ID: 441230
Sample Name: Corona als Dank.docx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 14:47:27
Date: 28/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

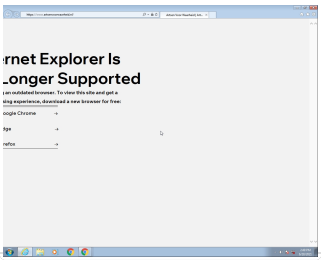
Windows Analysis Report Corona als Dank.docx

Overview

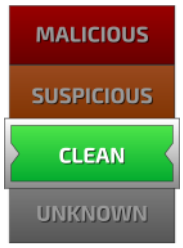
General Information

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

Most interesting Screenshot:



Detection

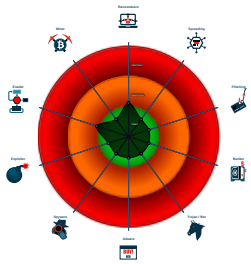


Score:	1
Range:	0 - 100
Whitelisted:	false
Confidence:	60%

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 w7x64**
- WINWORD.EXE (PID: 2480 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
- iexplore.exe (PID: 3044 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 4EB098135821348270F27157F7A84E65)
  - iexplore.exe (PID: 3032 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:3044 CREDAT:275457 /prefetch:2 MD5: 8A590F790A98F3D77399BE457E01386A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

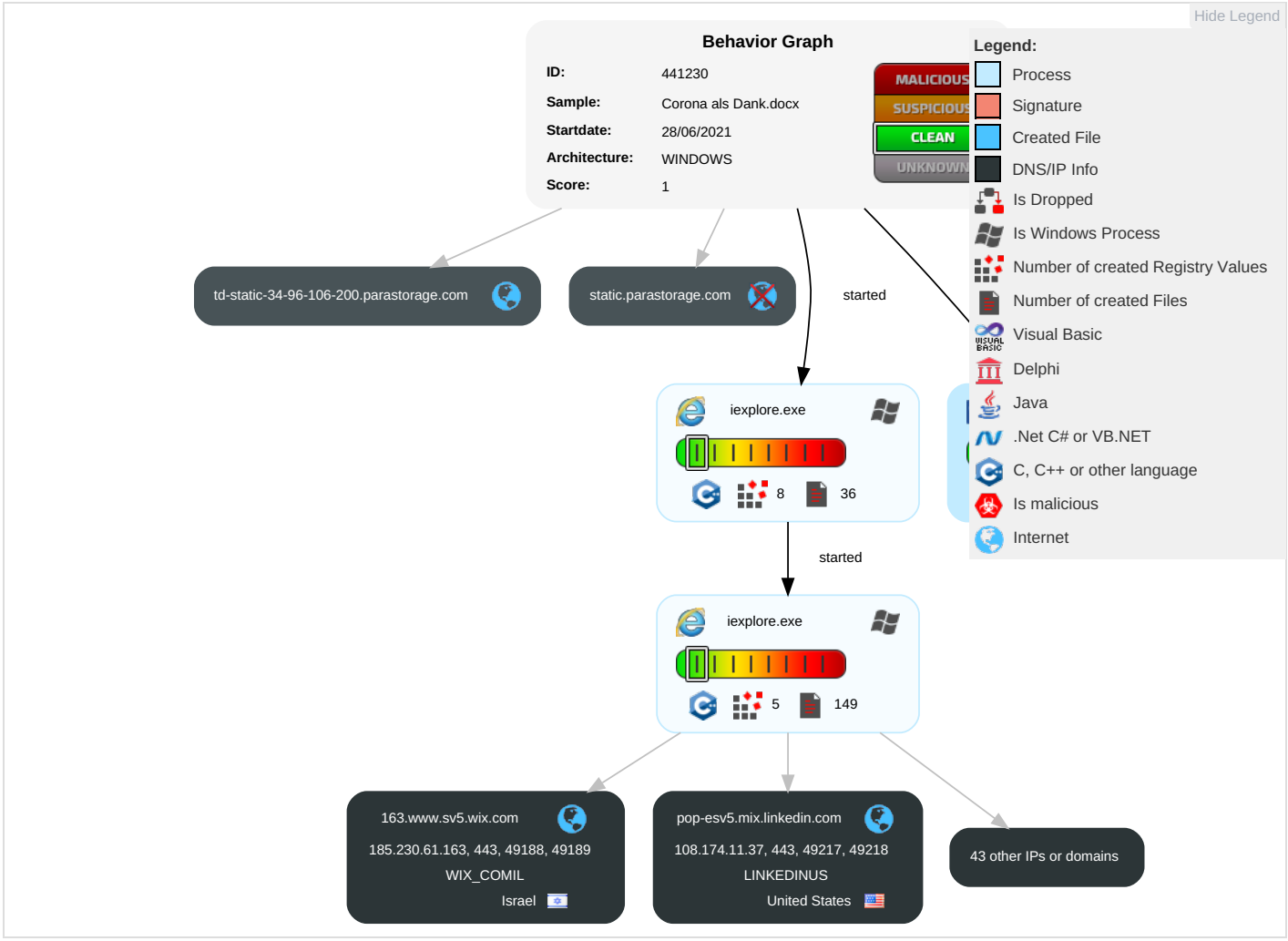
Click to jump to signature section

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 2	SIM Card Swap		Carri Billin Fraud

