capsule","mobileLayoutUtils"],(function(e,t,n,o,r,a,i,s,c){return function(e){var t={};function n(o){if(t[o])return t[o].exports;var r=t[o]={i:o,l:!1,exports:{}};return e[o].call(r.exports,r,r.exports,n),r.l=!0,r.exports}return n.m=e,n.c=t,n.d=function(e,t,o){n.o(e,t)||Object.defineProperty(e,t,{enumerable:!0,get:o})},n.r=function(e){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(e,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(e,"__esModule",{value:!0})},n.t=function(e,t){if(1&t&&(e=n(e)),8&t)return e;if(4&t&&"object"==typeof e&&e&&e.__esModule)return e;var o=Object.create(null);if(n.r(o),Object.defineProperty(o,"default",{enumerable:!0,value:e}),2&t&&"string"!=typeof e)for(var r in e)n.d(o,r,function(t){return e[t]}.bind(null,r));return o},n.n=function(e){var t=e&&e.__esModule?function(){return e.default}:function(){return e};retu

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\f[1].txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	2064
Entropy (8bit):	5.849226562863793
Encrypted:	false
SSDEEP:	48:0VUUIqzPrqTnJcgVhkGTQEJKggygOYxp7Fv7RZtnEOq0gs:+UURWTCgVhk8QEJYLXlZA0n
MD5:	596FC55C4F3FD615BB6969F664A464A3
SHA1:	4527C26560ED03822973BD20B88AEB2ED711BCD6
SHA-256:	A2982DC41BFC01CDC6E82B4B28B5C3738C9C93E44B04432FA78BC948C04E4ABD
SHA-512:	5B8C9D39E6C14B286EBD59BAEE276C41E5FCA48B7800D8466F50A733844AE5A1592D4F0CF5FC68EBDE0726BBEE5CF9F46EDE1730F575DDE4BF754C71E1C41 B2
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\f[1].txt	
Preview:	(function(){var s = {};(function(){/* Copyright The Closure Library Authors. SPDX-License-Identifier: Apache-2.0 */ var c={},f=this||self;var l=/#|$/;function n(d){var g =d.search(l),a;a:{for(a=0;0<=(a=d.indexOf("fmt",a))&&a<g;){var b=d.charCodeAt(a-1);if(38==b||63==b)if(b=d.charCodeAt(a+3),!b||61==b||38==b||35==b)break a;a+=4}a=-1}if(0>a)return null;b=d.indexOf("&",a);if(0>b||b>g)b=g;a+=4;return decodeURIComponent(d.substr(a,b-a).replace(/\+/g," "))};function r(d,g,a){function b(){--p;if(0>=p){var e;(e=d.GooglebQhCsO)||(e={});var q=e[g];q&&(delete e[g],(e=q[0])&&e.call&&e())}}for(var p=a.length+1,m=0;m<a.length;m++){var h=n(a[m]),k=null;1!=h&&2!=h||!(h=d.document.getElementById("goog_conv_iframe"))||h.src||(k=h);k||(k=new Image);k.onload=b;k.src=a[m]}b()}var t=["ss_"],u=s||f;t[0]in u||"undefined"==typeof u.execScript||u.execScript("var "+t[0]); for(var v;t.length&&(v=t.shift());)t.length||void 0===r?u[v]&&u[v]!==Object.prototype[v]?u=u[v]:u=u[v]={}:u[v]=r;}).call(this);;s.ss_(window,'

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\f[2].txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	2721
Entropy (8bit):	5.789718297930108
Encrypted:	false
SSDEEP:	48:0VUUIqzPrqTnJcgVhkG5NhggOlp7Fv7RZtqalkBbqhggOlp7Fv7RZtqalkB06:+UURWTCgVhk2NhFl0hBehFl0hBN
MD5:	2C0C28B10AD9BF05FBA5F0542B5A26F2
SHA1:	B3DF5F1839EB1A1A8497B29F99FEB072A4EF0891
SHA-256:	22A0E2368C1E68B800A539F972336AA5C9C6A376388B3267688D105FC4C2DAC9
SHA-512:	CC4FBB496E4024D412FC42B16A1AC863A141AE0A6E76C326875C54B11D416A63B5B690C3F5D5DEB2397B6A3E70019FC97FD9B3F3FF98FFC724D38A08D3CCF61
Malicious:	false
Preview:	(function(){var s = {};(function(){/* Copyright The Closure Library Authors. SPDX-License-Identifier: Apache-2.0 */ var c={},f=this||self;var l=/#|$/;function n(d){var g =d.search(l),a;a:{for(a=0;0<=(a=d.indexOf("fmt",a))&&a<g;){var b=d.charCodeAt(a-1);if(38==b||63==b)if(b=d.charCodeAt(a+3),!b||61==b||38==b||35==b)break a;a+=4}a=-1}if(0>a)return null;b=d.indexOf("&",a);if(0>b||b>g)b=g;a+=4;return decodeURIComponent(d.substr(a,b-a).replace(/\+/g," "))};function r(d,g,a){function b(){--p;if(0>=p){var e;(e=d.GooglebQhCsO)||(e={});var q=e[g];q&&(delete e[g],(e=q[0])&&e.call&&e())}}for(var p=a.length+1,m=0;m<a.length;m++){var h=n(a[m]),k=null;1!=h&&2!=h||!(h=d.document.getElementById("goog_conv_iframe"))||h.src||(k=h);k||(k=new Image);k.onload=b;k.src=a[m]}b()}var t=["ss_"],u=s||f;t[0]in u||"undefined"==typeof u.execScript||u.execScript("var "+t[0]); for(var v;t.length&&(v=t.shift());)t.length||void 0===r?u[v]&&u[v]!==Object.prototype[v]?u=u[v]:u=u[v]={}:u[v]=r;}).call(this);;s.ss_(window,'

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\f[3].txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	2723
Entropy (8bit):	5.777559640290872
Encrypted:	false
SSDEEP:	48:0VUUIqzPrqTnJcgVhkGh1egOlp7Fv7RZtqa5vL1bq1egOlp7Fv7RZtqa5vL106:+UURWTCgVhkI1Ll0eBe1Ll0eBN
MD5:	3D0EDCF134C7FEE86A7B7593F4A75E04
SHA1:	731366D908C8EA6C4C006BBBE0B4506B6CE828E8
SHA-256:	BFC4B126719AA370F0EB5515D2797EEA62979FB2CB2445E8C5D42D781AC4F56F
SHA-512:	29E0B8E6346EE479101FFEF4638ED88FFE66CD45EE66204D6CCA8B8DBC765A977AE4F6E86AF61602A786F717CC5EF8027CDB991EF4DAB81E60D7B3EAE691570B
Malicious:	false
Preview:	(function(){var s = {};(function(){/* Copyright The Closure Library Authors. SPDX-License-Identifier: Apache-2.0 */ var c={},f=this||self;var l=/#|$/;function n(d){var g =d.search(l),a;a:{for(a=0;0<=(a=d.indexOf("fmt",a))&&a<g;){var b=d.charCodeAt(a-1);if(38==b||63==b)if(b=d.charCodeAt(a+3),!b||61==b||38==b||35==b)break a;a+=4}a=-1}if(0>a)return null;b=d.indexOf("&",a);if(0>b||b>g)b=g;a+=4;return decodeURIComponent(d.substr(a,b-a).replace(/\+/g," "))};function r(d,g,a){function b(){--p;if(0>=p){var e;(e=d.GooglebQhCsO)||(e={});var q=e[g];q&&(delete e[g],(e=q[0])&&e.call&&e())}}for(var p=a.length+1,m=0;m<a.length;m++){var h=n(a[m]),k=null;1!=h&&2!=h||!(h=d.document.getElementById("goog_conv_iframe"))||h.src||(k=h);k||(k=new Image);k.onload=b;k.src=a[m]}b()}var t=["ss_"],u=s||f;t[0]in u||"undefined"==typeof u.execScript||u.execScript("var "+t[0]); for(var v;t.length&&(v=t.shift());)t.length||void 0===r?u[v]&&u[v]!==Object.prototype[v]?u=u[v]:u=u[v]={}:u[v]=r;}).call(this);;s.ss_(window,'

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\focus-within-polyfill[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	1171
Entropy (8bit):	5.1458024367829545
Encrypted:	false
SSDEEP:	24:YXw4ZXLL8jdOAT3r8j/uZp93ceY90l78BQLoOiQL4mT6xQMnmb3q/FcEmzNchNhx:6IMI38/8Xr+0l78B2vN4W6CRb31XzNcv
MD5:	C187011C9A45C15A6FCBF5D62A5D755F
SHA1:	E3FD6FAED2154EE94559F362EA0390B46ABF75BB
SHA-256:	452A163BE231D77006015E7D6F2A5B8AB5987D915C1F1E6907DDFBBA3AEC6EEC
SHA-512:	E5025DB65F3A66552C838B24374071130040D2E0CF13A4E4F75DA3A8C8DB00228EEAB8F45695F709CB834FF43D4B2DB757D8AA9046AB6A8E1990A4227AC0B4A
Malicious:	false
IE Cache URL:	http://https://static.parastorage.com/unpkg/focus-within-polyfill@5.0.9/dist/focus-within-polyfill.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\focus-within-polyfill[1].js	
Preview:	'use strict';(function(){(function(){function e(a){for(var b=[];a=a.parentNode||a.host||a.defaultView;)b.push(a);return b}function f(a){return function(b){var c="undefine d"!==typeof b.getAttribute?b.getAttribute("class")||"":void 0;"undefined"!==typeof c&&-1===c.indexOf(a)&&b.setAttribute("class",c.concat(" ",a).trim())}}function g(a){return function(b){var c="undefined"!==typeof b.getAttribute?b.getAttribute("class")||"":void 0;if(c){var d=c.indexOf(a);0<=d&&(0===d||0<=h.indexOf(c.charAt(d-1)))&&(c=c.re place(a,"").trim(),""===c?b.removeAttribute("class"):b.setAttribute("class",c))}}}function k(){var a=function(b){function a(){d=!1;"blur"===b.type&&Array.prototype.slice. call(e(b.target)).forEach(g("focus-within"));"focus"===b.type&&Array.prototype.slice.call(e(b.target)).forEach(f("focus-within"))}if(!d){window.requestAnimationFrame(a);var d=!0}};document.addEventListener("focus",a,!0);document.addEventListener("blur",a,!0);f("js-focus-within")(document.body);return!0}var h=["\n","\t"

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\ga-audiences[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped
Size (bytes):	84
Entropy (8bit):	2.9881439641616536
Encrypted:	false
SSDEEP:	3:CUXPQE/xlEqjdfXPQE/xlEy:1QEoqh3QEoy
MD5:	6A3F2D147842187CD48B1546EDDD5BA0
SHA1:	AB278C31189DF2939428CF81A3850A2C6DBF5E2E
SHA-256:	D4990F907BCA02F02B3D41216EEA5461609D4BCBA07A3CBEE0D7CF28A6D0D864
SHA-512:	998F55BF5C3D4A71CB3C23782B788F71E7625DF83A37FE8A18F915AAA3BDE5420183A3C709816664E262069EE2FE245CA44799E3476B6DE507B5D68FC86F8960
Malicious:	false
Preview:	GIF89a.....!.....,.....D.;GIF89a.....!.....,.....D.;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\helvetica[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	29917
Entropy (8bit):	5.035402319919693
Encrypted:	false
SSDEEP:	192:ZVlDpZKJ56E/Zn5v5D2Z9Ye+RUVMn0DpUZM9MBkzmNNfNefNtL/+8/U7748NWDYD:i1diD8FGS/PaL5ENOOz9oy
MD5:	39099ECA9738473EAA97CA6D87F4A5BF
SHA1:	6BA90D5D62954E52271BB44A2F5EE008CA576FAE
SHA-256:	2A238BAB6155365B6F5257D64D17277B0E70E5A217B90D53F2A3FC96F6707A9E
SHA-512:	641C0EACB9829FC34D4CC678E33BA96B156E54EE67F5D90C0238B9B241E8AFC24F7C1A0817CFFB27F8E805F33BBD9BD15E2B5243925A6B803B2612840D22E63F
Malicious:	false
IE Cache URL:	http://https://static.parastorage.com/services/santa-resources/resources/viewer/user-site-fonts/v7/helvetica.css
Preview:	/* fonts helvetica */../*@import url("//fast.fonts.com/t/1.css?apiType=css&projectid=33bd0973-5b82-45be-bb77-837225874dfe");*/..html{. background-image:url("//fast.fonts.com/t/1.css?apiType=css&projectid=33bd0973-5b82-45be-bb77-837225874dfe");.}.../* Original old fonts */..@font-face {. font-family: "Helvetica Neue";. src: url("//static.parastorage.com/services/third-party/fonts/Helvetica/Fonts/b7693a83-b861-4aa6-85e0-9ecf676bc4d6.eot?#iefix") format("embedded-opentype"),. url("//static.parastorage.com/services/third-party/fonts/Helvetica/Fonts/bcf54343-d033-41ee-bbd7-2b77df3fe7ba.woff") format("woff"),. url("//static.parastorage.com/services/third-party/fonts/Helvetica/Fonts/b0ffdcf0-26da-47fd-8485-20e4a40d4b7d.ttf") format("truetype"),. url("//static.parastorage.com/services/third-party/fonts/Helvetica/Fonts/da09f1f1-062a-45af-86e1-2bbdb3dd94f9.svg#da09f1f1-062a-45af-86e1-2bbdb3dd94f9") format("svg");.}..@font-face {. font-family: "Helvetica Neue Thin";. font-

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\lodash.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	73261
Entropy (8bit):	5.36112989542208
Encrypted:	false
SSDEEP:	1536:qaNdvaGKU+//A2kPJ3upjp5P/JpW3A3UNp:qauRP/SY+
MD5:	BC0594C54450E8AC689739B6B198067A
SHA1:	32F09EC3EC0950F47A35FC0D656559D5B164DACD
SHA-256:	55E35A1415438685F71FE809DFB0E94FF9D3B994DD8D8AE8F7206BB878D59A84
SHA-512:	DE86A9A5731555A73719EDCE9DD5B45AAA464D6C7D8E344903C4978A7F11C663DF73CAE0F3B6F7D451B2D785871BF64C4484A8F690637B35BDCB4D1160010E3
Malicious:	false
IE Cache URL:	http://https://static.parastorage.com/unpkg/lodash@4.17.15/lodash.min.js
Preview:	/**. * @license. * Lodash lodash.com/license | Underscore.js 1.8.3 underscorejs.org/LICENSE. */.;(function(){function n(n,t,r){switch(r.length){case 0:return n.call(t);case 1:return n.call(t,r[0]);case 2:return n.call(t,r[0],r[1]);case 3:return n.call(t,r[0],r[1],r[2])}return n.apply(t,r)}function t(n,t,r,e){for(var u=-1,i=null==n?0:n.length;++u<i;){var o=n[u];t(e,o,r(o),n)}return e}function r(n,t){for(var r=-1,e=null==n?0:n.length;++r<e&&!1==t(n[r],r,n););return n}function e(n,t){for(var r=null==n?0:n.length;r--&&!1==t(n[r],r,n););return n}function u(n,t){for(var r=-1,e=null==n?0:n.length;++r<e;)if(!t(n[r],r,n))return!1;return!0}function i(n,t){for(var r=-1,e=null==n?0:n.length,u=0,i=[];++r<e;){var o=n[r];t(o,r,n)&&(i[u++]=o)}return i}function o(n,t){return!(null==n||!n.length)&&-1<v(n,t,0)}function f(n,t,r){for(var e=-1,u=null==n?0:n.length;++e<u;)if(r(t,n[e]))return!0;return!1}function c(n,t){for(var r=-1,e=null==n?0:n.length,u=Array(e);++r<e;)u[r]=t(n[r],r,n)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\pfavico[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):	1.2100731437092027
Encrypted:	false
SSDEEP:	3:3NhDllvlNl/khXhCC1111111111111111111111111111111111111111111111111H:7Jq55555555555555R
MD5:	B53CE85A6CCE2AE00037A6CA13C90866
SHA1:	292D9AEB457AB7FEDBAD452854332AEFF267A78E
SHA-256:	33C1436F8C40CA2582D091C449FCCC34ED9BF73F02526C5FDEF44F4F06C6321B
SHA-512:	9271B4BD6B07C15662E9265359AD80CBEDF971C127F8C17EF289AE7A552C3BDA93A8416881493196E956FDC5B2A4DF03CBDA838F4203C7F7B12DCDBFE27B31B
Malicious:	false
IE Cache URL:	http://https://static.parastorage.com/client/pfavico.ico
Preview:	..... .h.....(..... ....@..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\pm-rpc.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	40801
Entropy (8bit):	5.179635720204025
Encrypted:	false
SSDEEP:	768:hivwQ+FtDocLb6VnWq8FSuzNBD8Ck6ZEn:hivwQ+PocX6OlRJ8Ck6Za
MD5:	6D2CE335B730660879C0B6949489201C
SHA1:	04207F9F622E642A257E7C60EB95368F8C77D49E
SHA-256:	F6F745CF79C117E16618576087B958DF0B47361BB672BD270F37CC7246C85FA7
SHA-512:	4C80DFB6B36D7A7E2D71594BC7AD39B252D8319E4993CC008C0985ED77521FCB32CE9FAE9E1BA4582B5EF5112224783EB787A757583C5EBEDCFFF97A0C33693
Malicious:	false
IE Cache URL:	http://https://static.parastorage.com/unpkg/pm-rpc@1.0.14/build/pm-rpc.min.js
Preview:	!function(t,r){"object"==typeof exports&&"object"==typeof module?module.exports=r():"function"==typeof define&&define.amd?define("pmrpc",[],r):"object"==typeof exports?exports.pmrpc=r():t.pmrpc=r()}(this,function(){return function(t){function r(n){if(e[n])return e[n].exports;var o=e[n]={i:n,l:!1,exports:{}};return t[n].call(o.exports,o,o.exports,r),o.l=!0,o.exports}var e={};return r.m=t,r.c=e,r.i=function(t){return t},r.d=function(t,e,n){r.o(t,e)||Object.defineProperty(t,e,{configurable:!1,enumerable:!0,get:n})},r.n=function(t){var e=t&&t.__esModule?function(){return t.default}:function(){return t};return r.d(e,"a",e),e},r.o=function(t,r){return Object.prototype.hasOwnProperty.call(t,r)},r.p="",r(r.s=150)}([function(t,r){var e=Array.isArray;t.exports=e},function(t,r,e){var n=e(40),o="object"==typeof self&&self&&self.Object===Object&&self,i=n||o||Function("return this")();t.exports=i},function(t,r,e){function n(t){return null==t?void 0===t?"[object Undefined]":"[object Null]":u&&u in Object(t)?i(t):u(t)}var o=e(8),i=e(