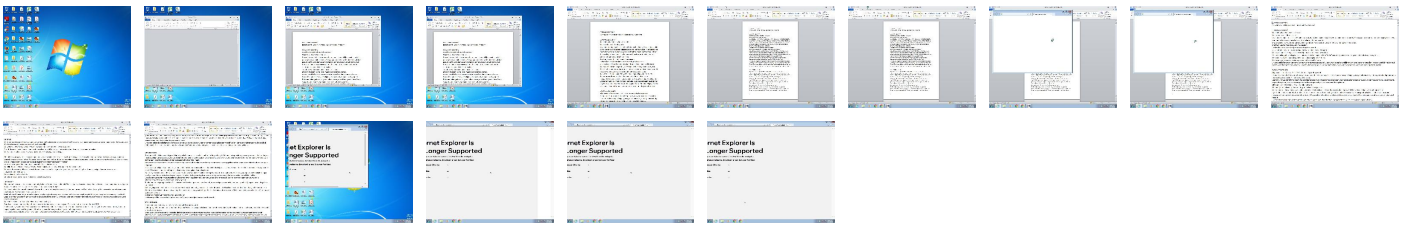
Behavior Graph

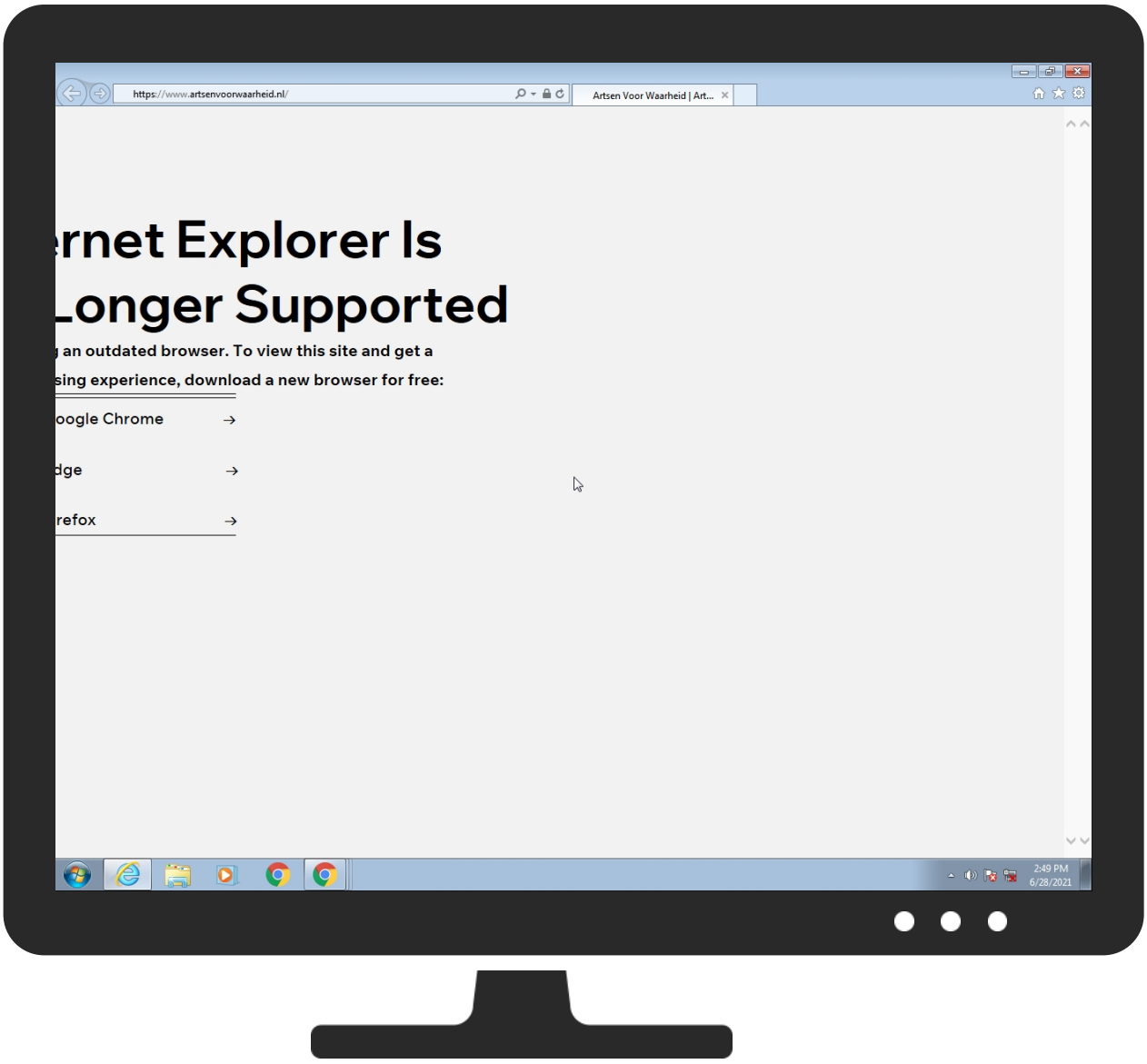


Screenshots

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://www.vrouwenvoorvrijheid.nl	0%	Avira URL Cloud	safe	
http://www.deguldenmiddenweg.nl	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://polymer.github.io/AUTHORS.txt	0%	Avira URL Cloud	safe	
http://www.vaccinvrij.nl	0%	Avira URL Cloud	safe	
http://https://www.artsenvoorwaarheid.nl	0%	Avira URL Cloud	safe	
http://www.artsenvoorwaarheid.nl	0%	Avira URL Cloud	safe	
http://www.moederhart.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://polymer.github.io/PATENTS.txt	0%	Avira URL Cloud	safe	
http://www.eenoorlogreesverloren.nl	0%	Avira URL Cloud	safe	
http://polymer.github.io/LICENSE.txt	0%	Avira URL Cloud	safe	
http://https://cct.google/taggy/agent.js	0%	URL Reputation	safe	
http://https://cct.google/taggy/agent.js	0%	URL Reputation	safe	
http://https://cct.google/taggy/agent.js	0%	URL Reputation	safe	
http://https://browser.sentry-cdn.com/5.21.4/bundle.min.js	0%	Avira URL Cloud	safe	
http://www.artsenvoorwaarheid.nl/	0%	Avira URL Cloud	safe	
http://https://www.google.%/ads/ga-audiences	0%	URL Reputation	safe	
http://https://www.google.%/ads/ga-audiences	0%	URL Reputation	safe	
http://https://www.google.%/ads/ga-audiences	0%	URL Reputation	safe	
http://https://www.artsenvoorwaarheid.nl/Root	0%	Avira URL Cloud	safe	
http://https://www.artsenvoorwaarheid.nl/informed-consent	0%	Avira URL Cloud	safe	
http://www.bluetiger.studio.nl	0%	Avira URL Cloud	safe	
http://https://recaptcha.net/recaptcha/api.js	0%	URL Reputation	safe	
http://https://recaptcha.net/recaptcha/api.js	0%	URL Reputation	safe	
http://https://recaptcha.net/recaptcha/api.js	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://www.deoorlogreedsverloren.nl	0%	Avira URL Cloud	safe	
http://www.devrijemare.nl	0%	Avira URL Cloud	safe	
http://polymer.github.io/CONTRIBUTORS.txt	0%	Avira URL Cloud	safe	
http://https://facebook.github.io/react/docs/top-level-api.html#react.createclass	0%	Avira URL Cloud	safe	
http://www.deblijeB.nl	0%	Avira URL Cloud	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
pagead46.l.doubleclick.net	142.250.185.194	true	false		high
browser.sentry-cdn.com	151.101.194.217	true	false	• 0%, Virustotal, Browse	unknown
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
fast.fonts.com	104.17.71.188	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
163.www.sv5.wix.com	185.230.61.163	true	false		high
googleads.g.doubleclick.net	216.58.212.162	true	false		high
sentry-nlb-e70282e8a06dcc98.elb.us-east-1.amazonaws.com	52.2.188.208	true	false		high
polyfill.io	151.101.129.26	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	34.231.78.0	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

Name	IP	Active	Malicious	Antivirus Detection	Reputation
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
adservice.google.de	unknown	unknown	false		high
en.wix.com	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

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.artsenvoorwaarheid.nl/	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.230.61.163	163.www.sv5.wix.com	Israel		58182	WIX_COMIL	false
34.96.106.200	td-static-34-96-106-200.parastorage.com	United States		15169	GOOGLEUS	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
151.101.194.217	browser.sentry-cdn.com	United States		54113	FASTLYUS	false
142.250.186.35	www.google.de	United States		15169	GOOGLEUS	false
104.17.71.188	fast.fonts.com	United States		13335	CLOUDFLARENETUS	false
142.250.185.198	dart.l.doubleclick.net	United States		15169	GOOGLEUS	false
34.231.78.0	bi-flogger-alb-ext-343643057.us-east-1.elb.amazonaws.com	United States		14618	AMAZON-AESUS	false
52.2.188.208	sentry-nlb-e70282e8a06dcc98.elb.us-east-1.amazonaws.com	United States		14618	AMAZON-AESUS	false
151.101.129.26	polyfill.io	United States		54113	FASTLYUS	false
142.250.185.194	pagead46.l.doubleclick.net	United States		15169	GOOGLEUS	false
34.102.176.152	gcp.media-router.wixstatic.com	United States		15169	GOOGLEUS	false
216.58.212.162	googleads.g.doubleclick.net	United States		15169	GOOGLEUS	false
108.174.11.37	pop-esv5.mix.linkedin.com	United States		14413	LINKEDINUS	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	441230
Start date:	28.06.2021
Start time:	14:47:27
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 28s

Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Corona als Dank.docx
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	6
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:	• EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean1.winDOCX@4/145@23/16
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
185.230.61.163	http://https://ademkeskin.wixsite.com/owa-projection-aspx	Get hash	malicious	Browse	
	http://https://portalstaffnew.wixsite.com/mysite	Get hash	malicious	Browse	
	http://nextstepdui.com/~canneo/Login-ppl.php	Get hash	malicious	Browse	
	http://https://mailservice66.wixsite.com/mysite	Get hash	malicious	Browse	
52.2.188.208	Sleek_Free.exe	Get hash	malicious	Browse	
	http://vcomdesign.com	Get hash	malicious	Browse	
	http://https://infozapyt.wixsite.com/mysite	Get hash	malicious	Browse	
	http://https://brechi5.wixsite.com/owa-webmail-updates	Get hash	malicious	Browse	
	MOI Support ship V2.docx	Get hash	malicious	Browse	
	MOI Support ship V2.docx	Get hash	malicious	Browse	
	MOI Support ship V2.docx	Get hash	malicious	Browse	
	MOI Support ship V2.docx	Get hash	malicious	Browse	
	MOI Support ship V2.docx	Get hash	malicious	Browse	
	http://https://outlookonedriveupd.wixsite.com/office	Get hash	malicious	Browse	
	http://https://ademkeskin.wixsite.com/owa-projection-aspx	Get hash	malicious	Browse	
	http://https://outlookmicrosoftwo.wixsite.com/upgrade	Get hash	malicious	Browse	
	http://https://www.shutdown-turnaround-industry-network.com/unsubscribe	Get hash	malicious	Browse	
	http://https://bee.co.za/	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://1drv.ms/u/s!Ag_TrhrEJITmdCoWx50Y40AGHGU?e=xMWw2h	Get hash	malicious	Browse	
	http://t.emk01.com/56cu_rd/mXNmaVrGdmJqZ2Vnll3IoWacbpOYY2-VjMh1aW9hnXJqXJVxZYqfbmNjZW2SaJeRZZlVk5RtapSglGhYnm6VX6BzY2pnmWlmV59xmtdd1aFmi6ifyKCilJeSm6GkV9J2bFyicZWsi2GUe4FqsbCe0ZjSe9e8ZYzYx7yGqJl4qmmZjWmpgLyHp5N6oJ--j6_UmayK17xlcNiy23Vv	Get hash	malicious	Browse	
151.101.194.217	http://catalog.amsz.ua/1.php	Get hash	malicious	Browse	
	http://vcomdesign.com	Get hash	malicious	Browse	
	http://https://brechi5.wixsite.com/owa-webmail-updates	Get hash	malicious	Browse	
	MOI Support ship V2.docx	Get hash	malicious	Browse	
	http://dlssm.free.fr	Get hash	malicious	Browse	
	http://https://owaonlineportalsfseyyq.yolasite.com/	Get hash	malicious	Browse	
	http://https://linkprotect.cudasvc.com/url?a=https%3a%2f%2fjoom.ag%2f9BjC&c=E,1,FEe77b6JikuybnZvWSPMtboj3kXPvfEd96gDBaPRghPkeeNMaiZ00lHXg2CVBvQXKcXw8950i4VfR2mq9wGKru5dQgG78LY4-xUIpbnM8tgzj5oG4pdo95PFgkNDQw,,&typo=1%3e	Get hash	malicious	Browse	
	http://https://joom.ag/iFjC	Get hash	malicious	Browse	
	http://https://www.shutdown-turnaround-industry-network.com/unsubscribe	Get hash	malicious	Browse	
	http://https://view.joomag.com/voice-message/0339362001599667702	Get hash	malicious	Browse	
	http://clicks.memberclicks-mail.net/ls/click?upn=arCqcQilrle0O-2BZra3ZluccVuScYzlA4t7hTwdxY0k07OIVAZxAaIFYnVwOwxM1L-2FLI-2BhJxCD1s9Skne42PmFePlHPK6DHGIFJAF0gDB1M7cOSTX47TaeD9eWDO4y-2BIy0tqA_3HGGU-2FUSr3MOBQ5zqyXP4bAUtuNdOnFewPwqCfcbcyqONV12LcALM8Y-2BL9bFHhZW-2BYdZqnLXzkYMj5ezZRZlOyPhgz6-2FF-2FcbKT4iTHz2bYS0esqNmqGDDaog9HdV1GBAmT8FzvuvfegHsqH0C-2BAkRGsNCFG-2F4nFPVinpoGMvWsngFXq9Eeq3HXQIRd61bEL7Cx8z8dleeosEV-2BmLnh5JPfln2YN-2BRQWhzBpcc4qWMRVQBunGFO8Gpa136bmN7A6tC8ryYzcb2nUi4-2B0RixdLDKOWGhrwiTWJIDYRXYmKoMxtPd1dP4hLg-2BI7x-2BjMLh0yARJR0zuOT-2Bi5GTAZGupCEw-3D-3D	Get hash	malicious	Browse	
	http://https://www.hover.com/control_panel/domain/midwestmotopunks.com/dns	Get hash	malicious	Browse	
	http://infograph.venngage.com/ps/yxUN0uhUFfU/outstanding-payment	Get hash	malicious	Browse	
	http://https://infograph.venngage.com/ps/RmQcdQLSgD4/payment	Get hash	malicious	Browse	
	http://https://www.secure-tix.com/	Get hash	malicious	Browse	
	http://https://linkprotect.cudasvc.com/url?a=https%3a%2f%2finfograph.venngage.com%2fpl%2f4suLHariKuA&c=E,1,6O5hBZA6Fp_B5PKUL1VTzW8ipjfNq3hQ2Z8cbNqB9IbXHP2jjKwPgrbi8w0t0NUzvsU-P-Ublxi8BXm0zm6KR9YtxlBJ4g7twy76qDB74Ak7Ru31&typo=1	Get hash	malicious	Browse	
	http://https://nenalandia-tv.blogspot.com/2012/09/alejandra-alloza-28092012.html?rndad=1476455992-1578670554	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
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
WIX_COMIL	xwKdahKPn8.exe	Get hash	malicious	Browse	• 185.230.63.107
	Swedbank.html	Get hash	malicious	Browse	• 185.230.60.98
	aVzUZCHkko.exe	Get hash	malicious	Browse	• 185.230.63.171
	Tz8eRwnGhm.exe	Get hash	malicious	Browse	• 185.230.63.171
	arm_crypt.exe	Get hash	malicious	Browse	• 185.230.63.171
	Sleek_Free.exe	Get hash	malicious	Browse	• 185.230.60.98
	cat.exe	Get hash	malicious	Browse	• 185.230.63.171
	$RAULIU9.exe	Get hash	malicious	Browse	• 185.230.63.171
	doc545567799890.exe	Get hash	malicious	Browse	• 185.230.60.161
	4GGwmv0AJm.exe	Get hash	malicious	Browse	• 185.230.63.171
	Bank Details.exe	Get hash	malicious	Browse	• 185.230.60.177
	S3d02jGrQo.exe	Get hash	malicious	Browse	• 185.230.60.161
	eQLPRPErea.exe	Get hash	malicious	Browse	• 185.230.60.177
	PO#41000055885.exe	Get hash	malicious	Browse	• 185.230.60.102
	211094.exe	Get hash	malicious	Browse	• 185.230.60.102
	UAE CONTRACT SUPPLY.exe	Get hash	malicious	Browse	• 185.230.60.102
	NEW ORDER - VOLVO HK HKPO2102-13561,pdf.exe	Get hash	malicious	Browse	• 185.230.60.177
	2S6VUd960E.exe	Get hash	malicious	Browse	• 185.230.60.102
	http://https://alijafari6.wixsite.com/owa-projection-aspx	Get hash	malicious	Browse	• 185.230.61.98
	http://https://xmailexpact.wixsite.com/mysite	Get hash	malicious	Browse	• 185.230.61.179
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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
7dcce5b76c8b17472d024758970a406b	PO20210628.xlsx	Get hash	malicious	Browse	• 142.250.186.35 • 185.230.61.163 • 34.96.106.200 • 104.17.71.188 • 142.250.185.198 • 157.240.17.35 • 34.231.78.0 • 157.240.17.15 • 52.2.188.208 • 35.246.6.109 • 151.101.194.217 • 151.101.129.26 • 142.250.185.194 • 34.102.176.152 • 216.58.212.162 • 108.174.11.37
	PO 33015.doc	Get hash	malicious	Browse	• 142.250.186.35 • 185.230.61.163 • 34.96.106.200 • 104.17.71.188 • 142.250.185.198 • 157.240.17.35 • 34.231.78.0 • 157.240.17.15 • 52.2.188.208 • 35.246.6.109 • 151.101.194.217 • 151.101.129.26 • 142.250.185.194 • 34.102.176.152 • 216.58.212.162 • 108.174.11.37