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\santa-components.prod[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	455527
Entropy (8bit):	5.47516385557914
Encrypted:	false
SSDEEP:	3072:3jVRgdJk6cO6sQin46M9R6fLRWm5/FkAX144ssjT9lOYWecZlbq310n6t8+qbRzw:3gd1xsgT9lOXeGlm3a+Cvy
MD5:	FCA502DA484645AC792BAEA4F24A48EB
SHA1:	CBCBB91C2B5C7DD2483CE65D10FB5EF7E8757D70
SHA-256:	F00D4C9E8A993C8799CE055C21F8BF9EE8475C20B3B1A04708568BB7CC028BC4
SHA-512:	CF2473055C2646159E914C1338752DA3E5488B274F6ABA5CBD7E156EC02604F9F3BEA18EA929796DB5E37FE8ED53B1D99763072E7C238D61194D94ADC2DD688
Malicious:	false
IE Cache URL:	http://https://static.parastorage.com/unpkg/@wix/santa-components@1.1977.0/dist/santa-components.prod.js
Preview:	!function(t,e){if("object"==typeof exports&&"object"==typeof module)module.exports=e(require("lodash"),require("coreUtilsLib"),require("prop-types"),require("react"),require("create-react-class"),require("reactDOM"),require("skinUtils"),require("image-client-api"));else if("function"==typeof define&&define.amd)define(["lodash","coreUtilsLib","prop-types","react","create-react-class","reactDOM","skinUtils","image-client-api"],e);else{var o="object"==typeof exports?e(require("lodash"),require("coreUtilsLib"),require("prop-types"),require("react"),require("create-react-class"),require("reactDOM"),require("skinUtils"),require("image-client-api")):e(t.lodash,t.coreUtilsLib,t["prop-types"],t.react,t["create-react-class"],t.reactDOM,t.skinUtils,t["image-client-api"]);for(var r in o)("object"==typeof exports?exports:t)[r]=o[r]}}(this,(function(t,e,o,r,i,n,a,s){return function(t){var e={};function o(r){if(e[r])return e[r].exports;var i=e[r]={i:r,l:!1,exports:{}};return t[r].call(i.exports,i,i.e

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\skinExports.min[1].js	
Size (bytes):	45545
Entropy (8bit):	4.985248326211914
Encrypted:	false
SSDEEP:	384:V8G3f6/N/U/w/h/EB/1/z/p/X/3/lsKbWcVnnx2eSPI1Z8MgzM5:V8Gj35V4BM5
MD5:	E3B310E8689B6965D19169917C521FB4
SHA1:	198FFCD1FCA30A54E77AAEC71CE000772FDB1C30
SHA-256:	33B44DD1DD54694D140CAFA355D6F929354909A8DF68CF24E739B0ED3FB13FB3
SHA-512:	7A1A3DF38CA2F7269CC67E67CAA868ACDB29579C7975330553B9E8CF8E2BD0D4D7A4A2569D19E6F0D9612DA61D2AA88DD02ACB8D8786F7ADDDF1659CF6E1E34
Malicious:	false
IE Cache URL:	http://https://static.parastorage.com/services/wix-bolt/1.7264.0/node_modules/wix-santa/dist/packages-bin/skinExports/skinExports.min.js
Preview:	define("skinExports",[],(function(){return function(i){var e={};function n(s){if(e[s])return e[s].exports;var r=e[s]={i:s,l:!1,exports:{}};return i[s].call(r.exports,r,r.exports,n),r.l=!0,r.exports}return n.m=i,n.c=e,n.d=function(i,e,s){n.o(i,e)||Object.defineProperty(i,e,{enumerable:!0,get:s})},n.r=function(i){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(i,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(i,"__esModule",{value:!0})},n.t=function(i,e){if(1&e&&(i=n(i)),8&e)return i;if(4&e&&"object"==typeof i&&i&&i.__esModule)return i;var s=Object.create(null);if(n.r(s),Object.defineProperty(s,"default",{enumerable:!0,value:i}),2&e&&"string"!=typeof i)for(var r in i)n.d(s,r,function(e){return i[e]}.bind(null,r));return s},n.n=function(i){var e=i&&i.__esModule?function(){return i.default}:function(){return i};return n.d(e,"a",e),e},n.o=function(i,e){return Object.prototype.hasOwnProperty.call(i,e)},n.p="",n(n.s=1073)}({1073:function(i,e,n){var s,r;s=[n(10

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\src=4382365;type=count;cat=websi0;ord=1;num=6375209772439;gtm=2wg6n0;auiddc=_;u1=0014774d-e86e-4006-895c-197a7e3747e8;~oref=https___www.wix[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped
Size (bytes):	42
Entropy (8bit):	2.9881439641616536
Encrypted:	false
SSDEEP:	3:CUXPQE/xlEy:1QEoy
MD5:	D89746888DA2D9510B64A9F031EAECD5
SHA1:	D5FCEB6532643D0D84FFE09C40C481ECDF59E15A
SHA-256:	EF1955AE757C8B966C83248350331BD3A30F658CED11F387F8EBF05AB3368629
SHA-512:	D5DA26B5D496EDB0221DF1A4057A8B0285D15592A8F8DC7016A294DF37ED335F3FDE6A2252962E0DF38B62847F8B771463A0124EF3F84299F262ED9D9D3CEE4
Malicious:	false
Preview:	GIF89a.....!.....,.....D.;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\textCommon.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	7855
Entropy (8bit):	5.181882266727943
Encrypted:	false
SSDEEP:	96:x69y6lhK+DBhilnuTi1z2x7qvMHSS5UeFaXj4yzmj90DCpUyoR4lJn8RcLQj7eiQ:x6Fs1Kx7qAV4Xjja5wCpI18CLQOiQ
MD5:	56CE57CA0F78C1AB251596C253AC711B
SHA1:	D407A6A577BC5AB9923144E6F2FD533AFC854489
SHA-256:	FBF6CBE620C3A67FBE96FB584E322C290C007E8FCB9666BE52AAB0586679FD65
SHA-512:	1DC43ABF2CCA0546F63B693C1C1F33F1ABC85EFA1B5566426C863E3ED829676D3271867AF2435B5645EEDA7B37790D9082A5F1121634AD54C60DBEF5E27D168
Malicious:	false
IE Cache URL:	http://https://static.parastorage.com/services/wix-bolt/1.7264.0/node_modules/wix-santa/dist/packages-bin/textCommon/textCommon.min.js
Preview:	define("textCommon",["lodash","santa-components","componentsCore","prop-types","skins"],(function(t,e,n,i,r){return function(t){var e={};function n(i){if(e[i])return e[i].exports;var r=e[i]={i:i,l:!1,exports:{}};return t[i].call(r.exports,r,r.exports,n),r.l=!0,r.exports}return n.m=t,n.c=e,n.d=function(t,e,i){n.o(t,e)||Object.defineProperty(t,e,{enumerable:!0,get:i})},n.r=function(t){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(t,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(t,"__esModule",{value:!0})},n.t=function(t,e){if(1&e&&(t=n(t)),8&e)return t;if(4&e&&"object"==typeof t&&t&&t.__esModule)return t;var i=Object.create(null);if(n.r(i),Object.defineProperty(i,"default",{enumerable:!0,value:t}),2&e&&"string"!=typeof t)for(var r in t)n.d(i,r,function(e){return t[e]}.bind(null,r));return i},n.n=function(t){var e=t&&t.__esModule?function(){return t.default}:function(){return t};return n.d(e,"a",e),e},n.o=function(t,e){return Object.prototype.hasOwnProp

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\tpaComponents.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	91651
Entropy (8bit):	5.348229763483598
Encrypted:	false
SSDEEP:	1536:FM1ivJrgqvjTzPlJ2FipSA2F6si81BEMzIJU:NrgqvjTzNJ2Fip3qi81BEMzIJU
MD5:	8498201A1530B7390D646F3ED7FA5D42
SHA1:	30907233847D6EB2F3723E64B2CC7FEC9566F90D

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\tpaComponents.min[1].js	
SHA-256:	3A676AC279CCE9BA7F68A291589783F0E322FEA414C7551848F78449ACB3698B
SHA-512:	D3A103B1392AC5D72B074EDE3320E1D1643C45DAF2B98003200670718B05E03AC4C3B6DFE6DF702940C5997AE6C51934D761108E7E3ECC179A4E0A6FD4F37BE D
Malicious:	false
IE Cache URL:	http://https://static.parastorage.com/services/wix-bolt/1.7264.0/node_modules/wix-santa/dist/packages-bin/tpaComponents/tpaComponents.min.js
Preview:	define("tpaComponents",["lodash","coreUtils","santa-components","componentsCore","prop-types","skins","reactDOM","zepto","experiment","warmupUtils","santa-core-utils","create-react-class","react","layout"],(function(e,t,i,n,s,r,o,a,p,c,d,l,u,h){return function(e){var t={};function i(n){if(t[n])return t[n].exports;var s=t[n]={i:n,l:!1,exports:{}};return e[n].call(s.exports,s,s.exports,i),s.l=!0,s.exports}return i.m=e,i.c=t,i.d=function(e,t,n){i.o(e,t)||Object.defineProperty(e,t,{enumerable:!0,get:n})},i.r=function(e){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(e,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(e,"__esModule",{value:!0})},i.t=function(e,t){if(1&t&&(e=i(e)),8&t)return e;if(4&t&&"object"==typeof e&&e&&e.__esModule)return e;var n=Object.create(null);if(i.r(n),Object.defineProperty(n,"default",{enumerable:!0,value:e}),2&t&&"string"!=typeof e)for(var s in e)i.d(n,s,function(t){return e[t]}.bind(null,s));return n},i.n=function(e){var t=e&&e.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\tr[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	downloaded
Size (bytes):	44
Entropy (8bit):	2.8317663774021287
Encrypted:	false
SSDEEP:	3:CU9yltxlHhn:mn
MD5:	B798F4CE7359FD815DF4BDF76503B295
SHA1:	F8CC6ADDF1707AD236AD9970B0A48F9733D07DA5
SHA-256:	10D8D42D73A02DDB877101E72FBFA15A0EC820224D97CEDEE4CF92D571BE5CAA
SHA-512:	921944DC10FBFB6224D69F0B3AC050F4790310FD1BCAC3B87C96512AD5ED9A268824F3F5180563D372642071B4704C979D209BAF40BC0B1C9A714769ABA7DFC
Malicious:	false
IE Cache URL:	http://https://www.facebook.com/tr/?id=704136006388169&ev=PageView&dl=https%3A%2F%2Fwww.wix.com%2Foutdated-browser%2Finternet-explorer%3FforceBolt%3D%26ssrIndicator%3Dfalse%26suppressbi%3Dtrue&rl=https%3A%2F%2Fwww.artsenvoorwaarheid.nl%2F&if=true&ts=1624884983650&sw=1280&sh=1024&v=2.9.42&r=stable&ec=0&o=14&fbp=fb.1.1624884983650.482060496&it=1624884983493&coo=false&rqm=GET
Preview:	GIF89a.....!.....,.....D..;.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\v3[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped
Size (bytes):	70
Entropy (8bit):	2.97020783365077
Encrypted:	false
SSDEEP:	3:CUU0/rllHhqwU0/rllHh/:S0TJqT0TJ/
MD5:	82C4A4D6A36BF8ED456A3FA11045F4C4
SHA1:	06AFF26185861A92EFB217B5B0D852B4FDBFB574
SHA-256:	2B141AE8655D23D9F74EA4BF2F01648B74288CEC38CB857AB8E7EE688DED2628
SHA-512:	FA00F2DF8899CB83BD3F7EBA43F3C0B0D7866FF1B4F5174302D4DEDEE5F178F718FA9DC88636D919B8736E2C5DC3244FD5F53D3841FFD9097009DD56F27352F
Malicious:	false
Preview:	GIF89a.....,.....D..;GIF89a.....,.....D..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\wix-perf-measure.bundle.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	33384
Entropy (8bit):	5.154989977522001
Encrypted:	false
SSDEEP:	384:3+46X/yV16sGkpDgUP+xWPxUXvaYqsZ5oy85QMCGtdeLnVmklBCLnVZ0XN:4XIkkpDDWXrT5o7CGtg9zC8
MD5:	0E37060EF731C573612C3D7024490E64
SHA1:	26463B9C00B3EF3BEB89340399D5FEA74986FAF1
SHA-256:	85A0E12E2B9DA4C18F8C348295244537AA93518D6151CEF0BF94E15358D4D32D
SHA-512:	54D124C4B101F52D50EBCB52574F9B6E6D05B30869A967AC41324EB39C12730328D07E113808B1A4989222E0560F04F05D7B03D05E7CC5DF087F024CB8047325
Malicious:	false
IE Cache URL:	http://https://static.parastorage.com/services/wix-perf-measure/1.501.0/wix-perf-measure.bundle.min.js
Preview:	!function(e,t){"object"==typeof exports&&"object"==typeof module?module.exports=t():"function"==typeof define&&define.amd?define("wix-perf-measure",[],t):"objec t"==typeof exports?exports["wix-perf-measure"]=t():e["wix-perf-measure"]=t()}("undefined"!=typeof self?self:this,(function(){return function(e){var t={};function n(r){if(t[r])retur n t[r].exports;var i=t[r]={i:r,l:!1,exports:{}};return e[r].call(i.exports,i,i.exports,n),i.l=!0,i.exports}return n.m=e,n.c=t,n.d=function(e,t,r){n.o(e,t)||Object.defineProperty(e,t, {enumerable:!0,get:r})},n.r=function(e){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(e,Symbol.toStringTag,{value:"Module"}),Object.de fineProperty(e,"__esModule",{value:!0})},n.t=function(e,t){if(1&t&&(e=n(e)),8&t)return e;if(4&t&&"object"==typeof e&&e&&e.__esModule)return e;var r=Object.create(null);if (n.r(r),Object.defineProperty(r,"default",{enumerable:!0,value:e}),2&t&&"string"!=typeof e)for(var i in e)n.d(r,i,function(t){return e[t]}.bind(null,i