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SecuriteInfo.com.Exploit.Rtf.Obfuscated.16.18008.rtf	Get hash	malicious	Browse	• 142.250.186.35 • 185.230.61.163 • 34.96.106.200 • 104.17.71.188 • 142.250.185.198 • 157.240.17.35 • 34.231.78.0 • 157.240.17.15 • 52.2.188.208 • 35.246.6.109 • 151.101.194.217 • 151.101.129.26 • 142.250.185.194 • 34.102.176.152 • 216.58.212.162 • 108.174.11.37
	Wilson-McShane Corporation ACH.xlsx	Get hash	malicious	Browse	• 142.250.186.35 • 185.230.61.163 • 34.96.106.200 • 104.17.71.188 • 142.250.185.198 • 157.240.17.35 • 34.231.78.0 • 157.240.17.15 • 52.2.188.208 • 35.246.6.109 • 151.101.194.217 • 151.101.129.26 • 142.250.185.194 • 34.102.176.152 • 216.58.212.162 • 108.174.11.37
	PO20210624.doc	Get hash	malicious	Browse	• 142.250.186.35 • 185.230.61.163 • 34.96.106.200 • 104.17.71.188 • 142.250.185.198 • 157.240.17.35 • 34.231.78.0 • 157.240.17.15 • 52.2.188.208 • 35.246.6.109 • 151.101.194.217 • 151.101.129.26 • 142.250.185.194 • 34.102.176.152 • 216.58.212.162 • 108.174.11.37
	order-0798.doc	Get hash	malicious	Browse	• 142.250.186.35 • 185.230.61.163 • 34.96.106.200 • 104.17.71.188 • 142.250.185.198 • 157.240.17.35 • 34.231.78.0 • 157.240.17.15 • 52.2.188.208 • 35.246.6.109 • 151.101.194.217 • 151.101.129.26 • 142.250.185.194 • 34.102.176.152 • 216.58.212.162 • 108.174.11.37

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	dridexxx.xlsb	Get hash	malicious	Browse	• 142.250.186.35 • 185.230.61.163 • 34.96.106.200 • 104.17.71.188 • 142.250.185.198 • 157.240.17.35 • 34.231.78.0 • 157.240.17.15 • 52.2.188.208 • 35.246.6.109 • 151.101.194.217 • 151.101.129.26 • 142.250.185.194 • 34.102.176.152 • 216.58.212.162 • 108.174.11.37
	vessel arrival notice.docx	Get hash	malicious	Browse	• 142.250.186.35 • 185.230.61.163 • 34.96.106.200 • 104.17.71.188 • 142.250.185.198 • 157.240.17.35 • 34.231.78.0 • 157.240.17.15 • 52.2.188.208 • 35.246.6.109 • 151.101.194.217 • 151.101.129.26 • 142.250.185.194 • 34.102.176.152 • 216.58.212.162 • 108.174.11.37
	sf0X1hMF0g.doc	Get hash	malicious	Browse	• 142.250.186.35 • 185.230.61.163 • 34.96.106.200 • 104.17.71.188 • 142.250.185.198 • 157.240.17.35 • 34.231.78.0 • 157.240.17.15 • 52.2.188.208 • 35.246.6.109 • 151.101.194.217 • 151.101.129.26 • 142.250.185.194 • 34.102.176.152 • 216.58.212.162 • 108.174.11.37
	sf0X1hMF0g.doc	Get hash	malicious	Browse	• 142.250.186.35 • 185.230.61.163 • 34.96.106.200 • 104.17.71.188 • 142.250.185.198 • 157.240.17.35 • 34.231.78.0 • 157.240.17.15 • 52.2.188.208 • 35.246.6.109 • 151.101.194.217 • 151.101.129.26 • 142.250.185.194 • 34.102.176.152 • 216.58.212.162 • 108.174.11.37

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Wilson-McShane Corporation ACH.xlsx	Get hash	malicious	Browse	• 142.250.186.35 • 185.230.61.163 • 34.96.106.200 • 104.17.71.188 • 142.250.185.198 • 157.240.17.35 • 34.231.78.0 • 157.240.17.15 • 52.2.188.208 • 35.246.6.109 • 151.101.194.217 • 151.101.129.26 • 142.250.185.194 • 34.102.176.152 • 216.58.212.162 • 108.174.11.37
	Bulk Order-0798.doc	Get hash	malicious	Browse	• 142.250.186.35 • 185.230.61.163 • 34.96.106.200 • 104.17.71.188 • 142.250.185.198 • 157.240.17.35 • 34.231.78.0 • 157.240.17.15 • 52.2.188.208 • 35.246.6.109 • 151.101.194.217 • 151.101.129.26 • 142.250.185.194 • 34.102.176.152 • 216.58.212.162 • 108.174.11.37
	PO20210624.xlsx	Get hash	malicious	Browse	• 142.250.186.35 • 185.230.61.163 • 34.96.106.200 • 104.17.71.188 • 142.250.185.198 • 157.240.17.35 • 34.231.78.0 • 157.240.17.15 • 52.2.188.208 • 35.246.6.109 • 151.101.194.217 • 151.101.129.26 • 142.250.185.194 • 34.102.176.152 • 216.58.212.162 • 108.174.11.37
	Quote Requirment R2106131401 .docx	Get hash	malicious	Browse	• 142.250.186.35 • 185.230.61.163 • 34.96.106.200 • 104.17.71.188 • 142.250.185.198 • 157.240.17.35 • 34.231.78.0 • 157.240.17.15 • 52.2.188.208 • 35.246.6.109 • 151.101.194.217 • 151.101.129.26 • 142.250.185.194 • 34.102.176.152 • 216.58.212.162 • 108.174.11.37

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	h2GeNTLcFz.xls	Get hash	malicious	Browse	• 142.250.186.35 • 185.230.61.163 • 34.96.106.200 • 104.17.71.188 • 142.250.185.198 • 157.240.17.35 • 34.231.78.0 • 157.240.17.15 • 52.2.188.208 • 35.246.6.109 • 151.101.194.217 • 151.101.129.26 • 142.250.185.194 • 34.102.176.152 • 216.58.212.162 • 108.174.11.37
	Purchase Order.doc	Get hash	malicious	Browse	• 142.250.186.35 • 185.230.61.163 • 34.96.106.200 • 104.17.71.188 • 142.250.185.198 • 157.240.17.35 • 34.231.78.0 • 157.240.17.15 • 52.2.188.208 • 35.246.6.109 • 151.101.194.217 • 151.101.129.26 • 142.250.185.194 • 34.102.176.152 • 216.58.212.162 • 108.174.11.37
	SecuriteInfo.com.Exploit.Rtf.Obfuscated.16.20619.rtf	Get hash	malicious	Browse	• 142.250.186.35 • 185.230.61.163 • 34.96.106.200 • 104.17.71.188 • 142.250.185.198 • 157.240.17.35 • 34.231.78.0 • 157.240.17.15 • 52.2.188.208 • 35.246.6.109 • 151.101.194.217 • 151.101.129.26 • 142.250.185.194 • 34.102.176.152 • 216.58.212.162 • 108.174.11.37
	Coupon-Codes-2021.doc	Get hash	malicious	Browse	• 142.250.186.35 • 185.230.61.163 • 34.96.106.200 • 104.17.71.188 • 142.250.185.198 • 157.240.17.35 • 34.231.78.0 • 157.240.17.15 • 52.2.188.208 • 35.246.6.109 • 151.101.194.217 • 151.101.129.26 • 142.250.185.194 • 34.102.176.152 • 216.58.212.162 • 108.174.11.37

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Wire Info.docx	Get hash	malicious	Browse	• 142.250.186.35 • 185.230.61.163 • 34.96.106.200 • 104.17.71.188 • 142.250.185.198 • 157.240.17.35 • 34.231.78.0 • 157.240.17.15 • 52.2.188.208 • 35.246.6.109 • 151.101.194.217 • 151.101.129.26 • 142.250.185.194 • 34.102.176.152 • 216.58.212.162 • 108.174.11.37
	new list P.O34456.xlsx	Get hash	malicious	Browse	• 142.250.186.35 • 185.230.61.163 • 34.96.106.200 • 104.17.71.188 • 142.250.185.198 • 157.240.17.35 • 34.231.78.0 • 157.240.17.15 • 52.2.188.208 • 35.246.6.109 • 151.101.194.217 • 151.101.129.26 • 142.250.185.194 • 34.102.176.152 • 216.58.212.162 • 108.174.11.37

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Microsoft Cabinet archive data, 61020 bytes, 1 file
Category:	dropped
Size (bytes):	61020
Entropy (8bit):	**7.994886945086499**
Encrypted:	**true**
SSDEEP:	1536:IZ/FdeYPeFusuQszEfL0/NfXfdl5lNQbGxO4EBJE:0tdeYPiuWAVtlLBGm
MD5:	2902DE11E30DCC620B184E3BB0F0C1CB
SHA1:	5D11D14A2558801A2688DC2D6DFAD39AC294F222
SHA-256:	E6A7F1F8810E46A736E80EE5AC6187690F28F4D5D35D130D410E20084B2C1544
SHA-512:	EFD415CDE25B827AC2A7CA4D6486CE3A43CDCC1C31D3A94FD7944681AA3E83A4966625BF2E6770581C4B59D05E35FF9318D9ADADDADE9070F131076892AF2FA0
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	MSCF....\.....,.....I.....I.....R.q .authroot.stl.N....5..CK..8T....c_.d....A.K....=.D.eWI..r."Y...."i..,.=.I.D.....3...3WW.....y...9..w..D.yM10....`.0.e.._'..a0xN....)F.C..t .z.,.O20.1``L.....m?H..C..X>Oc..q.....%.!^v%<...O...-..@/.....H.J.W..... T...Fp..2.|$....._Y..Y`&..s.1.....s.{...,":o}9.....%._.xW*S.K..4"9.....q.G:.....a.H.y.. ..r...q./6.p.;.` =*.Dwj.....!.....s).B..y.....A.!W.....D!s0..!"X...I.....D0.....Ba...Z.0.o..I.3.v..W1F hSp.S)@.....'Z..QW...G...G.G.y+.x...aa`.3..X&4E..N...._O..<X.....K...xm..+M...O.H...)... .....*..o..~4.6.....p.`Bt.(..*V.N.!.p.C>..%.ySXY.>.`..f|.*...'^K`\..e.....j/..|..)..&i...wEj.w...o..r<.$.....C.....}.x...L..&..).r..\...>....v.....7...^..L!.$..'m...*,*.....7F$..~..S.6$S.-y....|.!.....x ...~k...Q/.w.e...h.[...9<x...Q.x.][}*_%Z..K.).3..'....M.6QkJ.N.....Y..Q.n.[.(.... ...Bg..33..[...S..[... .Z..<i.-.]...po.k.,...X6.....y3^.t[.Dw.]ts. R..L..`..ut_F....

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	326
Entropy (8bit):	3.1065641919610587

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Encrypted:	false
SSDEEP:	6:kKtEdoW+N+SkQlPlEGYRMY9z+4KlDA3RUellD1Ut:VU5kPlE99SNxAhUe0et
MD5:	A924971BF538FC7CF77BFD2230924E08
SHA1:	6A2290C099F00E8B5CD9AE78CE418BB1F4B40712
SHA-256:	B68F2603780F879F9353EDA23D9FD39D9E0CA4B07E256C669C25573F41F7D99B
SHA-512:	29D352C862060C4D35736130459F2BD442CE606C4825EDBD2D9CBE3350B10B2783F6F50D4F6B7B207DA3CF99D21C0ABF2F8DBD2F212824C09DDEB69FE62D51C
Malicious:	false
Reputation:	low
Preview:	p..... .....Hgl..(..... .....T'._.....$.....\...h.t.t.p.:.//.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.d.6.5.4.2.7.7.5.f.d.7.1.:.0."...

C:\Users\user\AppData\LocalLow\Microsoft\Internet Explorer\Services\search_{0633EE93-D776-472f-A0FF-E1416B8B2E3A}.ico	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 1 icon, 32x32, 32 bits/pixel
Category:	dropped
Size (bytes):	4286
Entropy (8bit):	3.8046022951415335
Encrypted:	false
SSDEEP:	24:suZOWcCXPRS4QAUs/KBy3TYI42Apvl6wheXpktCH2Yn4KgISQggggFpz1k9PAYHu:HBRh+sCBykteatiBn4KWi1+Ne
MD5:	DA597791BE3B6E732F0BC8B20E38EE62
SHA1:	1125C45D285C360542027D7554A5C442288974DE
SHA-256:	5B2C34B3C4E8DD898B664DBA6C3786E2FF9869EFF55D673AA48361F11325ED07
SHA-512:	D8DC8358727590A1ED74DC70356AEDC0499552C2DC0CD4F7A01853DD85CEB3AEAD5FBDC7C75D7DA36DB6AF2448CE5ABDFF64CEBDCA3533ECAD953C061A9338E
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	....(... ...@..... .....N...Sz..R...R...P...N..L..H..DG.....R6..U...U...S...R...P...N..L..I..F..B...7.....S6..V...V...U...S...R...P...N..L..I..F..C...?..:z.....O...W...V...V...U...S...R...P...N..L..I..E..C...?...:..{7..q2$.....T..D..]...S)..p6..J...R...P...N..L..I..E..B..>..;..z7..p2..f,X.....A..O#..N!..N!..N!..P$..q:...P...N..K..I..E..A..=..9..x5..n0..e,...5.....Ea.Z,..T$..T$..T

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\MP98E46N\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):	1514
Entropy (8bit):	5.063126811429066
Encrypted:	false
SSDEEP:	24:WU7xsvhumU7xsvhumU7xsvhumU7xsvhunwTJmU7xsvhunwTJCak/JmU7xsvhunwJ:LNl7Nl7Nl7Nli7NliChx7NliChxspV+k
MD5:	FFE1FF03BE9445755001FEDB8E338B8C
SHA1:	F575FF145531800C1537A35CB210BBED97A52955
SHA-256:	E0506F713DCDD3F892F65660C20BEAB6C46B32DB406F2ED882E23ED9554753CF
SHA-512:	56EF848CC7AC1DD7C7390D2828BD4AE78237E47DECA35E94EE8528220A7C9E902E335B1CB008D204021E52F0D7A47AC9C7C03DF830EB70CA9F3EABD26B5B42E
Malicious:	false
Reputation:	low
Preview:	<root></root><root><item name="fedops.logger.sessionId" value="289f9b54-c931-497e-9390-4aa5db3717fe" ltime="1248149728" htime="30895207" /></root><root><item name="fedops.logger.sessionId" value="289f9b54-c931-497e-9390-4aa5db3717fe" ltime="1248149728" htime="30895207" /></root><root><item name="fedops.logger.sessionId" value="289f9b54-c931-497e-9390-4aa5db3717fe" ltime="1248149728" htime="30895207" /></root><root><item name="fedops.logger.sessionId" value="289f9b54-c931-497e-9390-4aa5db3717fe" ltime="1248149728" htime="30895207" /><item name="_uetsid" value="8b924b80d85a11eb8925f1dffc1b282d" ltime="1297139728" htime="30895207" /></root><root><item name="fedops.logger.sessionId" value="289f9b54-c931-497e-9390-4aa5db3717fe" ltime="1248149728" htime="30895207" /><item name="_uetsid" value="8b924b80d85a11eb8925f1dffc1b282d" ltime="1297139728" htime="30895207" /><item name="_uetsid_exp" value="Tue, 29 Jun 2021 21:48:16 GMT" ltime="1297139728" htime="30895207" /></root><root><item name="fed

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{822F0857-D85A-11EB-ADCF-ECF4BBB5915B}.dat	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	33368
Entropy (8bit):	1.8711368407368811
Encrypted:	false
SSDEEP:	48:IvtuGcpUDjZGwp0Xr8G/apnXmrHGIpHXmABPGvnZpEXmA/SGoYtVqpqXmA/prGo/:MAK/TKKpyJ4a80AB33ouhOah9by3
MD5:	99407C7AD25C5EB96E03F5AA16CC730C
SHA1:	BD3B4D0DAC43F6C17F30705AF7240C79FD3E3999