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\wixFreemiumBanner.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	91611
Entropy (8bit):	5.445501839664493
Encrypted:	false
SSDEEP:	768:l8vtZ/lLqh9E3Q9jf4Qs9h0QF8VX1+998wJX1k4X17Tq/X1C6:l8vtZ/lLq/E3gjf4Q8hTF8e9nYA+F
MD5:	141A4EB927C4D7FD81F6344DF8B1DE6E
SHA1:	0112AE5D15519E993A41771FB3009A08BFD07912
SHA-256:	AF7E09C58D9C820B8EE69C03F93DC6739DD8B9C5E945B07C91EA4D1138528E4C
SHA-512:	6289F9359B174CBCA2F32146A372B9EEF2C457EA269AF648F3B34159521F68DA383D691AB437455F2E7FC19695299089F7E1D74DFA51B77CFA13B94CEA29392C
Malicious:	false
IE Cache URL:	http://https://static.parastorage.com/services/wix-bolt/1.7264.0/node_modules/wix-santa/dist/packages-bin/wixFreemiumBanner/wixFreemiumBanner.min.js
Preview:	define("wixFreemiumBanner",["lodash","coreUtils","santa-components","componentsCore","prop-types","experiment","react"],(function(e,t,o,r,a,n,i){return function(e){var t={};function o(r){if(t[r])return t[r].exports;var a=t[r]={i:r,l:!1,exports:{}};return e[r].call(a.exports,a,a.exports,o),a.l=!0,a.exports}return o.m=e,o.c=t,o.d=function(e,t,r){o.o(e,t)||Object.defineProperty(e,t,{enumerable:!0,get:r})},o.r=function(e){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(e,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(e,"__esModule",{value:!0})},o.t=function(e,t){if(1&t&&(e=o(e)),8&t)return e;if(4&t&&"object"==typeof e&&e&&e.__esModule)return e;var r=Object.create(null);if(o.r(r),Object.defineProperty(r,"default",{enumerable:!0,value:e}),2&t&&"string"!=typeof e)for(var a in e)o.d(r,a,function(t){return e[t]}.bind(null,a));return r},o.n=function(e){var t=e&&e.__esModule?function(){return e.default}:function(){return e};return o.d(t,"a",t),t},o.o=function(e,t

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\wixMadefor[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	4339
Entropy (8bit):	4.828748558866936
Encrypted:	false
SSDEEP:	96:/QPOPLLQPbPU9QPfPgdQH4rDWQ1SpQZ+ADWQ4xlQKvjDWQTcTQoh/DWQpOO:/D7DQDADZ
MD5:	D76884A66F7EE1E86BE1841EE2B954F4
SHA1:	7BA60D9EAECD1E5CC809368B5912BBA8F370D3E2
SHA-256:	DB704B465A4ED21E3950FE3FFD95DBAA22F130D73AE7064D7E1EB643BF68A4C1
SHA-512:	89221219FA4868B78DB5480587FFA7C5065E179AD2D143F68F36EA08024B9638BBB86397D3F8E4AE0F5634684E423AEA516A41CE474FD30B770D7E5D71CC94E8
Malicious:	false
IE Cache URL:	http://https://static.parastorage.com/services/santa-resources/resources/viewer/user-site-fonts/v11/wixMadefor.css
Preview:	/* new wixMadefor font*/.../* Madefor Display */.@font-face{. font-family:"Madefor-Display";. src: url("//static.parastorage.com/services/santa-resources/resources/viewer/user-site-fonts/fonts/WixMadefor/v2/WixMadeforDisplay_W_Rg.woff2") format("woff2"),. url("//static.parastorage.com/services/santa-resources/resources/viewer/user-site-fonts/fonts/WixMadefor/v2/WixMadeforDisplay_W_Rg.woff") format("woff");.}..@font-face{. font-family:"Madefor-Display-Bold";. src: url("//static.parastorage.com/services/santa-resources/resources/viewer/user-site-fonts/fonts/WixMadefor/v2/WixMadeforDisplay_W_Bd.woff2") format("woff2"),. url("//static.parastorage.com/services/santa-resources/resources/viewer/user-site-fonts/fonts/WixMadefor/v2/WixMadeforDisplay_W_Bd.woff") format("woff");.}..@font-face{. font-family:"Madefor-Display-ExtraBold";. src: url("//static.parastorage.com/services/santa-resources/resources/viewer/user-site-fonts/fonts/WixMadefor/v2/WixMadeforDisplay_W_XBd.wo

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\wixui.Captcha.chunk[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF, LF line terminators
Category:	downloaded
Size (bytes):	89804
Entropy (8bit):	5.1837141612828725
Encrypted:	false
SSDEEP:	1536:+U6UnSMRIDYFzqtcWW3P9WcAJ2jVRrzh3L:+Ujzq23PdAJUVBhb
MD5:	6B17728A7AF8BBB32B5C1D8B8D219BA8
SHA1:	72E31504D27646632B85508B89B61D74889D5DD4
SHA-256:	E5ABAD50092D7EE0D9C75945152BCB383F43BD78D6502B0B670EF096A616F3A6
SHA-512:	3157F0AC1562FE175232938FEC918DE99269E575234509A4ABC442F4406F2D7035D4DCE7C2D0864F20B0494CBF70EA4B8660BA6C5E4206D5C5953E93B22E3096
Malicious:	false
IE Cache URL:	http://https://static.parastorage.com/unpkg/@wix/wix-ui-santa@2.0.294/dist/statics/wixui.Captcha.chunk.js
Preview:	((typeof self !== 'undefined' ? self : this)["webpackJsonp__wix_wix_ui_santa_dev"] = (typeof self !== 'undefined' ? self : this)["webpackJsonp__wix_wix_ui_santa_dev"] || []).push([[50],{../***/ 10:./*!**!*\. !*** ../node_modules/tslib/tslib.es6.js ***!. **/./*! exports provided: __extends, __assign, __rest, __decorate, __param, __metadata, __awaiter, __generator, __createBinding, __exportStar, __values, __read, __spread, __spreadArrays, __await, __asyncGenerator, __asyncDelegator, __asyncValues, __makeTemplateObject, __importStar, __importDefault, __classPrivateFieldGet, __classPrivateFieldSet */./*! all exports used */./***/ (function(module, __webpack_exports__, __webpack_require__) {.."use strict";.__webpack_require__.r(__webpack_exports__);./* harmony export (binding) */ __webpack_require__.d(__webpack_exports__, "__extends", function() { return __extends; });./* harmony export (binding) */ __webpack

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\wixui.StylableButton.chunk[1].js	
Size (bytes):	28050
Entropy (8bit):	5.324952278071198
Encrypted:	false
SSDEEP:	768:JEz4Z70W20J/0vDGH3eZL6b5EzKd7/Tmyp75EzK3IWx78resld3m:UWuG2WZ
MD5:	F75363F15AEB3199495C50D3FB3167E1
SHA1:	35B6F65FDA472D5105D72AC3E71AB585D9EFCB09
SHA-256:	D0C8E3EC83BD76EC5724A8DD62EAFA0709B74A5BB6DEA6D3CF1B5FE53C882EF5
SHA-512:	CB4367751374A35C011E823C57C4751E1A0924B4984EC2315EEFC7571B5005AFAB46DC48EBAED736C3BA3220B3C9B438117AA66967EE20BB584D09FF8245D42
Malicious:	false
IE Cache URL:	http://https://static.parastorage.com/unpkg/@wix/wix-ui-santa@2.0.294/dist/statics/wixui.StylableButton.chunk.js
Preview:	((typeof self !== 'undefined' ? self : this)["webpackJsonp__wix_wix_ui_santa_dev"] = (typeof self !== 'undefined' ? self : this)["webpackJsonp__wix_wix_ui_santa_dev"] || []).push([[67],{../***/ 16:./*!**********!*\. !*** ./components/StylableButton/StylableButton.js ***!. ********** **********/./*! exports provided: StylableButton */./*! exports used: StylableButton */./***/ (function(module, __webpack_exports__, __webpack_require__) {.."use strict";./* harmony export (binding) */ __webpack_require__.d(__webpack_exports__, "a", function() { return StylableButton; });./* harmony import */ var react__WEBPAC K_IMPORTED_MODULE_0__ = __webpack_require__(/*! react */ 0);./* harmony import */ var react__WEBPACK_IMPORTED_MODULE_0___default = /*#__PURE __*/__webpack_require__.n(react__WEBPACK_IMPORTED_MODULE_0__);./* harmony import */ var prop_types__WEBPACK_IMPORTED_MODULE_1__ = __webpack_require__(/*! prop-types */ 1)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\xss.min[1].js	
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):	27954
Entropy (8bit):	5.2180021601732784
Encrypted:	false
SSDEEP:	384:DDJ6NokIwHWvsSHzxc5R61A0+3PJ8K73imq2fw/94HFzKvkGuIcDYP8ALJiy+03V:DEflwZ9ztyyw/etKvvqI7lmpo
MD5:	03A1F336E798CB76FD006A89BB5C86CD
SHA1:	22DD332C6E792D26784CA427F4E95BB45AB5EDA1
SHA-256:	7021FC60565C79ECBE0D8113A83DBF68E9E719EFEAC07B360D9CDA18863E5A55
SHA-512:	9CC7CDB71F2426EA9878703AD9D1FD992C4605B0F96D7360575965995A73C09875FC755220DEA60C74B6FB61B55666B7D90A0DFD861F0A9DA4849C1F53893475
Malicious:	false
IE Cache URL:	http://https://static.parastorage.com/unpkg/xss@0.2.18/dist/xss.min.js
Preview:	(function e(t,n,r){function s(o,u){if(!n[o]){if(!t[o]){var a=typeof require=="function"&&require;if(!u&&a)return a(o,!0);if(i)return i(o,!0);var f=new Error("Cannot find module '"+ o+"'");throw f.code="MODULE_NOT_FOUND",f}var l=n[o]={exports:{}};t[o][0].call(l.exports,function(e){var n=t[o][1][e];return s(n?n:e)},l,l.exports,e,t,n,r)}return n[o].exp orts}var i=typeof require=="function"&&require;for(var o=0;o<r.length;o++)s(r[o]);return s})({1:[function(require,module,exports){var FilterCSS=require("cssfilter").Filte rCSS;var getDefaultCSSWhiteList=require("cssfilter").getDefaultWhiteList;var _=require("./util");function getDefaultWhiteList(){return{a:["target","href","title"],abbr:["title"],ad dress:[],area:["shape","coords","href","alt"],article:[],aside:[],audio:["autoplay","controls","loop","preload","src"],b:[],bdi:["dir"],bdo:["dir"],big:[],blockquote:["cite"],br:[],caption:[ ],center:[],cite:[],code:[],col:["align","valign","span","width"],colgroup:["align","valign","span","width"],d

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\050b1948-f226-4d20-a65a-15d8ed031222[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 22912, version 1.0
Category:	downloaded
Size (bytes):	22912
Entropy (8bit):	7.981203288200719
Encrypted:	false
SSDEEP:	384:9llcXrCfMOBb/3v42KcHscKd5Hz5TUEbtYXQjVa7ZZx+YdkaUpSV/QRBsbQJ:9llc7AbfVHSFUXuyZZElaUpG/q
MD5:	6AA6E18FE4F8FCAF8147E6196A2ED4F2
SHA1:	94850CC02FDD10CE3626B4717A20BA2A84E36720
SHA-256:	4A636E6C5A476278C861C00829AFB12B122F074B1E34693C8C6788D857D66D2F
SHA-512:	BF9211CB4EB1D8EE2C5DA099044D2911A647958D5DC4215B651C84D721919B5B94277677046511453455F5231FE5D918F9FEA1DD955CBCE9F53024FCD3B9D535
Malicious:	false
IE Cache URL:	http://https://static.parastorage.com/services/santa-resources/resources/viewer/user-site-fonts/fonts/Helvetica/v2/050b1948-f226-4d20-a65a-15d8ed031222.woff
Preview:	wOFF.....Y.....S.....GPOS...l.....^.O..OS/2.....T...`e...VDMX...p...\....p.x|cmap.....g.....cvt ...4...X....:..fpgm.....,...gasp.....glyf... ..:C..]. .@head..Hd...6...6..}.hhea..H.... ...$...,hmtx..H.....mloca..J....\.....*.`maxp..M... ... ...Tname..M0.....post..S..... ...2prep..S.....x..S.k.A..f.d7?l..".. ".....6..%V[.bL. [D..*(9.GQP...{... .B..4....k....H...o.4I.*...f..{ow.o.....a....5.8.....J.....6_*.X.~...J..9@k..pV.IE...N4.H<Z{R...#b...]...r.:.....C(")>?.7...ot.U..>.....X...P..<D.~.....f..m4.../..0.*WU ...rzG..z....fu.....&.m..Z...o...i..r....k.....2q.v=F..d.Lf=H.(a.7Av...]....%..e..<.@..@.X$....[D....V...<..w...N=<| .>..#7..~.>.....|.....^.A...u....RS..Ym.v.vp.*.....X.k.....0.0..;I....*.s.. ...+..BF.W...n...5N.....IrhTH..2.5....:!.>.S...r.Me...'...O.O.&..*..D.r...*.B...}..S...}s.cnc.....#.}.-.6$/..p....~..]_?..{O.+}T'~rl..."...v+j....Ej.(.1./.4.D....3-...\"...t...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\26b8484e-52e3-44ac-b958-865809934ebb[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 48908, version 1.0
Category:	downloaded
Size (bytes):	48908
Entropy (8bit):	**7.9908769597228275**
Encrypted:	**true**

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\26b8484e-52e3-44ac-b958-865809934ebb[1].woff	
SSDEEP:	768:2noxWxiIDP1D007rQc2v/5eRPz2S76YGQ3AmzfwSqwSmBHPch7vsqazs6/B40fB8:2n5Q0CZe12S76YGQwmzIhmivsqaAcBF8
MD5:	B1C2C4A57ABC248FA5B015E5DD93000C
SHA1:	E287387E70687D521E839DF86F38CFF3F1D71301
SHA-256:	4D18B41D696C25E7E1A9372398C555C52162D9C995552E792ECDC054274CC8F2
SHA-512:	4769393B4D3A6DB167AC9FEAABFBA27D55056415D3F039A5F14FE3142B49B06A4636379D1E738D1B97C5072E095DE7955799136229D8D7FB273C58014957C0FC
Malicious:	false
IE Cache URL:	http://https://static.parastorage.com/services/santa-resources/resources/viewer/user-site-fonts/fonts/Helvetica/v2/26b8484e-52e3-44ac-b958-865809934ebb.woff
Preview:	wOFF.....Z.....L.....GPOS.....1,...;GSUB... .....N./.<OS/2...,...S...`h5|.VDMX.....|....o.w.cmap.....#.<.cvt .."....X.....:..fpgm.."".....6...gasp..'p.....'glyf..'...}.....*c.head.....6...6...hhea...<...!...$.M.6hmtx...`..._....Z.T.loca.....W.....4maxp..... ... .[.dname...8.....3.post..... ...2prep.....x....T...~w.f.....[D^."*"/.....]...p.5....&..L.Q.q$..:hX...+.....#C.....uP....[...8:.c.s.l.....W_}.....}.(...b9$...x.m.d.o....~...!^.1.Z..W.^\|W...O...~L...7fX...p..<.:q..3.:S{2.7S.2.?S.$x..;.Ho..`.C.v.....v..N'.7..o...X..Y.*D...5.x..L.L...y.S.y..g.g....m.m.....{.w..!...{7y...o.....o.o..!_.o.....f.,.|...../.?._.....?..@.@.....'.....`.`.....].....C.BcB.B.C....=.Z.....*.....*..B.P2..7.7....;.{.{.....G.....w.?...FZD.G.....e.HAdUdC.$.v.N..g.3.....Y...r.:_G..p.c.gt@thtdt\tbtZtVt~ta....-.].d.x...=.hm.W.}.%Y...Y=.FfM..=<.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\50ac1699-f3d2-47b6-878f-67a368a17c41[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 22537, version 1.0
Category:	downloaded
Size (bytes):	22537
Entropy (8bit):	7.980046807695369
Encrypted:	false
SSDEEP:	384:7jtnrP2HkbVPlywA397tSeRHNm/gWsatewLC6/q7LJxtL42eHa3NmQNxF:7jhrmUyj3rNlth1q7Nxt824dQ3F
MD5:	AFC80FD38B63916E55B3434D6DC50AA8
SHA1:	A93E6A628D615ECC4A03268D615B2C7339BB82CA
SHA-256:	8E1FB2C958070695B9633261993A47CDAC70A25EB9C321EA0DC7207036D5140D
SHA-512:	AC516CEB938F721E006D05A3E712E6142A0F086EA71A44CA00187A48C183DF7B4B3EEBF9811C8FE9840CB6D345E445DD9A5A3E892B3BBE9DDF7A670161A3B8A8
Malicious:	false
IE Cache URL:	http://https://static.parastorage.com/services/santa-resources/resources/viewer/user-site-fonts/fonts/Helvetica/v2/50ac1699-f3d2-47b6-878f-67a368a17c41.woff
Preview:	wOFF.....X.....Rt.....GPOS...l...^.....HOS/2.....T...`e...VDMX... ...V....r8y.cmap...x...m...../cvt .....K.....fpgm...4.....,...gasp.....glyf.....9;..\n W...head..G....6...6.z}whhea..G<... ...$.>..hmtx..G\.....loca..IX...b.....+~.maxp..K.... ... ...Mname..K.....!=..$post..Q..... ...2prep..Q.....y..x...OO.Q...Li.RhE...4..`HHJ..4FME..R..7F.....}....1..u#&.j.BM ...v...;t..x..uD.....w.....&....-}.s...E....&u8{..T.|..T:..\R'f.....W..]..|....B...,j...kS.....Y.,...cm...].T....^OU!.iD)..r..4.1MjZ+Z.=j...S...0k..v.z.+...u...1p7.]]J.....Xf....B.uPm..frK.d..1?.....h.}_6.u.e...h...-!..g].%....2(y.....7.L..k.".su.>l|.....d~...^...Y.^.b..-se..X....uu.x..~..N.M#.....y...&.2.`.N....m.kA....s...A..0.$k..5.....i..0.....q.>..g..}...7..*.....L...=.....j;V..jtY..V#.t.1..t...i.b.;.19j.....i.....t.Dt.t.*h.5.....u...;.....Jh..KT^.~..2*oAD.....+..G.....x.c`a.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\ScrollToPlugin.min[1].js	
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):	2852
Entropy (8bit):	5.217000388303245
Encrypted:	false
SSDEEP:	48:QXSHhNKsC6TmTAJpl5ZQ5wamo7VJm6fAjyud3qZtzqOyAFqVCG7EPEQEWs9XCYYQ:C8KsCEmTAJpl5ZQ5wamSRfAutWOfF0Tx
MD5:	D29232AA62F9740CB6F1A8CEDC26D8DC
SHA1:	E6742CEE6B36AE8EB1BF26D4529BC7BA2AEB8D3E
SHA-256:	7090E6A71A15E2D47E830528798A657BECC16D41B78EADE27EC8624EA6A38812
SHA-512:	917465EA8903E6700A0B4A50C3236AF1A3F327560A6C3FCC6D55A9A693CFAA3B093675936B8EDD2D8243439D2658CF737E9077DCDE9EE3366CAAE8AD4A65DDA
Malicious:	false
IE Cache URL:	http://https://static.parastorage.com/unpkg/@wix/santa-external-modules@1.644.0/tweenmax-plugins/3.1.1-transition-phase/ScrollToPlugin.min.js
Preview:	!function(t,e){"object"==typeof exports&&"undefined"!=typeof module?e(exports):"function"==typeof define&&define.amd?define(["exports"],e):e((t=t||self).window=t.window||{})}(this,function(t){"use strict";var e,i,o,s,n,r,l,u=function(){return"undefined"!=typeof window},f=function(){return e||u()&&(e=window.gsap)&&e.registerPlugin&&e},p=function(t){return"string"==typeof t},a=function(t,e){var i="x"===e?"Width":"Height",r="scroll"+i,l="client"+i;return t===o||t===s||t===n?Math.max(s[r],n[r])-(o["inner"+i]||s[l]||n[l]):t[r]-t["offset"+i]},c=function(t,e){var i="scroll"+("x"===e?"Left":"Top");return t===o&&(null!=t.pageXOffset?i="page"+e.toUpperCase()+"Offset":t=null!=s[i]?s:n),function(){return t[i]}},h=function(t,e){var i=r(t)[0].getBoundingClientRect(),l=!e||e===o||e===n,u=!?{top:s.clientTop-(o.pageYOffset||s.scrollTop||n.scrollTop||0),left:s.clientLeft-(o.pageXOffset||s.scrollLeft||n.scrollLeft||0)}:e.getBoundingClientRect(),f={x:i.left-u.left,y:i.top-u.top};return!l&&e&&(f.x+=c(e,"x"

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\analytics[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	49377
Entropy (8bit):	5.521008419138659
Encrypted:	false
SSDEEP:	768:/yR3fYFBCwsNDsP5XqY0TyPnHpl1TY3SoavyVv6PU+CgYUD0lgEw0stZK:/y9g1r5h0UHp/Y3SowCw0sy
MD5:	042B7183D8645F5CF9D0D6ACD5FF8358
SHA1:	447A98467EA31E253ECB63EE8564C8B5E1E77D58

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\analytics[1].js	
SHA-256:	73D6A5EA11FB7BF6E6A6CCD44B1635D52C79B0A00623D0387C9DDDD4B7C68E89
SHA-512:	72AA2F221BB5EFEC3A9C0CBC2D01DEBD827361369F7E84AA613D4CA70838FF68EA2C3300167FB263A4F416A857BABF0354A1FF8B3EC669BF88452633981CA18F
Malicious:	false
IE Cache URL:	http://https://www.google-analytics.com/analytics.js
Preview:	(function(){/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var n=this||self,p=function(a,b){a=a.split(".");var c=n;a[0]in c||"undefined"==typeof c.execScript||c.execScript("var "+a[0]);for(var d;a.length&&(d=a.shift());)a.length||void 0===b?c=c[d]&&c[d]!==Object.prototype[d]?c[d]:c[d]={}:c[d]=b};var q={},r=function(){q.TAGGING=q.TAGGING||[];q.TAGGING[1]=!0};var t=function(a,b){for(var c in b)b.hasOwnProperty(c)&&(a[c]=b[c])},v=function(a){for(var b in a)if(a.hasOwnProperty(b))return!0;return!1};var x=/^(?:(?:https?|mailto|ftp):|[^:/?#]*(?:[/?#]|$))/i;var y=window,z=document,A=function(a,b){z.addEventListener?z.addEventListener(a,b,!1):z.attachEvent&&z.attachEvent("on"+a,b)};var B=/:[0-9]+$/,C=function(a,b,c){a=a.split("&");for(var d=0;d<a.length;d++){var e=a[d].split("=");if(decodeURIComponent(e[0]).replace(/\+/g," ")===b)return b=e.slice(1).join("="),c?b:decodeURIComponent(b).replace(/\+/g," ")}},F=function(a,b){b&&(b=String(b).toLowerCase());if("p

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\bat[1].js	
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):	30494
Entropy (8bit):	5.30355290011164
Encrypted:	false
SSDEEP:	384:otKVCwh9wC22fo5EB4b7AWhbwM05Jkr9qNHfs9nB/wDSliNqCET8zT7QAEqnyJYk:ZCwhBR/DOZwDhzT7QSnSYyebQ
MD5:	5562385CBAFDDC33276BA10BA59890F7
SHA1:	A030EE46C99511E12EBB6257138FBE3E75232540
SHA-256:	73E2E5173ED0D5A77B02914FA0EF1F67BB53143DA75F0348F558F95565220CA1
SHA-512:	3D12741A718FE0CC3756C8018E29C07B84D28702E8783F42677431213CC4F79A6852C3A26A8D29C6FC515A069D4543C6114A0C56FC19AC48F680EE9439D2ECE7
Malicious:	false
IE Cache URL:	http://https://bat.bing.com/bat.js
Preview:	function UET(o){this.stringExists=function(n){return n&&n.length>0};this.domain="bat.bing.com";this.URLLENGTHLIMIT=4096;this.pageLoadEvt="pageLoad";this.customEvt="custom";this.pageViewEvt="page_view";o.Ver=o.Ver!==undefined&&(o.Ver==="1"||o.Ver===1)?1:2;this.uetConfig={};this.uetConfig.consent={enabled:!1,adStorageAllowed:!0,adStorageUpdated:!1,hasWaited:!1,waitForUpdate:0};this.beaconParams={};this.supportsCORS=this.supportsXDR=!1;this.paramValidations={string_currency:{type:"regex",regex:/^[a-zA-Z]{3}$/,error:"{p} value must be ISO standard currency code"},number:{type:"num",digits:3,max:999999999999},integer:{type:"num",digits:0,max:999999999999},hct_los:{type:"num",digits:0,max:30},date:{type:"regex",regex:/^\d{4}-\d{2}-\d{2}$/,error:"{p} value must be in YYYY-MM-DD date format"},"enum":{type:"enum",error:"{p} value must be one of the allowed values"},array:{type:"array",error:"{p} must be an array with 1+ elements"}};this.knownParams={event_action:{beacon:"ea"},event_category:{be

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\bolt-main-prod-old[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	2025262
Entropy (8bit):	5.619675393315964
Encrypted:	false
SSDEEP:	49152:9XnETJDfo8iVNQjUztndFsaL5599MeatTcHWx/ziVlDr86xO3wPi:GsQandFscpatTcHWx/ziVlDr86xO3wPi
MD5:	9F28BA3398110B8ADBAF3CFA5448424B
SHA1:	6DA96C048375B63FE8C53DF4DBD81982B7E5D268
SHA-256:	5248C7F1D9BC66B3F095B9DCF9A8205B1EB23807FCD7A5BF20DC79BB35514B1B
SHA-512:	CE203774E1A2AFAE29F76FD52FD5392F6CBBA7248C886EA032B26A441829B9D00DA2BB7AB3B162C53F513B3471C8679F38ADD737AA15BC6D1C83F9F76415B506
Malicious:	false
IE Cache URL:	http://https://static.parastorage.com/services/wix-bolt/1.7264.0/bolt-main/app/bolt-main-prod-old.js
Preview:	define(["lodash","coreUtilsLib","react","prop-types","warmupUtils","zepto","react-dom","santa-components","coreUtils","tpaComponents","color","thirdPartyAnalytics","create-react-class","layout-utils","layout","wix-dom-sanitizer","data-capsule","galleriesCommon","bolt-components"],function(e,t,n,r,a,o,i,s,u,l,c,p,d,f,g,m,v,y,h){return function(e){var t={};function n(r){if(t[r])return t[r].exports;var a=t[r]={i:r,l:!1,exports:{}};return e[r].call(a.exports,a,a.exports,n),a.l=!0,a.exports}return n.m=e,n.c=t,n.d=function(e,t,r){n.o(e,t)||Object.defineProperty(e,t,{enumerable:!0,get:r})},n.r=function(e){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(e,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(e,"__esModule",{value:!0})},n.t=function(e,t){if(1&t&&(e=n(e)),8&t)return e;if(4&t&&"object"==typeof e&&e&&e.__esModule)return e;var r=Object.create(null);if(n.r(r),Object.defineProperty(r,"default",{enumerable:!0,value:e}),2&t&&"string"!=typeof e)for(var a in e)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\bundle.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	65304
Entropy (8bit):	5.220447655902976
Encrypted:	false
SSDEEP:	768:5thPgk5Zi8QLtFJ0+nMACXn3nVWa062vjg4/aBkaAYPiIZRSfWRV0lspnFAz6QCs:pa0CUXgvjg4/UkaAYPigRLnkCdEhs0L
MD5:	CA197586ED80A7767CC602668C7B18BE
SHA1:	4C529C1C294D362DE3CC90CAF487FFEEA8827F56
SHA-256:	D58AE5786D8A1FECE18908C69B138536CB2FC61A5507ACFC2A7107A2D31F10DD

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\bundle.min[1].js	
SHA-512:	C857991615F1D1662F275648F757DC80BC8D13C6166C97ECAA121EA290211182D88CF6E1DBD443C313DEE20BC3A3238B01CF2D0908DB106080C32BC37E8D95(
Malicious:	false
IE Cache URL:	http://https://static.parastorage.com/unpkg/@wix/santa-bundle@1.1061.0/dist/bundle.min.js
Preview:	/** MobX - (c) Michel Weststrate 2015, 2016 - MIT Licensed */..!function(e){if("object"==typeof exports&&"undefined"!=typeof module)module.exports=e();else if("function"==typeof define&&define.amd)define("prop-types",[],e);else{var t;t="undefined"!=typeof window?window:"undefined"!=typeof global?global:"undefined"!=typeof self?self:this,t.PropTypes=e()}}(function(){return function e(t,n,r){function o(a,s){if(!n[a]){if(!t[a]){var u="function"==typeof require&&require;if(!s&&u)return u(a,!0);if(i)return i(a,!0);var c=new Error("Cannot find module '"+a+"'");throw c.code="MODULE_NOT_FOUND",c}var l=n[a]={exports:{}};t[a][0].call(l.exports,function(e){var n=t[a][1][e];return o(n||e)},l,l.exports,e,t,n,r)}return n[a].exports}for(var i="function"==typeof require&&require,a=0;a<r.length;a++)o(r[a]);return o}({1:[function(e,t){"use strict";var n=e(4),r=e(5),o=e(3);t.exports=function(){function e(e,t,n,i,a,s){s!==o&&r(!1,"Calling PropTypes validators directly is not supported by the `prop-types`

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\cdn_detect[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	11
Entropy (8bit):	3.459431618637298
Encrypted:	false
SSDEEP:	3:OWY:OWY
MD5:	7C12772809C1C0C3DEDA6103B10FDFA0
SHA1:	12039D6DD9A7E27622301E935B6EEFC78846802E
SHA-256:	4795A1C2517089E4DF569AFD77C04E949139CF299C87F012B894FCCF91DF4594
SHA-512:	3775186C9EDAD1CBDD412A66873511F2C34A65C93862C6B7AA4E1A39EBE354BE0B7E0353B3A24DAC6C09855D32F7630B496466F028E1420B38D2E35E2ECC026C
Malicious:	false
IE Cache URL:	http://https://static.parastorage.com/cdn_detect
Preview:	1234567890.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\custom-elements-polyfill.39b1b49f.chunk.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	18451
Entropy (8bit):	5.185439143536412
Encrypted:	false
SSDEEP:	384:vqtsdLFiBQZB0H/T5hXj2sRv1dHAjuHyq8TCr69t3F:vJjB+3VH8q49t3F
MD5:	DFE52C9F7BABD80F905E827D5F55933B
SHA1:	E7E488D0063A2C563A09DDF8868F00746D7E5CCE
SHA-256:	988E9DD23AA9172B6C5494C1C8F0CBF88ACC1D90D6B5014FE7884D024B28D326
SHA-512:	0AD23B1D6E46D4E7090EFEA9D7A5EE621D1A21F2AB7EC0D403C65365337178F6AC76E8F2E6CB20313AC4FB6B9CEE94115BF2833F0EE78A980CB669E80A74031
Malicious:	false
IE Cache URL:	http://https://static.parastorage.com/services/wix-thunderbolt/dist/custom-elements-polyfill.39b1b49f.chunk.min.js
Preview:	(self.webpackJsonp__wix_thunderbolt_app=self.webpackJsonp__wix_thunderbolt_app||[]).push([[6211],{45918:function(){(function(){"use strict";var t=window.Document.prototype.createElement,e=window.Document.prototype.createElementNS,n=window.Document.prototype.importNode,o=window.Document.prototype.prepend,r=window.Document.prototype.append,i=window.DocumentFragment.prototype.prepend,a=window.DocumentFragment.prototype.append,l=window.Node.prototype.cloneNode,c=window.Node.prototype.appendChild,s=window.Node.prototype.insertBefore,u=window.Node.prototype.removeChild,h=window.Node.prototype.replaceChild,f=Object.getOwnPropertyDescriptor(window.Node.prototype,"textContent"),d=window.Element.prototype.attachShadow,p=Object.getOwnPropertyDescriptor(window.Element.prototype,"innerHTML"),m=window.Element.prototype.getAttribute,w=window.Element.prototype.setAttribute,y=window.Element.prototype.removeAttribute,v=window.Element.prototype.getAttributeNS,E=window.Element.prototype.setAttributeNS,b=w

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\gsap.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	57826
Entropy (8bit):	5.336045925794379
Encrypted:	false
SSDEEP:	768:N1JsoGPTyHRUxrSOdlWfT2OlUFi2rLei2YCv0BiDTTW9t9gE0aZC3n5N:NDFGlrSGlWTCPb9b+
MD5:	663FD753CAE2B462CF8ED119C3F991AB
SHA1:	06A63BC0EC823880B5420C23071E3C3C0582C11A
SHA-256:	732117AC92A33B760D9290A33F1541762EE9449DC417EA249B5A0DF50738AD16
SHA-512:	D11607AA8380466A71344C3E7ACC4D1D768FA17594DFAB300BC6B90609A77B164D98E8437B00AF2913568AD262C1FE34A3C254B20F37D54BBF71120DEEC09D2
Malicious:	false
IE Cache URL:	http://https://static.parastorage.com/unpkg/@wix/santa-external-modules@1.644.0/tweenmax-plugins/3.1.1-transition-phase/gsap.min.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\gsap.min[1].js	
Preview:	/*!. * GSAP 3.1.1. * https://greensock.com. * . * @license Copyright 2020, GreenSock. All rights reserved.. * Subject to the terms at https://greensock.com/standard-license or for Club GreenSock members, the agreement issued with that membership.. * @author: Jack Doyle, jack@greensock.com. */..!function(t,e){"object"==typeof exp orts&&"undefined"!=typeof module?e(exports):"function"==typeof define&&define.amd?define(["exports"],e):e((t=t||self).window=t.window||{})}(this,function(e){"use strict"; function _inheritsLoose(t,e){t.prototype=Object.create(e.prototype),(t.prototype.constructor=t).__proto__=e}function _assertThisInitialized(t){if(void 0===t)throw new Ref erenceError("this hasn't been initialised - super() hasn't been called");return t}function n(t){return"string"==typeof t}function o(t){return"function"==typeof t}function p(t){retu rn"number"==typeof t}function q(t){return void 0===t}function r(t){return"object"==typeof t}function s(t){return!1!==t}function t(){return"undefined"!