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{822F0857-D85A-11EB-ADCF-ECF4BBB5915B}.dat	
SHA-256:	8BECF02A849C96627A86115B8CA8B521D31C0C57B78A7B75CA58CFCCE80C80EE
SHA-512:	654AD202EB13919CFDD848F8E0FE6EB9F89AF1B03248D110D63C9DAF844FFE97C122A1B112C031BFF33070968C21196389709B1F0DDF82C4315CBFC70BA51E2
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\{822F0859-D85A-11EB-ADCF-ECF4BBB5915B}.dat	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	24180
Entropy (8bit):	1.631700500022934
Encrypted:	false
SSDEEP:	48:IvjGcpUOZGwpNSG4pPSGrapgSFGQpCWGHHpnrTGUpHbGzYp11VGopB3JLPUAGWXg:MZKOTbiJUeSvcVpFJhzF3Vdg
MD5:	B5D5451040A493256D8F5D315983DCEE
SHA1:	BB81843C7E21D61CE5256A2F9872A63C647B44CB
SHA-256:	3702A140993696CE73BFE7ADED7F30E319E7ED0D4F848597B5DA7A7419E0EFF8
SHA-512:	995BA0FBBF09450C26A0117D9EB6D1048A8C1D8FB92538B641A7DCE675DAC0598479C2A8E3CB1EE425D032F18350D6BF90FF85D8F7D004F73A167BC6A430C08
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\{9928C6D3-D85A-11EB-ADCF-ECF4BBB5915B}.dat	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5640117402231462
Encrypted:	false
SSDEEP:	48:IvxGcpUDZGwpNQG4pP4GrapgSIGQpZqG7HpCdTGIpG:MHKDTbQJGeSw/F0bA
MD5:	A19C5B7BFDC5254423E0C131738D48A7
SHA1:	112F8963B47D560FB9B372E93DAFA61C838450D6
SHA-256:	8CE476361B240C7BAF3E4A3DBE6BA65E0C8753B985195372A150E7F794AF3E77
SHA-512:	DF14A85ABD647ED3257F2B4F6E301BE73AEB890E35B84D8B3A042FE300E1CC83BB1A42AC58239F4B34BA534F2DB0C0BBA760FB6A05454710DB0039B2B635A402
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\lr5drzg\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:tYmRMhZTMic8ReJq55555555555555pllNm+4:amEtg8ReJq55555555555555ple
MD5:	2A3DEDBED1F7425CFC1062B3A017FD73
SHA1:	D6771AD13E9D1D5137C1ECCA4627CA868B1A515C
SHA-256:	3FA7DBA70AD80939A2F9E185A925BB3AD8CCD59008B1CF341EB4BF5FD15880E0
SHA-512:	EDB5A31FC3FF1B60C2EA458481E9EDBFB73069AC27B0BF53B7EDD26D13C4A8E49847A69193A46DD6D20ED60C85135262F84DA811435249EAACC6A7AC667D58A
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\lr5drzg\imagestore.dat	
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\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\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
Reputation:	moderate, very likely benign file
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 1.816.1522.705.032.295.091.581.133.873.085.589.173 1.176.298 1.751.073.338.169.665.256.997.135.515.273 1.027.439 1.529.114.342.243.675.37 1.01.18.476.369.945.5771.406.149.331.308.657.472.98.225.446.463.883.714 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\Temporary Internet Files\Content.IE5\5JC0A1KN\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
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("lodash"),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\Temporary Internet Files\Content.IE5\5JC0A1KN\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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\bolt-custom-elements.min[1].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\Temporary Internet Files\Content.IE5\5JC0A1KN\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+l65nFuM9:DTFHN6vPX+7DOegpSnoVT7FDW6bM9
MD5:	7F8F0363808B72AE76DE192F51689D33
SHA1:	212EEE29A63222FD2B558CC5F432347EE31407D8
SHA-256:	CE88CFE2A86DD05C6ED0B3A876C0FD93C3B5CCCAE146D2FB9CF0BA2E2EC729F6
SHA-512:	4846DB41108A0BE652B183C0081746FC0180AC7233B9977254270B3C0073EB09200ABC62A6F8BCD5ADAF3D1F5B56FA746FE495E63316113D486DF22E60E9C697
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"&&requi re;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 con vert=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\Temporary Internet Files\Content.IE5\5JC0A1KN\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){i f(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.cre ate(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=f unction(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\Temporary Internet Files\Content.IE5\5JC0A1KN\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:	5DF21A378372ABDC425FA2E62FACA0DCF02F664C08C1B7F2D894836E7ADE6E4723289C95FC9A610CE896523366B6F6DA339ED259038508150472426 1DC8C015
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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\components.min[1].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\Temporary Internet Files\Content.IE5\5JC0A1KN\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
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\Temporary Internet Files\Content.IE5\5JC0A1KN\dataRefs.bundle[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	5342
Entropy (8bit):	5.085458326375951
Encrypted:	false
SSDEEP:	96:UpMvR8dtyEvEWlEmcfXGunhXWiIrKBK9vhK8:SkefyEvEW6mcfXGunhXPIrvdhK8
MD5:	F9566BB58AE69CE40A18EF585AECB63C
SHA1:	4B369BE919F55D3C594749D16741BFA1C148A3B4
SHA-256:	6B3B422CFAE9850BD0D8CF21582A5A7FE5A5419D219183841DE3732B4810F167
SHA-512:	EF3562E0CB7E97C34688849C05E0367DED5FCC9B3F261DB795792A0FBA04E85D1F80D42DAA78BFD0EA13FB7F6525BFF4E0F1BBBA4AD6596CF9F69414D9169F0
Malicious:	false
IE Cache URL:	http://https://static.parastorage.com/unpkg/@wix/wix-ui-santa@2.0.294/dist/statics/dataRefs.bundle.js
Preview:	(function webpackUniversalModuleDefinition(root, factory) {..if(typeof exports === 'object' && typeof module === 'object')...module.exports = factory();..else if(typeof define === 'function' && define.amd)...define([], factory);..else if(typeof exports === 'object')...exports["dataRefs"] = factory();..else...root["dataRefs"] = factory();..})((typeof self !== 'undefined' ? self : this), function() {.return /******/ (function(modules) { // webpackBootstrap./******/ .// The module cache./******/ .var installedModules = {};./******/./******/ .// The require function./******/ .function __webpack_require__(moduleId) {./******/./******/ ..// Check if module is in cache./******/ ..if(installedModules[moduleId]) {./******/ ...return installedModules[moduleId].exports;./******/ ..}./******/ ..// Create a new module (and put it into the cache)./******/ ..var module = installedModules[moduleId] = {./******/ ..i: moduleId,./******/ ...l: false,./******/ ...exports: {}./******/ ..};./******/./******

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\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):	2035
Entropy (8bit):	5.852822592055182
Encrypted:	false
SSDEEP:	48:0VUUIqzPrqTnJcgVhkGYPZEJWjDVggyWOYxp7Fv7RZtpETSqxP:+UURWTCgVhkdZEJWHfDXlbchxP
MD5:	B6040C8B4CC68C2280D4A03433512ABD
SHA1:	CE1310D66C871889CAEE1D9721DCF8E03721CAD3
SHA-256:	F6D40D28DC5AD8998DB2FF238DBE3D5E5F4EBA1868985D80131AC3A98DCF7F3A
SHA-512:	21CDFE707DC975C017976703352888846F3BDF395E138AF727712025DB0D90FF61AE2BC752DB91CC1FA21E2F568962D457B2BC4437BB93815A2883886D774EBD
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\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.e xecScript||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\Temporary Internet Files\Content.IE5\5JC0A1KN\favicon[1].ico	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 1 icon, 32x32, 32 bits/pixel
Category:	downloaded
Size (bytes):	4286
Entropy (8bit):	3.8046022951415335
Encrypted:	false
SSDEEP:	24:suZOWcCXPRS4QAUs/KBy3TYl42Apvl6wheXpktCH2Yn4KgISQggggFpz1k9PAYHu:HBRh+sCBykteatiBn4KWi1+Ne
MD5:	DA597791BE3B6E732F0BC8B20E38EE62
SHA1:	1125C45D285C360542027D7554A5C442288974DE
SHA-256:	5B2C34B3C4E8DD898B664DBA6C3786E2FF9869EFF55D673AA48361F11325ED07
SHA-512:	D8DC8358727590A1ED74DC70356AEDC0499552C2DC0CD4F7A01853DD85CEB3AEAD5FBDC7C75D7DA36DB6AF2448CE5ABDFF64CEBDCA3533ECAD953C061A9 338E
Malicious:	false
IE Cache URL:	http://www.bing.com/favicon.ico
Preview:	....(... ...@..... .....N...Sz..R...R...P. ..N..L..H..DG.....R6..U...U...S...R...P...N..L..I..F..B...7.....S6..V...V...U...S ...R...P...N..L..I..F..C...?..:z.....O...W...V...V...U...S...R...P...N..L..I..E..C...?...;..{7..q2$.....T..D ..]...S)..p6..J...R...P...N..L..I..E..B..>..;..z7..p2..f,X.....A..O#..N!..N!..N!..P$..q:...P...N..K..I..E..A..=..9..x5..n0..e,...5..... .....Ea.Z,..T$..T$..T