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\imageClientApi[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	35995
Entropy (8bit):	5.575170334715127
Encrypted:	false
SSDEEP:	768:LlTm0T2sEA93iTuoaL1/QsUjpv0scpd1dpbxvFNdlcdmdsEs/dbgL0ziK:Vd3iTuoaL1/VXMPGL0eK
MD5:	BF11A31D6BD9EAD3F8EF9C871D38EAB7
SHA1:	EF16C90A04FF70B304F222A6FFC97336D817FED9
SHA-256:	7A1E77C13481F363D05F6612817E84C7C27F2E294AB84609C5442542F63C80AF
SHA-512:	6480175F9F08D142F4D71B31DB9AF6AF6E9E79EA804E50F7E576761E2FDFF8C2A271C388BA47C022735214A14D5A6CC47FF6CFF6FAE87625973B46DB58D18CC
Malicious:	false
IE Cache URL:	http://https://static.parastorage.com/unpkg/image-client-api@1.4060.0/dist/imageClientApi.js
Preview:	!function(e,t){"object"==typeof exports&&"object"==typeof module?module.exports=t():"function"==typeof define&&define.amd?define([],t):"object"==typeof exports? exports.imageClientApi=t():e.imageClientApi=t()}(this,(function(){return function(e){var t={};function i(r){if(t[r])return t[r].exports;var a=t[r]={i:r,l:!1,exports:{}};return e[r] .call(a.exports,a,a.exports,i),a.l=!0,a.exports}return i.m=e,i.c=t,i.d=function(e,t,r){i.o(e,t)||Object.defineProperty(e,t,{enumerable:!0,get:r})},i.r=function(e){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(e,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(e,"__esModule",{value:!0})},i.t=function(e,t){if(1&t&& (e=i(e)),8&t)return e;if(4&t&&"object"==typeof e&&e&&e.__esModule)return e;var r=Object.create(null);if(i.r(r),Object.defineProperty(r,"default",{enumerable:!0,value:e}),2& t&&"string"!=typeof e)for(var a in e)i.d(r,a,function(t){return e[t]}.bind(null,a));return r},i.n=function(e){var t=e&&e.__esModule?function

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\intersection-observer-polyfill.67fb87dd.chunk.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	8903
Entropy (8bit):	5.145462364242022
Encrypted:	false
SSDEEP:	192:Cg/PYNqqzDODGgXdDDo4SpQmNhhWa3DQgUtigFmgJWBC425NVGpJYh3gkC6YFZmy:CgH8t3ihXdDjsQmNhh3DJUJDJWBCjca2
MD5:	E9B45B82453DD736C5DF26BB5AF37C03
SHA1:	541A574186A57C42A2CF001745C311F75B7DE1CF
SHA-256:	B638F0A9AB14A9DEDDBA3576B7B8299C419D980ACFF9DE9EE1B62C02093C2F49
SHA-512:	B790FE7BB1D57741EA27462EAACB9A0E333473073CD221FC4E7372862FE69FDBC9E2B3060C1925E89682772B4599B31E046720379074948D9E10064FD1A95945
Malicious:	false
IE Cache URL:	http://https://static.parastorage.com/services/wix-thunderbolt/dist/intersection-observer-polyfill.67fb87dd.chunk.min.js
Preview:	(self.webpackJsonp__wix_thunderbolt_app=self.webpackJsonp__wix_thunderbolt_app||[]).push([[7294],{47946:function(){!function(){"use strict";if("object"==typeof window)if("IntersectionObserver"in window&&"IntersectionObserverEntry"in window&&"intersectionRatio"in window.IntersectionObserverEntry.prototype)"isIntersecting"in window.IntersectionObserverEntry.prototype||Object.defineProperty(window.IntersectionObserverEntry.prototype,"isIntersecting",{get:function(){return this.intersectio nRatio>0}});else{var t=window.document,e=[],n=null,o=null;r.prototype.THROTTLE_TIMEOUT=100,r.prototype.POLL_INTERVAL=null,r.prototype.USE_MUTATION_OBS ERVER=!0,r._setupCrossOriginUpdater=function(){return n||(n=function(t,n){o=t&&n?a(t,n):{top:0,bottom:0,left:0,right:0,width:0,height:0},e.forEach((function(t){t._checkFo rIntersections()}))},n)},r._resetCrossOriginUpdater=function(){n=null,o=null},r.prototype.observe=function(t){if(!this._observationTargets.some((function(e){return e.elem ent==t}))){if(!t||1!

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\layout.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	145100
Entropy (8bit):	5.2708595759890695
Encrypted:	false
SSDEEP:	1536:smMr3o1C+p78HehPcX4d4jMicDeEWuC5RWRwWeLFXU1MRPw25:ZWo1CdHehPcIKMifEWuC5gVcDPw25
MD5:	3C7BE492D3FCBF651216971F47F16B47
SHA1:	AD5ACD4A9EF738034D62240D58682AEB9C540490
SHA-256:	4420362D8F902E22B9562DB3B9AA303531AD297D15ED3E17BDDB19047A4C729D
SHA-512:	5F99DCCAA3864E5AD54EB6BDCB83D65F4B0A65A72BC8BA28DC1D8E058ED50B0639AE9203B3712346CF04BEB8CDBAC3D611A609ED703559CA94E1856CED0A E9C4
Malicious:	false
IE Cache URL:	http://https://static.parastorage.com/services/wix-bolt/1.7264.0/node_modules/wix-santa/dist/packages-bin/layout/layout.min.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\layout.min[1].js	
Preview:	define("layout",["lodash","zepto","experiment","warmupUtils","warmupUtilsLib","image-client-api","santa-components-layout"],(function(e,t,i,n,r,o,a){return function(e){var t={};function i(n){if(t[n])return t[n].exports;var r=t[n]={i:n,l:!1,exports:{}};return e[n].call(r.exports,r,r.exports,i),r.l=!0,r.exports}return i.m=e,i.c=t,i.d=function(e,t,n){i.o(e,t)||Object.defineProperty(e,t,{enumerable:!0,get:n})},i.r=function(e){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(e,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(e,"__esModule",{value:!0})},i.t=function(e,t){if(1&t&&(e=i(e)),8&t)return e;if(4&t&&"object"==typeof e&&e&&e.__esModule)return e;var n=Object.create(null);if(i.r(n),Object.defineProperty(n,"default",{enumerable:!0,value:e}),2&t&&"string"!=typeof e)for(var r in e)i.d(n,r,function(t){return e[t]}.bind(null,r));return n},i.n=function(e){var t=e&&e.__esModule?function(){return e.default}:function(){return e};return i.d(t,"a",t),t},i.o=function

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\main-r.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	191443
Entropy (8bit):	5.2866469331419434
Encrypted:	false
SSDEEP:	1536:a5xsbDr+ywcpJ5FkXK8zQY1OZ+CkZp9uiPHGHRBthURTCWbNX8KH1N+CF287peJQ:4ODFkXzE3d8YBmH1KlAq3
MD5:	E68524881B247597994CE5FAF1ACE88F
SHA1:	AC3DCD3CACBD8BB6D076171E6BD961CBC44A0659
SHA-256:	1EE4BD7DA67BCEDB101FA317B6B6619FEAAB6797458BF87D501B9846BE80FC8F
SHA-512:	4E2CD9EBB6A34F79745363713DFD511C1017FCBCF464D18547FBD28EC37B8FA76666D5EC62D2932B382535FC11DD67098E94C63551D1D89483E0FF506B9EFEE
Malicious:	false
IE Cache URL:	http://https://static.parastorage.com/services/wix-bolt/1.7264.0/bolt-main/app/main-r.min.js
Preview:	!function(e){function t(t){for(var n,o,i=t[0],a=t[1],s=0,c=[];s<i.length;s++)o=i[s],Object.prototype.hasOwnProperty.call(r,o)&&r[o]&&c.push(r[o][0]),r[o]=0;for(n in a)Object.prototype.hasOwnProperty.call(a,n)&&(e[n]=a[n]);for(u&&u(t);c.length;)c.shift()()}var n={},r={5:0};function o(t){if(n[t])return n[t].exports;var r=n[t]={i:t,l:!1,exports:{}};return e[t].call(r.exports,r,r.exports,o),r.l=!0,r.exports}o.e=function(e){var t=[],n=r[e];if(0!==n)if(n)t.push(n[2]);else{var i=new Promise(function(t,o){n=r[e]=[t,o]});t.push(n[2]=i);var a,s=document.createElement("script");s.charset="utf-8",s.timeout=1800,o.nc&&s.setAttribute("nonce",o.nc),s.src=function(e){return o.p+"bolt-main-r."+({1:"animations",2:"bolt-ds-viewer-manager",3:"custom-elements",4:"init",6:"vendors~bolt-ds-viewer-manager",7:"vendors~custom-elements",8:"vendors~init"}[e]||e)+".js"}(e),0!==s.src.indexOf(window.location.origin+"/")&&(s.crossOrigin="anonymous");var u=new Error;a=function(t){s.onerror=s.onload=null,clearTimeout(c

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\minified[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with LF, NEL line terminators
Category:	downloaded
Size (bytes):	137771
Entropy (8bit):	5.302873083232577
Encrypted:	false
SSDEEP:	1536:0krhOL89lCIR2/XW9Pu9CABZ4XCbbXHaNG5ViGTct:0kkLeFRoWfABZ4ybbX6A5V3Yt
MD5:	18EB21E8D1074FD7A594D3748BA0CB33
SHA1:	0A226FA07A6E2DB5F5F03F1E980740CB67CEBFFA
SHA-256:	C64775436F34A6D26E276BBBC97BECDA2D4C73F15D70D5B13587D72123DFC5FD
SHA-512:	8ADFD7C67270EE6B98B89C06E3983BE03C625736EEE178597A588CB664E5268390387AA5611771A10A77466210AFC7F47066D85EAF9207B89A2DAF04A796802B
Malicious:	false
IE Cache URL:	http://https://static.parastorage.com/unpkg/core-js-bundle@3.2.1/minified.js
Preview:	/**. * core-js 3.2.1. * https://github.com/zloirock/core-js. * License: http://rock.mit-license.org. * . 2019 Denis Pushkarev (zloirock.ru). */.!function(kt){"use strict";function __webpack_require__(t){if(e[t])return e[t].exports;var r=e[t]={i:t,l:!1,exports:{}};return n[t].call(r.exports,r,r.exports,__webpack_require__),r.l=!0,r.exports}var n,e={},__webpack_require__.m=n=[function(t,r,n){n(1),n(60),n(61),n(62),n(63),n(64),n(65),n(66),n(67),n(68),n(69),n(70),n(71),n(72),n(73),n(74),n(77),n(80),n(82),n(84),n(85),n(86),n(87),n(89),n(90),n(92),n(100),n(101),n(102),n(103),n(111),n(112),n(114),n(115),n(116),n(118),n(119),n(120),n(121),n(122),n(123),n(125),n(126),n(127),n(128),n(134),n(135),n(137),n(138),n(139),n(143),n(144),n(146),n(147),n(149),n(150),n(151),n(152),n(159),n(161),n(162),n(163),n(165),n(166),n(168),n(169),n(171),n(172),n(173),n(174),n(175),n(176),n(177),n(178),n(179),n(180),n(181),n(184),n(185),n(187),n(189),n(190),n(191),n(192),n(193),n(195),n(197),n(199),n(200),n(202),n

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\react.production.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	12463
Entropy (8bit):	5.381746255537871
Encrypted:	false
SSDEEP:	384:U97UMSCgItJCmeTfNQUlxwMmerA0NPYe7:ogI4SKxV
MD5:	EDF56A42BCA6B565BF7DFCBD8FFC221A
SHA1:	31CB4CEA0064ED80C1B0C5F5D58E1956A7E2293F
SHA-256:	C9486F126615859FC61AC84840A02B2EFC920D287A71D99D708C74B2947750FE
SHA-512:	49426E8E1B54599525C2C0016993674C5465BC2BBB5C605904BD55177DEA46FBE0364DE9052F44DF9DE471A838240BF4E7F9EC07DB1A9D25C56DD1C0516F7E9
Malicious:	false
IE Cache URL:	http://https://static.parastorage.com/unpkg/react@16.13.1/umd/react.production.min.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\react.production.min[1].js	
Preview:	/** @license React v16.13.1. * react.production.min.js. *. * Copyright (c) Facebook, Inc. and its affiliates.. *. * This source code is licensed under the MIT license found in the. * LICENSE file in the root directory of this source tree.. */.'use strict';(function(d,r){"object"===typeof exports&&"undefined"!==typeof module?r(exports):"function"===typeof define&&define.amd?define(["exports"],r):(d=d||self,r(d.React={}))})(this,function(d){function r(a){for(var b="https://reactjs.org/docs/error-decoder.html?invarian t="+a,c=1;c<arguments.length;c++)b+="&args[]="+encodeURIComponent(arguments[c]);return"Minified React error #"+a+"; visit "+b+" for the full message or use the non-minified dev environment for full errors and additional helpful warnings."}.function w(a,b,c){this.props=a;this.context=b;this.refs=ba;this.updater=c||ca}function da(){}function L(a,b,c){this.props=a;this.context=b;this.refs=ba;this.updater=c||ca}function ea(a,b,c){var g,e={},fa=null,d=null;if(null!=b)for(g in void

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\santa-animations[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	145106
Entropy (8bit):	5.232092877992787
Encrypted:	false
SSDEEP:	3072:JoIbR0xr9S3A97yVOHjbXYbBOx2GKEQmz1:JoIbR0xr9S3A97yVOHjbXYbBOx2GKElx
MD5:	19F081BF57FC59651F6948EBD9FE63D5
SHA1:	3173319BAD8974EB84224F416A293DC0F326E018
SHA-256:	B0BB3035E130188B671956EF5BD957B9281C19151CE60A742F4AD460CE1E3BC3
SHA-512:	9DCD07E8D680945017D75D76E32358E6AF2FF8219BE947A3AAAA87D73912BCC5C487AC8AC05697F360F994B25161AAC6BDECF4D84DF7B6A0461A4DD8BF04E6FD
Malicious:	false
IE Cache URL:	http://https://static.parastorage.com/unpkg/@wix/santa-animations@1.493.0/dist/santa-animations.js
Preview:	!function(e,t){"object"==typeof exports&&"object"==typeof module?module.exports=t():"function"==typeof define&&define.amd?define([],t):"object"==typeof exports?exports["santa-animations"]=t():e["santa-animations"]=t()}(this,(function(){return function(e){var t={};function n(r){if(t[r])return t[r].exports;var a=t[r]={i:r,l:!1,exports:{}};return e[r].call(a.exports,a,a.exports,n),a.l=!0,a.exports}return n.m=e,n.c=t,n.d=function(e,t,r){n.o(e,t)||Object.defineProperty(e,t,{enumerable:!0,get:r})},n.r=function(e){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(e,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(e,"__esModule",{value:!0})},n.t=function(e,t){if(1&t&&(e=n(e)),8&t)return e;if(4&t&&"object"==typeof e&&e&&e.__esModule)return e;var r=Object.create(null);if(n.r(r),Object.defineProperty(r,"default",{enumerable:!0,value:e}),2&t&&"string"!=typeof e)for(var a in e)n.d(r,a,function(t){return e[t]}.bind(null,a));return r},n.n=function(e){var t=e&&e.__esModul

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\santa-components-layout.prod[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	2983
Entropy (8bit):	5.216252227384569
Encrypted:	false
SSDEEP:	48:Zok0twETRDeVtSuMY69cL4l07kG2bXU2pUqbsXrH3ey8eW+NnW7zWbexZ88vEL:R0tNaSn1CQGegimHj8eaUe72L
MD5:	7E287BDF343DA557A915BFCB40AE08E4
SHA1:	96790857D76D8EA49F533C89D848FAC73DCCF76C
SHA-256:	C661B9B701C71340A925671BA2888A3E59AD66301D97490E82FAA8F5A01AE519
SHA-512:	9C4CE49CFBEB1855D68E65511F69C1E16AAEB75913764BEF9594C21DC55E1528FFF1F6797C35F59CF039807902D38F9918C24034B9D0EBA7552614D8350F66BB
Malicious:	false
IE Cache URL:	http://https://static.parastorage.com/unpkg/@wix/santa-components@1.1977.0/dist/santa-components-layout.prod.js
Preview:	!function(e,t){if("object"==typeof exports&&"object"==typeof module)module.exports=t(require("lodash"));else if("function"==typeof define&&define.amd)define(["lodash"],t);else{var n="object"==typeof exports?t(require("lodash")):t(e.lodash);for(var r in n)("object"==typeof exports?exports:e)[r]=n[r]}}(this,(function(e){return function(e){var t={};function n(r){if(t[r])return t[r].exports;var i=t[r]={i:r,l:!1,exports:{}};return e[r].call(i.exports,i,i.exports,n),i.l=!0,i.exports}return n.m=e,n.c=t,n.d=function(e,t,r){n.o(e,t)||Object.defineProperty(e,t,{enumerable:!0,get:r})},n.r=function(e){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(e,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(e,"__esModule",{value:!0})},n.t=function(e,t){if(1&t&&(e=n(e)),8&t)return e;if(4&t&&"object"==typeof e&&e&&e.__esModule)return e;var r=Object.create(null);if(n.r(r),Object.defineProperty(r,"default",{enumerable:!0,value:e}),2&t&&"string"!=typeof e)for(var i in e)n.d(r,i,f

Static File Info

General

File type:	Microsoft Word 2007+
Entropy (8bit):	7.946348698955512
TrID:	• Word Microsoft Office Open XML Format document (49504/1) 49.01% • Word Microsoft Office Open XML Format document (43504/1) 43.07% • ZIP compressed archive (8000/1) 7.92%
File name:	Corona als Dank.docx
File size:	109718
MD5:	a19832a2c9c96060b65abb12ec718d6e
SHA1:	3f7a955accb1b1a9ea77a8f02006fa8781f1232c

General

SHA256:	44756d412d9244cc966b63f44435779e9d9d6fe55fd15c08818b1614c8f81312
SHA512:	9bb1b9500e5c3a127571a6c44044c17dd6f15145b8941d790eb0032c3590239d94af8bde90c5c98eb6d366c68e0a0741df3b7fd6826e492e785954ccd09883c
SSDEEP:	3072:ZGm1JF9MOkRRiMZYt6tKeFd2NNKIHgJaFP/:ZGm1JFnsRi4sH1HgJad
File Content Preview:	PK.....!.7.....,.....[Content_Types].xml ...(..... ....

File Icon

Icon Hash:	74fcd0d2d6d6d0cc

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 28, 2021 14:56:08.686414957 CEST	192.168.2.4	8.8.8.8	0x7480	Standard query (0)	www.artsenvoorwaarheid.nl	A (IP address)	IN (0x0001)
Jun 28, 2021 14:56:09.303929090 CEST	192.168.2.4	8.8.8.8	0xeb9d	Standard query (0)	static.parastorage.com	A (IP address)	IN (0x0001)
Jun 28, 2021 14:56:09.306675911 CEST	192.168.2.4	8.8.8.8	0x1333	Standard query (0)	polyfill.io	A (IP address)	IN (0x0001)
Jun 28, 2021 14:56:09.923172951 CEST	192.168.2.4	8.8.8.8	0xeefd	Standard query (0)	static.wixstatic.com	A (IP address)	IN (0x0001)
Jun 28, 2021 14:56:10.067289114 CEST	192.168.2.4	8.8.8.8	0xa46c	Standard query (0)	frog.wix.com	A (IP address)	IN (0x0001)
Jun 28, 2021 14:56:13.328950882 CEST	192.168.2.4	8.8.8.8	0xc3d1	Standard query (0)	en.wix.com	A (IP address)	IN (0x0001)
Jun 28, 2021 14:56:13.691906929 CEST	192.168.2.4	8.8.8.8	0x7f8e	Standard query (0)	www.wix.com	A (IP address)	IN (0x0001)
Jun 28, 2021 14:56:13.841026068 CEST	192.168.2.4	8.8.8.8	0x9547	Standard query (0)	browser.sentry-cdn.com	A (IP address)	IN (0x0001)
Jun 28, 2021 14:56:14.232616901 CEST	192.168.2.4	8.8.8.8	0x87ac	Standard query (0)	sentry.wixpress.com	A (IP address)	IN (0x0001)
Jun 28, 2021 14:56:15.166482925 CEST	192.168.2.4	8.8.8.8	0xd1c8	Standard query (0)	fast.fonts.com	A (IP address)	IN (0x0001)
Jun 28, 2021 14:56:15.701128006 CEST	192.168.2.4	8.8.8.8	0xa7e5	Standard query (0)	siteassets.parastorage.com	A (IP address)	IN (0x0001)
Jun 28, 2021 14:56:21.098294020 CEST	192.168.2.4	8.8.8.8	0x64a8	Standard query (0)	4382365.fls.doubleclick.net	A (IP address)	IN (0x0001)
Jun 28, 2021 14:56:21.161947012 CEST	192.168.2.4	8.8.8.8	0xa70f	Standard query (0)	s.pinimg.com	A (IP address)	IN (0x0001)
Jun 28, 2021 14:56:21.213243961 CEST	192.168.2.4	8.8.8.8	0xa750	Standard query (0)	snap.licdn.com	A (IP address)	IN (0x0001)
Jun 28, 2021 14:56:21.227942944 CEST	192.168.2.4	8.8.8.8	0x8b7e	Standard query (0)	connect.facebook.net	A (IP address)	IN (0x0001)
Jun 28, 2021 14:56:21.623636961 CEST	192.168.2.4	8.8.8.8	0xd04a	Standard query (0)	stats.g.doubleclick.net	A (IP address)	IN (0x0001)
Jun 28, 2021 14:56:21.633166075 CEST	192.168.2.4	8.8.8.8	0x71bc	Standard query (0)	px.ads.linkedin.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 28, 2021 14:56:21.653441906 CEST	192.168.2.4	8.8.8.8	0xe48b	Standard query (0)	googleads.g.doubleclick.net	A (IP address)	IN (0x0001)
Jun 28, 2021 14:56:21.738883972 CEST	192.168.2.4	8.8.8.8	0xe60a	Standard query (0)	ct.pinterest.com	A (IP address)	IN (0x0001)
Jun 28, 2021 14:56:21.937613010 CEST	192.168.2.4	8.8.8.8	0xefe3	Standard query (0)	www.google.de	A (IP address)	IN (0x0001)
Jun 28, 2021 14:56:22.436162949 CEST	192.168.2.4	8.8.8.8	0xa5b7	Standard query (0)	www.linkedin.com	A (IP address)	IN (0x0001)
Jun 28, 2021 14:56:24.495573044 CEST	192.168.2.4	8.8.8.8	0x974	Standard query (0)	www.facebook.com	A (IP address)	IN (0x0001)
Jun 28, 2021 14:57:19.624751091 CEST	192.168.2.4	8.8.8.8	0x356a	Standard query (0)	static.parastorage.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 28, 2021 14:56:08.744843006 CEST	8.8.8.8	192.168.2.4	0x7480	No error (0)	www.artsenvoorwaarheid.nl	www179.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Jun 28, 2021 14:56:08.744843006 CEST	8.8.8.8	192.168.2.4	0x7480	No error (0)	www179.wixdns.net	balancer.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Jun 28, 2021 14:56:08.744843006 CEST	8.8.8.8	192.168.2.4	0x7480	No error (0)	balancer.wixdns.net	5f36b111-balancer.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Jun 28, 2021 14:56:08.744843006 CEST	8.8.8.8	192.168.2.4	0x7480	No error (0)	5f36b111-balancer.wixdns.net	td-balancer-euw2-6-109.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Jun 28, 2021 14:56:08.744843006 CEST	8.8.8.8	192.168.2.4	0x7480	No error (0)	td-balancer-euw2-6-109.wixdns.net		35.246.6.109	A (IP address)	IN (0x0001)
Jun 28, 2021 14:56:09.357274055 CEST	8.8.8.8	192.168.2.4	0x1333	No error (0)	polyfill.io		151.101.1.26	A (IP address)	IN (0x0001)
Jun 28, 2021 14:56:09.357274055 CEST	8.8.8.8	192.168.2.4	0x1333	No error (0)	polyfill.io		151.101.193.26	A (IP address)	IN (0x0001)
Jun 28, 2021 14:56:09.357274055 CEST	8.8.8.8	192.168.2.4	0x1333	No error (0)	polyfill.io		151.101.129.26	A (IP address)	IN (0x0001)
Jun 28, 2021 14:56:09.357274055 CEST	8.8.8.8	192.168.2.4	0x1333	No error (0)	polyfill.io		151.101.65.26	A (IP address)	IN (0x0001)
Jun 28, 2021 14:56:09.365129948 CEST	8.8.8.8	192.168.2.4	0xeb9d	No error (0)	static.parastorage.com	td-static-34-96-106-200.parastorage.com		CNAME (Canonical name)	IN (0x0001)
Jun 28, 2021 14:56:09.365129948 CEST	8.8.8.8	192.168.2.4	0xeb9d	No error (0)	td-static-34-96-106-200.parastorage.com		34.96.106.200	A (IP address)	IN (0x0001)
Jun 28, 2021 14:56:09.972014904 CEST	8.8.8.8	192.168.2.4	0xeefd	No error (0)	static.wixstatic.com	gcp.media-router.wixstatic.com		CNAME (Canonical name)	IN (0x0001)
Jun 28, 2021 14:56:09.972014904 CEST	8.8.8.8	192.168.2.4	0xeefd	No error (0)	gcp.media-router.wixstatic.com		34.102.176.152	A (IP address)	IN (0x0001)
Jun 28, 2021 14:56:10.125514984 CEST	8.8.8.8	192.168.2.4	0xa46c	No error (0)	frog.wix.com	bi-flogger-alb-ext-343643057.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jun 28, 2021 14:56:10.125514984 CEST	8.8.8.8	192.168.2.4	0xa46c	No error (0)	bi-flogger-alb-ext-343643057.us-east-1.elb.amazonaws.com		54.236.202.140	A (IP address)	IN (0x0001)
Jun 28, 2021 14:56:10.125514984 CEST	8.8.8.8	192.168.2.4	0xa46c	No error (0)	bi-flogger-alb-ext-343643057.us-east-1.elb.amazonaws.com		18.211.135.58	A (IP address)	IN (0x0001)
Jun 28, 2021 14:56:10.125514984 CEST	8.8.8.8	192.168.2.4	0xa46c	No error (0)	bi-flogger-alb-ext-343643057.us-east-1.elb.amazonaws.com		54.145.24.80	A (IP address)	IN (0x0001)
Jun 28, 2021 14:56:10.125514984 CEST	8.8.8.8	192.168.2.4	0xa46c	No error (0)	bi-flogger-alb-ext-343643057.us-east-1.elb.amazonaws.com		3.89.173.226	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 28, 2021 14:56:10.125514984 CEST	8.8.8.8	192.168.2.4	0xa46c	No error (0)	bi-flogger-alb-ext-343643057.us-east-1.elb.amazonaws.com		54.175.222.143	A (IP address)	IN (0x0001)
Jun 28, 2021 14:56:10.125514984 CEST	8.8.8.8	192.168.2.4	0xa46c	No error (0)	bi-flogger-alb-ext-343643057.us-east-1.elb.amazonaws.com		34.202.132.253	A (IP address)	IN (0x0001)
Jun 28, 2021 14:56:10.125514984 CEST	8.8.8.8	192.168.2.4	0xa46c	No error (0)	bi-flogger-alb-ext-343643057.us-east-1.elb.amazonaws.com		54.91.27.83	A (IP address)	IN (0x0001)
Jun 28, 2021 14:56:10.125514984 CEST	8.8.8.8	192.168.2.4	0xa46c	No error (0)	bi-flogger-alb-ext-343643057.us-east-1.elb.amazonaws.com		52.71.197.101	A (IP address)	IN (0x0001)
Jun 28, 2021 14:56:13.387278080 CEST	8.8.8.8	192.168.2.4	0xc3d1	No error (0)	en.wix.com	username.wix.com		CNAME (Canonical name)	IN (0x0001)
Jun 28, 2021 14:56:13.387278080 CEST	8.8.8.8	192.168.2.4	0xc3d1	No error (0)	username.wix.com	5f36b111-username.wix.com		CNAME (Canonical name)	IN (0x0001)
Jun 28, 2021 14:56:13.387278080 CEST	8.8.8.8	192.168.2.4	0xc3d1	No error (0)	5f36b111-username.wix.com	td-username-euw2-6-109.wix.com		CNAME (Canonical name)	IN (0x0001)
Jun 28, 2021 14:56:13.387278080 CEST	8.8.8.8	192.168.2.4	0xc3d1	No error (0)	td-username-euw2-6-109.wix.com		35.246.6.109	A (IP address)	IN (0x0001)
Jun 28, 2021 14:56:13.748250008 CEST	8.8.8.8	192.168.2.4	0x7f8e	No error (0)	www.wix.com	wwworigin.wix.com		CNAME (Canonical name)	IN (0x0001)
Jun 28, 2021 14:56:13.748250008 CEST	8.8.8.8	192.168.2.4	0x7f8e	No error (0)	wwworigin.wix.com	179.www.sv5.wix.com		CNAME (Canonical name)	IN (0x0001)
Jun 28, 2021 14:56:13.748250008 CEST	8.8.8.8	192.168.2.4	0x7f8e	No error (0)	179.www.sv5.wix.com		185.230.61.179	A (IP address)	IN (0x0001)
Jun 28, 2021 14:56:13.893599033 CEST	8.8.8.8	192.168.2.4	0x9547	No error (0)	browser.sentry-cdn.com		151.101.130.217	A (IP address)	IN (0x0001)
Jun 28, 2021 14:56:13.893599033 CEST	8.8.8.8	192.168.2.4	0x9547	No error (0)	browser.sentry-cdn.com		151.101.194.217	A (IP address)	IN (0x0001)
Jun 28, 2021 14:56:13.893599033 CEST	8.8.8.8	192.168.2.4	0x9547	No error (0)	browser.sentry-cdn.com		151.101.66.217	A (IP address)	IN (0x0001)
Jun 28, 2021 14:56:13.893599033 CEST	8.8.8.8	192.168.2.4	0x9547	No error (0)	browser.sentry-cdn.com		151.101.2.217	A (IP address)	IN (0x0001)
Jun 28, 2021 14:56:14.293071032 CEST	8.8.8.8	192.168.2.4	0x87ac	No error (0)	sentry.wixpress.com	sentry-nlb-e70282e8a06dcc98.elb.us-east-1.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jun 28, 2021 14:56:14.293071032 CEST	8.8.8.8	192.168.2.4	0x87ac	No error (0)	sentry-nlb-e70282e8a06dcc98.elb.us-east-1.amazonaws.com		52.2.188.208	A (IP address)	IN (0x0001)
Jun 28, 2021 14:56:15.224313021 CEST	8.8.8.8	192.168.2.4	0xd1c8	No error (0)	fast.fonts.com		104.17.70.188	A (IP address)	IN (0x0001)
Jun 28, 2021 14:56:15.224313021 CEST	8.8.8.8	192.168.2.4	0xd1c8	No error (0)	fast.fonts.com		104.17.71.188	A (IP address)	IN (0x0001)
Jun 28, 2021 14:56:15.787894964 CEST	8.8.8.8	192.168.2.4	0xa7e5	No error (0)	siteassets.parastorage.com	static.parastorage.com		CNAME (Canonical name)	IN (0x0001)
Jun 28, 2021 14:56:15.787894964 CEST	8.8.8.8	192.168.2.4	0xa7e5	No error (0)	static.parastorage.com	td-static-34-96-106-200.parastorage.com		CNAME (Canonical name)	IN (0x0001)
Jun 28, 2021 14:56:15.787894964 CEST	8.8.8.8	192.168.2.4	0xa7e5	No error (0)	td-static-34-96-106-200.parastorage.com		34.96.106.200	A (IP address)	IN (0x0001)
Jun 28, 2021 14:56:21.164236069 CEST	8.8.8.8	192.168.2.4	0x64a8	No error (0)	4382365.fls.doubleclick.net	dart.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 28, 2021 14:56:21.164236069 CEST	8.8.8.8	192.168.2.4	0x64a8	No error (0)	dart.l.doubleclick.net		142.250.185.198	A (IP address)	IN (0x0001)
Jun 28, 2021 14:56:21.227202892 CEST	8.8.8.8	192.168.2.4	0xa70f	No error (0)	s.pinimg.com	s-pinimg-com.gslb.pinterest.com		CNAME (Canonical name)	IN (0x0001)
Jun 28, 2021 14:56:21.227202892 CEST	8.8.8.8	192.168.2.4	0xa70f	No error (0)	s-pinimg-com.gslb.pinterest.com	2-01-37d2-0006.cdx.cedexis.net		CNAME (Canonical name)	IN (0x0001)
Jun 28, 2021 14:56:21.273864031 CEST	8.8.8.8	192.168.2.4	0xa750	No error (0)	snap.licdn.com	wildcard.licdn.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jun 28, 2021 14:56:21.285301924 CEST	8.8.8.8	192.168.2.4	0x8b7e	No error (0)	connect.facebook.net	scontent.xx.fbcdn.net		CNAME (Canonical name)	IN (0x0001)
Jun 28, 2021 14:56:21.285301924 CEST	8.8.8.8	192.168.2.4	0x8b7e	No error (0)	scontent.xx.fbcdn.net		157.240.17.15	A (IP address)	IN (0x0001)
Jun 28, 2021 14:56:21.672188044 CEST	8.8.8.8	192.168.2.4	0xd04a	No error (0)	stats.g.doubleclick.net	stats.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Jun 28, 2021 14:56:21.672188044 CEST	8.8.8.8	192.168.2.4	0xd04a	No error (0)	stats.l.doubleclick.net		108.177.15.154	A (IP address)	IN (0x0001)
Jun 28, 2021 14:56:21.672188044 CEST	8.8.8.8	192.168.2.4	0xd04a	No error (0)	stats.l.doubleclick.net		108.177.15.155	A (IP address)	IN (0x0001)
Jun 28, 2021 14:56:21.672188044 CEST	8.8.8.8	192.168.2.4	0xd04a	No error (0)	stats.l.doubleclick.net		108.177.15.157	A (IP address)	IN (0x0001)
Jun 28, 2021 14:56:21.672188044 CEST	8.8.8.8	192.168.2.4	0xd04a	No error (0)	stats.l.doubleclick.net		108.177.15.156	A (IP address)	IN (0x0001)
Jun 28, 2021 14:56:21.697005033 CEST	8.8.8.8	192.168.2.4	0x71bc	No error (0)	px.ads.linkedin.com	mix.linkedin.com		CNAME (Canonical name)	IN (0x0001)
Jun 28, 2021 14:56:21.697005033 CEST	8.8.8.8	192.168.2.4	0x71bc	No error (0)	mix.linkedin.com	glb-na.mix.linkedin.com		CNAME (Canonical name)	IN (0x0001)
Jun 28, 2021 14:56:21.697005033 CEST	8.8.8.8	192.168.2.4	0x71bc	No error (0)	glb-na.mix.linkedin.com	pop-esv5.mix.linkedin.com		CNAME (Canonical name)	IN (0x0001)
Jun 28, 2021 14:56:21.697005033 CEST	8.8.8.8	192.168.2.4	0x71bc	No error (0)	pop-esv5.mix.linkedin.com		108.174.11.37	A (IP address)	IN (0x0001)
Jun 28, 2021 14:56:21.701179028 CEST	8.8.8.8	192.168.2.4	0xe48b	No error (0)	googleads.g.doubleclick.net		172.217.16.130	A (IP address)	IN (0x0001)
Jun 28, 2021 14:56:21.798994064 CEST	8.8.8.8	192.168.2.4	0xe60a	No error (0)	ct.pinterest.com	www.pinterest.com		CNAME (Canonical name)	IN (0x0001)
Jun 28, 2021 14:56:21.798994064 CEST	8.8.8.8	192.168.2.4	0xe60a	No error (0)	www.pinterest.com	www-pinterest-com.gslb.pinterest.com		CNAME (Canonical name)	IN (0x0001)
Jun 28, 2021 14:56:21.798994064 CEST	8.8.8.8	192.168.2.4	0xe60a	No error (0)	www-pinterest-com.gslb.pinterest.com	2-01-37d2-0018.cdx.cedexis.net		CNAME (Canonical name)	IN (0x0001)
Jun 28, 2021 14:56:21.798994064 CEST	8.8.8.8	192.168.2.4	0xe60a	No error (0)	prod.pinterest.global.map.fastly.net		151.101.0.84	A (IP address)	IN (0x0001)
Jun 28, 2021 14:56:21.798994064 CEST	8.8.8.8	192.168.2.4	0xe60a	No error (0)	prod.pinterest.global.map.fastly.net		151.101.64.84	A (IP address)	IN (0x0001)
Jun 28, 2021 14:56:21.798994064 CEST	8.8.8.8	192.168.2.4	0xe60a	No error (0)	prod.pinterest.global.map.fastly.net		151.101.128.84	A (IP address)	IN (0x0001)
Jun 28, 2021 14:56:21.798994064 CEST	8.8.8.8	192.168.2.4	0xe60a	No error (0)	prod.pinterest.global.map.fastly.net		151.101.192.84	A (IP address)	IN (0x0001)
Jun 28, 2021 14:56:22.004501104 CEST	8.8.8.8	192.168.2.4	0xefe3	No error (0)	www.google.de		142.250.186.35	A (IP address)	IN (0x0001)
Jun 28, 2021 14:56:22.483685017 CEST	8.8.8.8	192.168.2.4	0xa5b7	No error (0)	www.linkedin.com	www-linkedin-com.l-0005.l-msedge.net		CNAME (Canonical name)	IN (0x0001)
Jun 28, 2021 14:56:24.557657957 CEST	8.8.8.8	192.168.2.4	0x974	No error (0)	www.facebook.com	star-mini.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 28, 2021 14:56:24.557657957 CEST	8.8.8.8	192.168.2.4	0x974	No error (0)	star-mini.c10r.facebook.com		157.240.17.35	A (IP address)	IN (0x0001)
Jun 28, 2021 14:57:19.671391964 CEST	8.8.8.8	192.168.2.4	0x356a	No error (0)	static.parastorage.com	td-static-34-96-106-200.parastorage.com		CNAME (Canonical name)	IN (0x0001)
Jun 28, 2021 14:57:19.671391964 CEST	8.8.8.8	192.168.2.4	0x356a	No error (0)	td-static-34-96-106-200.parastorage.com		34.96.106.200	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.artsenvoorwaarheid.nl