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\fetch.umd[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	14805
Entropy (8bit):	4.758498348901479
Encrypted:	false
SSDEEP:	384:2c9oamnRGWqkphLV53G8FsDujopncgkrDTho7RR9c:2iunRGWqkpRTwE8cNrxo7RR9c
MD5:	456C02EE2A496580A24E5AEE614BA9B3
SHA1:	508EF9378B49D348BC88C92E02F459724971EA5F
SHA-256:	9A0C4301B6E804A7A808EB69694ED08567605811AE9BEF1D3F19C88E20BDEC92
SHA-512:	58D5718D7C7A018A206339C9529085C6A714188FAF548B8CBD7DA2FED997DE898F580DAB1DEA138189186021404AE5510CAD57D3F052A2D20ABDBC2505A16AE
Malicious:	false
IE Cache URL:	http://https://static.parastorage.com/unpkg/whatwg-fetch@3.0.0/dist/fetch.umd.js
Preview:	(function (global, factory) {. typeof exports === 'object' && typeof module !== 'undefined' ? factory(exports) :. typeof define === 'function' && define.amd ? define([' exports'], factory) :. (factory((global.WHATWGFetch = {}));.}(this, (function (exports) { 'use strict';.. var support = {. searchParams: 'URLSearchParams' in self,. iterab le: 'Symbol' in self && 'iterator' in Symbol,. blob:. 'FileReader' in self &&. 'Blob' in self &&. (function() {. try {. new Blob();. return true. } ca tch (e) {. return false. }. })(),. formData: 'FormData' in self,. arrayBuffer: 'ArrayBuffer' in self. };.. function isDataView(obj) {. return obj && DataView. prototype.isPrototypeOf(obj). }.. if (support.arrayBuffer) {. var viewClasses = [. '[object Int8Array]',. '[object Uint8Array]',. '[object Uint8ClampedArray]',. '[object Int16Array]',. '[object Uint16Array]',. '[object Int32A

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\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:	641C0EACB9829FC34D4CC678E33BA96B156E54EE67F5D90C0238B9B241E8AFC24F7C1A0817CFFB27F8E805F33BBD9BD15E2B5243925A6B803B2612840D22E63 F
Malicious:	false
IE Cache URL:	http://https://static.parastorage.com/services/santa-resources/resources/viewer/user-site-fonts/v7/helvetica.css

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\helvetica[1].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\Temporary Internet Files\Content.IE5\5JC0A1KN\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\Temporary Internet Files\Content.IE5\5JC0A1KN\internet-explorer[1].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):	338701
Entropy (8bit):	5.6011623554271885
Encrypted:	false
SSDEEP:	3072:5V4aptfrDwWctPwvcnT1y4+lemuRmdHMIU:DptfrDwW8PwERy4+lemuRmdHM
MD5:	2909FF085BFA6DF335D90A6B800B4754
SHA1:	34082C0ADB144A674A899876C1A3F6299F3D3A3C
SHA-256:	DFA6F160548A2B080CB97C4F8407273C334F708EBA7BD4BAF38060EF5F6E535A
SHA-512:	59D82213E3D87E82B2D1B954176CEBD90E57BB5AB70C1DA0B0DBC1D0873AD3BE29E840F14CBD3378F69A76D53DA5CEEB3B7C212A952605394E201EDF396BE14
Malicious:	false
IE Cache URL:	http://https://www.wix.com/outdated-browser/internet-explorer?forceBolt=&ssrIndicator=false&suppressbi=true
Preview:	<!DOCTYPE html>.<html lang="en">.<head>. <meta http-equiv="X-UA-Compatible" content="IE=Edge"/>. . <meta charset="utf-8"/>. <meta name="generator" content="Wix.com Website Builder"/>. <link rel="shortcut icon" href="https://www.wix.com/favicon.ico" type="image/x-icon"/>. <link rel="apple-touch-icon" href="https://www.wix.com/favicon.ico" type="image/x-icon"/>. . . . . <meta http-equiv="X-Wix-Meta-Site-Id" content="7495ef56-6f96-4160-bf8f-3e452f199a48"/>. <meta http-equiv="X-Wix-Application-Instance-Id" content="8ec0be37-3817-4e57-bb3d-85e551922dc7"/>. . . <meta http-equiv="X-Wix-Published-Version" content="23"/>. . . . . <meta name = "format-detection" content = "telephone=no"/>.. <meta name="SKYPE_TOOLBAR" content="SKYPE_TOOLBAR_PARSER_COMPATIBLE"/>.. . <meta id="wixMobileViewport" name="viewport" content="width=980, user-scalable=yes"/>. .. . . META DATA -->. <script typ

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\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:	5F99DCCAA3864E5AD54EB6BDCB83D65F4B0A65A72BC8BA28DC1D8E058ED50B0639AE9203B3712346CF04BEB8CDBAC3D611A609ED703559CA94E1856CED0AE9C4
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\Temporary Internet Files\Content.IE5\5JC0A1KN\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\Temporary Internet Files\Content.IE5\5JC0A1KN\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):	73015
Entropy (8bit):	5.342744191670081
Encrypted:	false
SSDEEP:	1536:X9ylPegosd1p8X4Kx2iiC0guaihfaZgb9pL/:X9cVaizgehfaZCX/
MD5:	9BECC40FB1D85D21D0CA38E2F7069511
SHA1:	AE854B04025DB8B7F48FDD6DEDF41E77EAE44394
SHA-256:	A9705DFC47C0763380D851AB1801BE6F76019F6B67E40E9B873F8B4A0603F7A9
SHA-512:	585374E3CE3AB1D28C20FE4B28DA6131A5B353B629332094DB8E5EB4ADE0FF601161B3CAF546F5F1E1BE96353DEAA29109687EAAE098EF279F4A6964430D403
Malicious:	false
IE Cache URL:	http://https://static.parastorage.com/unpkg/lodash@4.17.21/lodash.min.js
Preview:	/**. * @license. * Lodash <https://lodash.com/>. * Copyright OpenJS Foundation and other contributors <https://openjsf.org/>. * Released under MIT license <https://lodash.com/license>. * Based on Underscore.js 1.8.3 <http://underscorejs.org/LICENSE>. * Copyright Jeremy Ashkenas, DocumentCloud and Investigative Reporters & Editors. */.(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&&t(n[r],r,n)!==!1;);return n}function e(n,t){for(var r=null==n?0:n.length;r--&&t(n[r],r,n)!==!1;);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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\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+H9XvaLNr1ttlkLj7IlHhBPAdk: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\Temporary Internet Files\Content.IE5\5JC0A1KN\main.c6ca189a[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	50784
Entropy (8bit):	5.562079214321805
Encrypted:	false
SSDEEP:	768:HB5fb43pdsRj8rCs62oiO+opB51Q1AnhAIhVulw4RzirrAoKiWQ4nEHxrp1j4tzy:gsRjX2o3+gV34ti5JWb0xrpKs
MD5:	FC68B47C0F233BB6631EE8E94771528F
SHA1:	3DB3643B63E57E026D2D89B285FB669E7CDAF194
SHA-256:	6E68C7F596671913CDE21EA0A5C4367B743A79422D87B0659E22F00673C5AEB8
SHA-512:	17204B3E5EBEE24C004BF0DD3634C5571AF1744C176F421978C1F56013D43CDD321A4A2AE7E5F5ABF260C8F16106CA4892A1937C0C7B4D5F37A51152C070096
Malicious:	false
IE Cache URL:	http://https://s.pinimg.com/ct/lib/main.c6ca189a.js