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49765	35.246.6.109	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jun 28, 2021 14:56:08.826327085 CEST	1546	OUT	GET / HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: www.artsenvoorwaarheid.nl Connection: Keep-Alive
Jun 28, 2021 14:56:08.898066998 CEST	1547	IN	HTTP/1.1 301 Moved Permanently Date: Mon, 28 Jun 2021 12:56:08 GMT Content-Length: 0 Connection: keep-alive location: https://www.artsenvoorwaarheid.nl/ strict-transport-security: max-age=120 Age: 5722 Server-Timing: cache;desc=hit, varnish;desc=hit, dc;desc=euw2 X-Seen-By: sHU62EDOGnH2FBkJkG/Wx8EeXWsWdHrhlvbxtlynkVgPe+WFeWpo3WXm+APPEjUG,qquldgcFrj2n046g4RNSVJWsHd48QfxhscEwgNQIOKxYgeUJqUXtid+86vZww+nL,2d58ifebGbosy5xc+FRalqdX8831MFHXFKqRYaEZzAcOJWkxZCqq91Ges8EO1XyOGgqFbFMYwiXnFojPwdof6FXyyNPi0zmFz5puF55pXZQ=,2UNV7KOq4oGjA5+PKsX47JpxpkqGEXQxSEKO4wY/fJs= Cache-Control: no-cache X-Wix-Request-Id: 1624884968.872535880792117868 X-Content-Type-Options: nosniff Server: Pepyaka/1.19.0

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
Jun 28, 2021 14:56:09.042582035 CEST	35.246.6.109	443	192.168.2.4	49767	CN=artsenvoorwaarheid.nl CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Sun Jun 06 02:00:00 CEST 2021 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Sun Sep 05 01:59:59 CEST 2021 Wed Jan 01 00:59:59 CET 2031 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=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jun 28, 2021 14:56:09.449846029 CEST	34.96.106.200	443	192.168.2.4	49771	CN=*.parastorage.com CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, 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 CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Sun Feb 07 01:00:00 CET 2021 Thu Jan 01 01:00:00 CET 2004 Tue Mar 12 01:00:00 CET 2019 Fri Nov 02 01:00:00 CET 2018	Sat Aug 07 01:59:59 CEST 2021 Mon Jan 01 00:59:59 CET 2029 Mon Jan 01 00:59:59 CET 2029 Wed Jan 01 00:59:59 CET 2031	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=AAA Certificate Services, 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		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
Jun 28, 2021 14:56:09.449937105 CEST	151.101.1.26	443	192.168.2.4	49768	CN=polyfill.io CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Fri Jun 04 21:31:46 CEST 2021 Tue Jul 28 02:00:00 CEST 2020	Wed Jul 06 21:31:45 CEST 2022 Sun Mar 18 01:00:00 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=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Jul 28 02:00:00 CEST 2020	Sun Mar 18 01:00:00 CET 2029		
Jun 28, 2021 14:56:09.450237036 CEST	151.101.1.26	443	192.168.2.4	49769	CN=polyfill.io CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Fri Jun 04 21:31:46 CEST 2021 Tue Jul 28 02:00:00 CEST 2020	Wed Jul 06 21:31:45 CEST 2022 Sun Mar 18 01:00:00 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=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Jul 28 02:00:00 CEST 2020	Sun Mar 18 01:00:00 CET 2029		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jun 28, 2021 14:56:09.453197002 CEST	34.96.106.200	443	192.168.2.4	49770	CN=*.parastorage.com CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, 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 CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Sun Feb 07 01:00:00 CET 2021 Thu Jan 01 01:00:00 CET 2004 Tue Mar 12 01:00:00 CET 2019 Fri Nov 02 01:00:00 CET 2018	Sat Aug 07 01:59:59 CEST 2021 Mon Jan 01 00:59:59 CET 2029 Mon Jan 01 00:59:59 CET 2029 Wed Jan 01 00:59:59 CET 2031	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=AAA Certificate Services, 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		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
Jun 28, 2021 14:56:09.478815079 CEST	34.96.106.200	443	192.168.2.4	49772	CN=*.parastorage.com CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, 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 CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Sun Feb 07 01:00:00 CET 2021 Thu Jan 01 01:00:00 CET 2004 Tue Mar 12 01:00:00 CET 2019 Fri Nov 02 01:00:00 CET 2018	Sat Aug 07 01:59:59 CEST 2021 Mon Jan 01 00:59:59 CET 2029 Mon Jan 01 00:59:59 CET 2029 Wed Jan 01 00:59:59 CET 2031	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=AAA Certificate Services, 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		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jun 28, 2021 14:56:09.482419014 CEST	34.96.106.200	443	192.168.2.4	49774	CN=*.parastorage.com CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, 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 CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Sun Feb 07 01:00:00 CET 2021 Thu Jan 01 01:00:00 CET 2004 Tue Mar 12 01:00:00 CET 2019 Fri Nov 02 01:00:00 CET 2018	Sat Aug 07 01:59:59 CEST 2021 Mon Jan 01 00:59:59 CET 2029 Mon Jan 01 00:59:59 CET 2029 Wed Jan 01 00:59:59 CET 2031	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=AAA Certificate Services, 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		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
Jun 28, 2021 14:56:09.483109951 CEST	34.96.106.200	443	192.168.2.4	49773	CN=*.parastorage.com CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, 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 CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Sun Feb 07 01:00:00 CET 2021 Thu Jan 01 01:00:00 CET 2004 Tue Mar 12 01:00:00 CET 2019 Fri Nov 02 01:00:00 CET 2018	Sat Aug 07 01:59:59 CEST 2021 Mon Jan 01 00:59:59 CET 2029 Mon Jan 01 00:59:59 CET 2029 Wed Jan 01 00:59:59 CET 2031	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=AAA Certificate Services, 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		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jun 28, 2021 14:56:09.487333059 CEST	34.96.106.200	443	192.168.2.4	49775	CN=*.parastorage.com CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, 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 CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Sun Feb 07 01:00:00 CET 2021 Thu Jan 01 01:00:00 CET 2004 Tue Mar 12 01:00:00 CET 2019 Fri Nov 02 01:00:00 CET 2018	Sat Aug 07 01:59:59 CEST 2021 Mon Jan 01 00:59:59 CET 2029 Mon Jan 01 00:59:59 CET 2029 Wed Jan 01 00:59:59 CET 2031	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=AAA Certificate Services, 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		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
Jun 28, 2021 14:56:10.065695047 CEST	34.102.176.152	443	192.168.2.4	49777	CN=*.wixstatic.com CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, 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 CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Feb 05 01:00:00 CET 2021 Thu Jan 01 01:00:00 CET 2004 Tue Mar 12 01:00:00 CET 2019 Fri Nov 02 01:00:00 CET 2018	Thu Aug 05 01:59:59 CEST 2021 Mon Jan 01 00:59:59 CET 2029 Mon Jan 01 00:59:59 CET 2029 Wed Jan 01 00:59:59 CET 2031	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=AAA Certificate Services, 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		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jun 28, 2021 14:56:10.067296982 CEST	34.102.176.152	443	192.168.2.4	49776	CN=*.wixstatic.com CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, 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 CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Feb 05 01:00:00 CET 2021 Thu Jan 01 01:00:00 CET 2004 Tue Mar 12 01:00:00 CET 2019 Fri Nov 02 01:00:00 CET 2018	Thu Aug 05 01:59:59 CEST 2021 Mon Jan 01 00:59:59 CET 2029 Mon Jan 01 00:59:59 CET 2029 Wed Jan 01 00:59:59 CET 2031	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=AAA Certificate Services, 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		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
Jun 28, 2021 14:56:10.629237890 CEST	54.236.202.140	443	192.168.2.4	49778	CN=*.wix.com CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, 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 CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Wed May 05 02:00:00 CEST 2021 Thu Jan 01 01:00:00 CET 2004 Tue Mar 12 01:00:00 CET 2019 Fri Nov 02 01:00:00 CET 2018	Tue Nov 02 00:59:59 CET 2021 Mon Jan 01 00:59:59 CET 2029 Mon Jan 01 00:59:59 CET 2029 Wed Jan 01 00:59:59 CET 2031	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=AAA Certificate Services, 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		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jun 28, 2021 14:56:10.631704092 CEST	54.236.202.140	443	192.168.2.4	49779	CN=*.wix.com CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, 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 CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Wed May 05 02:00:00 CEST 2021 Thu Jan 01 01:00:00 CET 2004 Tue Mar 12 01:00:00 CET 2019 Fri Nov 02 01:00:00 CET 2018	Tue Nov 02 00:59:59 CET 2021 Mon Jan 01 00:59:59 CET 2029 Mon Jan 01 00:59:59 CET 2029 Wed Jan 01 00:59:59 CET 2031	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=AAA Certificate Services, 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		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
Jun 28, 2021 14:56:13.544430017 CEST	35.246.6.109	443	192.168.2.4	49780	CN=*.wix.com CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, 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 CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Wed May 05 02:00:00 CEST 2021 Thu Jan 01 01:00:00 CET 2004 Tue Mar 12 01:00:00 CET 2019 Fri Nov 02 01:00:00 CET 2018	Tue Nov 02 00:59:59 CET 2021 Mon Jan 01 00:59:59 CET 2029 Mon Jan 01 00:59:59 CET 2029 Wed Jan 01 00:59:59 CET 2031	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=AAA Certificate Services, 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		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jun 28, 2021 14:56:13.545160055 CEST	35.246.6.109	443	192.168.2.4	49781	CN=*.wix.com CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, 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 CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Wed May 05 02:00:00 CEST 2021 Thu Jan 01 01:00:00 CET 2004 Tue Mar 12 01:00:00 CET 2019 Fri Nov 02 01:00:00 CET 2018	Tue Nov 02 00:59:59 CET 2021 Mon Jan 01 00:59:59 CET 2029 Mon Jan 01 00:59:59 CET 2029 Wed Jan 01 00:59:59 CET 2031	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=AAA Certificate Services, 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		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
Jun 28, 2021 14:56:14.069272041 CEST	151.101.130.217	443	192.168.2.4	49784	CN=*.sentry-cdn.com CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Mon Feb 22 20:39:57 CET 2021 Tue Jul 28 02:00:00 CEST 2020	Sat Mar 26 20:39:57 CET 2022 Sun Mar 18 01:00:00 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=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Jul 28 02:00:00 CEST 2020	Sun Mar 18 01:00:00 CET 2029		
Jun 28, 2021 14:56:14.069518089 CEST	151.101.130.217	443	192.168.2.4	49785	CN=*.sentry-cdn.com CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Mon Feb 22 20:39:57 CET 2021 Tue Jul 28 02:00:00 CEST 2020	Sat Mar 26 20:39:57 CET 2022 Sun Mar 18 01:00:00 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=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Jul 28 02:00:00 CEST 2020	Sun Mar 18 01:00:00 CET 2029		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jun 28, 2021 14:56:14.183283091 CEST	185.230.61.179	443	192.168.2.4	49782	CN=*.wix.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, 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	Wed May 05 02:00:00 CEST 2021 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019 Thu Jan 01 01:00:00 CET 2004	Tue Nov 02 00:59:59 CET 2021 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029 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=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
					CN=AAA Certificate Services, 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		
Jun 28, 2021 14:56:14.251931906 CEST	185.230.61.179	443	192.168.2.4	49783	CN=*.wix.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, 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	Wed May 05 02:00:00 CEST 2021 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019 Thu Jan 01 01:00:00 CET 2004	Tue Nov 02 00:59:59 CET 2021 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029 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=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
					CN=AAA Certificate Services, 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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jun 28, 2021 14:56:14.619019985 CEST	52.2.188.208	443	192.168.2.4	49787	CN=*.wixpress.com CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, 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 CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Sun Jan 31 01:00:00 CET 2021 Thu Jan 01 01:00:00 CET 2004 Tue Mar 12 01:00:00 CET 2019 Fri Nov 02 01:00:00 CET 2018	Sat Jul 31 01:59:59 CEST 2021 Mon Jan 01 00:59:59 CET 2029 Mon Jan 01 00:59:59 CET 2029 Wed Jan 01 00:59:59 CET 2031	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=AAA Certificate Services, 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		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
Jun 28, 2021 14:56:14.619600058 CEST	52.2.188.208	443	192.168.2.4	49788	CN=*.wixpress.com CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, 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 CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Sun Jan 31 01:00:00 CET 2021 Thu Jan 01 01:00:00 CET 2004 Tue Mar 12 01:00:00 CET 2019 Fri Nov 02 01:00:00 CET 2018	Sat Jul 31 01:59:59 CEST 2021 Mon Jan 01 00:59:59 CET 2029 Mon Jan 01 00:59:59 CET 2029 Wed Jan 01 00:59:59 CET 2031	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=AAA Certificate Services, 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		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jun 28, 2021 14:56:14.621368885 CEST	52.2.188.208	443	192.168.2.4	49786	CN=*.wixpress.com CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, 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 CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Sun Jan 31 01:00:00 CET 2021 Thu Jan 01 01:00:00 CET 2004 Tue Mar 12 01:00:00 CET 2019 Fri Nov 02 01:00:00 CET 2018	Sat Jul 31 01:59:59 CEST 2021 Mon Jan 01 00:59:59 CET 2029 Mon Jan 01 00:59:59 CET 2029 Wed Jan 01 00:59:59 CET 2031	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=AAA Certificate Services, 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		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
Jun 28, 2021 14:56:15.316205025 CEST	104.17.70.188	443	192.168.2.4	49789	CN=*.fonts.com, O=Monotype Imaging Inc., L=Woburn, ST=Massachusetts, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 02 01:00:00 CET 2020 Fri Mar 08 13:00:00 CET 2013	Wed Nov 17 00:59:59 CET 2021 Wed Mar 08 13:00:00 CET 2023	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
Jun 28, 2021 14:56:15.331408978 CEST	104.17.70.188	443	192.168.2.4	49790	CN=*.fonts.com, O=Monotype Imaging Inc., L=Woburn, ST=Massachusetts, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 02 01:00:00 CET 2020 Fri Mar 08 13:00:00 CET 2013	Wed Nov 17 00:59:59 CET 2021 Wed Mar 08 13:00:00 CET 2023	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jun 28, 2021 14:56:15.924487114 CEST	34.96.106.200	443	192.168.2.4	49792	CN=*.parastorage.com CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, 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 CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Sun Feb 07 01:00:00 CET 2021 Thu Jan 01 01:00:00 CET 2004 Tue Mar 12 01:00:00 CET 2019 Fri Nov 02 01:00:00 CET 2018	Sat Aug 07 01:59:59 CEST 2021 Mon Jan 01 00:59:59 CET 2029 Mon Jan 01 00:59:59 CET 2029 Wed Jan 01 00:59:59 CET 2031	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=AAA Certificate Services, 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		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
Jun 28, 2021 14:56:15.924735069 CEST	34.96.106.200	443	192.168.2.4	49791	CN=*.parastorage.com CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, 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 CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Sun Feb 07 01:00:00 CET 2021 Thu Jan 01 01:00:00 CET 2004 Tue Mar 12 01:00:00 CET 2019 Fri Nov 02 01:00:00 CET 2018	Sat Aug 07 01:59:59 CEST 2021 Mon Jan 01 00:59:59 CET 2029 Mon Jan 01 00:59:59 CET 2029 Wed Jan 01 00:59:59 CET 2031	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=AAA Certificate Services, 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		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jun 28, 2021 14:56:21.279805899 CEST	142.250.185.198	443	192.168.2.4	49799	CN=*.doubleclick.net CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Mon May 31 03:31:25 CEST 2021 Thu Aug 13 02:00:42 CEST 2020 Fri Jun 19 02:00:42 CEST 2020	Mon Aug 23 03:31:24 CEST 2021 Thu Sep 30 02:00:42 CEST 2027 Fri Jan 28 01:00:42 CET 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1C3, O=Google Trust Services LLC, C=US	CN=GTS Root R1, O=Google Trust Services LLC, C=US	Thu Aug 13 02:00:42 CEST 2020	Thu Sep 30 02:00:42 CEST 2027		
					CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Fri Jun 19 02:00:42 CEST 2020	Fri Jan 28 01:00:42 CET 2028		
Jun 28, 2021 14:56:21.283658981 CEST	142.250.185.198	443	192.168.2.4	49800	CN=*.doubleclick.net CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Mon May 31 03:31:25 CEST 2021 Thu Aug 13 02:00:42 CEST 2020 Fri Jun 19 02:00:42 CEST 2020	Mon Aug 23 03:31:24 CEST 2021 Thu Sep 30 02:00:42 CEST 2027 Fri Jan 28 01:00:42 CET 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1C3, O=Google Trust Services LLC, C=US	CN=GTS Root R1, O=Google Trust Services LLC, C=US	Thu Aug 13 02:00:42 CEST 2020	Thu Sep 30 02:00:42 CEST 2027		
					CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Fri Jun 19 02:00:42 CEST 2020	Fri Jan 28 01:00:42 CET 2028		
Jun 28, 2021 14:56:21.356244087 CEST	157.240.17.15	443	192.168.2.4	49807	CN=*.facebook.com, O="Facebook, Inc.", L=Menlo Park, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed May 26 02:00:00 CEST 2021 Tue Oct 22 14:00:00 CEST 2013	Wed Aug 25 01:59:59 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Jun 28, 2021 14:56:21.424819946 CEST	157.240.17.15	443	192.168.2.4	49808	CN=*.facebook.com, O="Facebook, Inc.", L=Menlo Park, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed May 26 02:00:00 CEST 2021 Tue Oct 22 14:00:00 CEST 2013	Wed Aug 25 01:59:59 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jun 28, 2021 14:56:21.787347078 CEST	108.177.15.154	443	192.168.2.4	49809	CN=*.g.doubleclick.net, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Mon May 31 03:33:18 CEST 2021 Thu Jun 15 02:00:42 CEST 2017	Mon Aug 23 03:33:17 CEST 2021 Wed Dec 15 01:00:42 CET 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=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Jun 28, 2021 14:56:21.788219929 CEST	108.177.15.154	443	192.168.2.4	49810	CN=*.g.doubleclick.net, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Mon May 31 03:33:18 CEST 2021 Thu Jun 15 02:00:42 CEST 2017	Mon Aug 23 03:33:17 CEST 2021 Wed Dec 15 01:00:42 CET 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=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Jun 28, 2021 14:56:21.804585934 CEST	172.217.16.130	443	192.168.2.4	49814	CN=*.g.doubleclick.net CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Mon May 31 03:33:26 CEST 2021 Thu Aug 13 02:00:42 CEST 2020 Fri Jun 19 02:00:42 CEST 2020	Mon Aug 23 03:33:25 CEST 2021 Thu Sep 30 02:00:42 CEST 2027 Fri Jan 28 01:00:42 CET 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1C3, O=Google Trust Services LLC, C=US	CN=GTS Root R1, O=Google Trust Services LLC, C=US	Thu Aug 13 02:00:42 CEST 2020	Thu Sep 30 02:00:42 CEST 2027		
					CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Fri Jun 19 02:00:42 CEST 2020	Fri Jan 28 01:00:42 CET 2028		
Jun 28, 2021 14:56:21.805742979 CEST	172.217.16.130	443	192.168.2.4	49813	CN=*.g.doubleclick.net CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Mon May 31 03:33:26 CEST 2021 Thu Aug 13 02:00:42 CEST 2020 Fri Jun 19 02:00:42 CEST 2020	Mon Aug 23 03:33:25 CEST 2021 Thu Sep 30 02:00:42 CEST 2027 Fri Jan 28 01:00:42 CET 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1C3, O=Google Trust Services LLC, C=US	CN=GTS Root R1, O=Google Trust Services LLC, C=US	Thu Aug 13 02:00:42 CEST 2020	Thu Sep 30 02:00:42 CEST 2027		
					CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Fri Jun 19 02:00:42 CEST 2020	Fri Jan 28 01:00:42 CET 2028		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jun 28, 2021 14:56:21.826792955 CEST	172.217.16.130	443	192.168.2.4	49815	CN=*.g.doubleclick.net CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Mon May 31 03:33:26 CEST 2021 Thu Aug 13 02:00:42 CEST 2020 Fri Jun 19 02:00:42 CEST 2020	Mon Aug 23 03:33:25 CEST 2021 Thu Sep 30 02:00:42 CEST 2027 Fri Jan 28 01:00:42 CET 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1C3, O=Google Trust Services LLC, C=US	CN=GTS Root R1, O=Google Trust Services LLC, C=US	Thu Aug 13 02:00:42 CEST 2020	Thu Sep 30 02:00:42 CEST 2027		
					CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Fri Jun 19 02:00:42 CEST 2020	Fri Jan 28 01:00:42 CET 2028		
Jun 28, 2021 14:56:21.910901070 CEST	151.101.0.84	443	192.168.2.4	49816	CN=*.pinterest.com, O="Pinterest, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Jul 16 02:00:00 CEST 2020 Tue Oct 22 14:00:00 CEST 2013	Wed Aug 04 14:00:00 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Jun 28, 2021 14:56:21.910968065 CEST	151.101.0.84	443	192.168.2.4	49818	CN=*.pinterest.com, O="Pinterest, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Jul 16 02:00:00 CEST 2020 Tue Oct 22 14:00:00 CEST 2013	Wed Aug 04 14:00:00 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Jun 28, 2021 14:56:21.916112900 CEST	151.101.0.84	443	192.168.2.4	49817	CN=*.pinterest.com, O="Pinterest, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Jul 16 02:00:00 CEST 2020 Tue Oct 22 14:00:00 CEST 2013	Wed Aug 04 14:00:00 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Jun 28, 2021 14:56:22.145602942 CEST	142.250.186.35	443	192.168.2.4	49826	CN=www.google.de CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Mon May 31 05:15:24 CEST 2021 Thu Aug 13 02:00:42 CEST 2020 Fri Jun 19 02:00:42 CEST 2020	Mon Aug 23 05:15:23 CEST 2021 Thu Sep 30 02:00:42 CEST 2027 Fri Jan 28 01:00:42 CET 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=GTS CA 1C3, O=Google Trust Services LLC, C=US	CN=GTS Root R1, O=Google Trust Services LLC, C=US	Thu Aug 13 02:00:42 CEST 2020	Thu Sep 30 02:00:42 CEST 2027		
					CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Fri Jun 19 02:00:42 CEST 2020	Fri Jan 28 01:00:42 CET 2028		
Jun 28, 2021 14:56:22.148559093 CEST	142.250.186.35	443	192.168.2.4	49825	CN=www.google.de CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Mon May 31 05:15:24 CEST 2021 Thu Aug 13 02:00:42 CEST 2020 Fri Jun 19 02:00:42 CEST 2020	Mon Aug 23 05:15:23 CEST 2021 Thu Sep 30 02:00:42 CEST 2027 Fri Jan 28 01:00:42 CET 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1C3, O=Google Trust Services LLC, C=US	CN=GTS Root R1, O=Google Trust Services LLC, C=US	Thu Aug 13 02:00:42 CEST 2020	Thu Sep 30 02:00:42 CEST 2027		
					CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Fri Jun 19 02:00:42 CEST 2020	Fri Jan 28 01:00:42 CET 2028		
Jun 28, 2021 14:56:22.148714066 CEST	142.250.186.35	443	192.168.2.4	49827	CN=www.google.de CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Mon May 31 05:15:24 CEST 2021 Thu Aug 13 02:00:42 CEST 2020 Fri Jun 19 02:00:42 CEST 2020	Mon Aug 23 05:15:23 CEST 2021 Thu Sep 30 02:00:42 CEST 2027 Fri Jan 28 01:00:42 CET 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1C3, O=Google Trust Services LLC, C=US	CN=GTS Root R1, O=Google Trust Services LLC, C=US	Thu Aug 13 02:00:42 CEST 2020	Thu Sep 30 02:00:42 CEST 2027		
					CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Fri Jun 19 02:00:42 CEST 2020	Fri Jan 28 01:00:42 CET 2028		
Jun 28, 2021 14:56:22.177256107 CEST	108.174.11.37	443	192.168.2.4	49811	CN=px.ads.linkedin.com, O=LinkedIn Corporation, L=Sunnyvale, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Apr 15 02:00:00 CEST 2021 Wed Sep 23 02:00:00 CEST 2020	Sat Oct 16 01:59:59 CEST 2021 Mon Sep 23 01:59:59 CEST 2030	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Sep 23 02:00:00 CEST 2020	Mon Sep 23 01:59:59 CEST 2030		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jun 28, 2021 14:56:22.187324047 CEST	108.174.11.37	443	192.168.2.4	49812	CN=px.ads.linkedin.com, O=LinkedIn Corporation, L=Sunnyvale, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Apr 15 02:00:00 CEST 2021 Wed Sep 23 02:00:00 CEST 2020	Sat Oct 16 01:59:59 CEST 2021 Mon Sep 23 01:59:59 CEST 2030	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Sep 23 02:00:00 CEST 2020	Mon Sep 23 01:59:59 CEST 2030		
Jun 28, 2021 14:56:24.635622978 CEST	157.240.17.35	443	192.168.2.4	49830	CN=*.facebook.com, O="Facebook, Inc.", L=Menlo Park, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed May 26 02:00:00 CEST 2021 Tue Oct 22 14:00:00 CEST 2013	Wed Aug 25 01:59:59 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Jun 28, 2021 14:56:24.637470961 CEST	157.240.17.35	443	192.168.2.4	49831	CN=*.facebook.com, O="Facebook, Inc.", L=Menlo Park, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed May 26 02:00:00 CEST 2021 Tue Oct 22 14:00:00 CEST 2013	Wed Aug 25 01:59:59 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Jun 28, 2021 14:57:19.757416010 CEST	34.96.106.200	443	192.168.2.4	49851	CN=*.parastorage.com CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, 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 CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Sun Feb 07 01:00:00 CET 2021 Thu Jan 01 01:00:00 CET 2004 Tue Mar 12 01:00:00 CET 2019 Fri Nov 02 01:00:00 CET 2018	Sat Aug 07 01:59:59 CEST 2021 Mon Jan 01 00:59:59 CET 2029 Mon Jan 01 00:59:59 CET 2029 Wed Jan 01 00:59:59 CET 2031	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=AAA Certificate Services, 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		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: 7064 Parent PID: 800

General

Start time:	14:55:35
Start date:	28/06/2021
Path:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE' /Automation -Embedding
Imagebase:	0x11b0000
File size:	1937688 bytes
MD5 hash:	0B9AB9B9C4DE429473D6450D4297A123
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Key Value Modified

Analysis Process: iexplore.exe PID: 984 Parent PID: 800

General

Start time:	14:56:05
Start date:	28/06/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding

Imagebase:	0x7ff64f3b0000
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 Show Windows behavior

Registry Activities Show Windows behavior

Analysis Process: iexplore.exe PID: 6880 Parent PID: 984

General

Start time:	14:56:06
Start date:	28/06/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:984 CREDAT:17410 /prefetch:2
Imagebase:	0x1260000
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 Show Windows behavior

Registry Activities Show Windows behavior

Disassembly