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\main.c6ca189a[1].js	
Preview:	!function(r){var i={};function e(t){if(i[t])return i[t].exports;var n=i[t]={i:t,l:!1,exports:{}};return r[t].call(n.exports,n,n.exports,e),n.l=!0,n.exports}e.m=r,e.c=i,e.d=function(t,n,r){e.o(t,n)||Object.defineProperty(t,n,{enumerable:!0,get:r})},e.r=function(t){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(t,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(t,"u",{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.u)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 i in n)e.d(r,i,function(t){return n[t]}.bind(null,i));return r},e.n=function(t){var n=t&&t.u?function(){return t.default}:function(){return t};return e.d(n,"a",n),n},e.o=function(t,n){return Object.prototype.hasOwnProperty.call(t,n)},e.p="",e(e.s=5)}([function(t,P,n){"use strict";(function(t){var i=n(15),o=n(16),u=n(17);function r(){return c.TYPED_ARRAY_SUPPORT?214

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\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;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\Temporary Internet Files\Content.IE5\5JC0A1KN\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
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?invariant="+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\Temporary Internet Files\Content.IE5\5JC0A1KN\requirejs.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):	17493
Entropy (8bit):	5.208224058486374
Encrypted:	false
SSDEEP:	384:ayznN5k6MTQmeYl8oSdNdSoUYdHvEDezCnGgqo6N6TBIueHtf:hI6MTQxYl8oSdNdS/QHvED9StETBKHtf
MD5:	18823F6A6D208EE1E361BB266AB794D5
SHA1:	E9FA356AC13BD24C051804A6E4EC3E053BC8001C
SHA-256:	D5F10F852B112A514A19F2B778EEF5D2D1307878757F0A24539C051831CEFAF8
SHA-512:	737365F3EEE0E0B3124DDAE6EB6D72EE47FDBF74833E78712CD85C8C525B2840959E66474DDA3E2113B4E6C34B4C7FC3DEF03ABB55F7D9E8682C2ED6155761A
Malicious:	false
IE Cache URL:	http://https://static.parastorage.com/unpkg/requirejs-bolt@2.3.6/requirejs.min.js

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\requirejs.min[1].js	
Preview:	var requirejs,require,define;!function(global,setTimeout){var req,s,head,baseElement,dataMain,src,interactiveScript,currentlyAddingScript,mainScript,subPath,version="2.3.6",commentRegExp=/\/*[\s\S]*?*\/|([^:'"=]|^)\/\/.*$/gm,cjsRequireRegExp=/[^.]\s*require\s*\(\s*["']([^'"\s]+)["']\s*\)/g,jsSuffixRegExp=/\.js$/,currDirRegExp=/^\.\//,op=Object.prototype,ostring=op.toString,hasOwn=op.hasOwnProperty,isBrowser=!("undefined"==typeof window||"undefined"==typeof navigator||!window.document),isWebWorker=!isBrowser&&"undefined"!=typeof importScripts,readyRegExp=isBrowser&&"PLAYSTATION 3"===navigator.platform?/^complete$/:/^(complete|loaded)$/,defContextName="_",isOpera="undefined"!=typeof opera&&"[object Opera]"===opera.toString(),contexts={},cfg={},globalDefQueue=[],useInteractive=!1;function commentReplace(e,t){return t||""}function isFunction(e){return"[object Function]"===ostring.call(e)}function isArray(e){return"[object Array]"===ostring.call(e)}function each(e,t){var i;if(e)for(i=0;i<

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\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=1624916899433&sw=1280&sh=1024&v=2.9.42&r=stable&ec=0&o=14&it=1624916899179&coo=false&rqm=GET
Preview:	GIF89a.....!.....,.....D..;.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\warmupUtils.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	174067
Entropy (8bit):	5.258727931343642
Encrypted:	false
SSDEEP:	3072:HpDEWGvVWX/srVL8NLt7CYIz9/2nHj7H5iuUOjWw:HpDEWGvVcqet7FIZ2DdbUc
MD5:	1A5877338994D930F3A420B91DE9FE58
SHA1:	C0C7E4F7DDC46F78117C8499D1653DD729364F95
SHA-256:	F1AA81CE2B1B682CD90663DA8326B775569B78C2A12836BE751ED6360698FFCE
SHA-512:	2B0422713FB79774813CC51E8D7242B49A56C09A830502ED043B701607C787BA2565BEBBB10863AA44609CC33A199289BAC38734B60EBA31950B603B62F01855
Malicious:	false
IE Cache URL:	http://https://static.parastorage.com/services/wix-bolt/1.7264.0/node_modules/wix-santa/dist/packages-bin/warmupUtils/warmupUtils.min.js
Preview:	define("warmupUtils",["lodash","zepto","experiment","warmupUtilsLib","image-client-api","wix-ui-santa/dataRefs.bundle.min"],(function(e,t,n,i,r,a){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}:function(){return e};return n.d(t,"a",t),t},n.o=function(e

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\warmupUtils[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):	129615
Entropy (8bit):	5.515337896421485
Encrypted:	false
SSDEEP:	1536:mHGDXtC7bdzxIv9ypDF09wtvhKFdcaB7ads39HhdT:GGD+bdzxIvuD8wtJKrcaB7adS9HhdT
MD5:	AFC6490902D6657926F4A87927EE82FE
SHA1:	DD9C648CB400CDAD9CA8B47FA6F0FAC359D8F6A6
SHA-256:	9751D4502766815EE357F5E4712E77B9DCB8E07E0E707F9C1AA48E5D5D0E6515
SHA-512:	5DD4A8FFFF0FEFFC63784D1BF6B18E50BEDFAC0CBC64C3DE0E9C2FF6839044D0A4BF3537E806E3F8F865843DBB3F2CCAF3B6BDD1C5316BF77C6E8BEEE643563D
Malicious:	false
IE Cache URL:	http://https://static.parastorage.com/unpkg/@wix/santa-core-utils@1.2706.0/dist/warmupUtils.js

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\warmupUtils[1].js	
Preview:	!function(e,t){"object"==typeof exports&&"object"==typeof module?module.exports=t(require("lodash"),require("zepto"),require("image-client-api")):"function"==typeof define&&define.amd?define(["lodash","zepto","image-client-api"],t):"object"==typeof exports?exports.warmupUtils=t(require("lodash"),require("zepto"),require("image-client-api")):e.warmupUtils=t(e.lodash,e.zepto,e["image-client-api"])}(this,(function(e,t,a){return function(e){var t={};function a(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,a),r.l=!0,r.exports}return a.m=e,a.c=t,a.d=function(e,t,i){a.o(e,t)||Object.defineProperty(e,t,{enumerable:!0,get:i})},a.r=function(e){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(e,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(e,"__esModule",{value:!0})},a.t=function(e,t){if(1&t&&(e=a(e)),8&t)return e;if(4&t&&"object"==typeof e&&e&&e.__esModule)return e;var i=Object.create(null);if(a.r(i),Objec

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\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\Temporary Internet Files\Content.IE5\5JC0A1KN\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\Temporary Internet Files\Content.IE5\5JC0A1KN\wixui.StylableButton.chunk[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\wixui.StylableButton.chunk[1].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\Temporary Internet Files\Content.IE5\5JC0A1KN\zepto.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	26386
Entropy (8bit):	5.176792166274628
Encrypted:	false
SSDEEP:	384:He+VbNwN6J4wfYRWzmEABSF0ztlbtj4jXh2FYx:HbNwvRWh2xlBjCx2e
MD5:	50A4556B0089CFA1CB61E88EA23BBCCE
SHA1:	6865443A258954FA19B8AA682E1F4C77D42493D1
SHA-256:	BEB9F5E32ED61FBCE010497242A9B6B8219242B5FFC636038E7891510C773725
SHA-512:	06BBD560D84A87AC924F6E04E4363F2E8A4B3B977EF0A626217CABA41209D8F2BE0B2C89C3F70B486FC17C9A2658B0B521B94DAE688958696B1AE78A2DDFC4 3
Malicious:	false
IE Cache URL:	http://https://static.parastorage.com/unpkg/zepto@1.2.0/dist/zepto.min.js
Preview:	/* Zepto v1.2.0 - zepto event ajax form ie - zeptojs.com/license */.!function(t,e){"function"==typeof define&&define.amd?define(function(){return e(t)}):e(t)}(this,function(t) {var e=function(){function $(t){return null==t?String(t):S[C.call(t)]\|\|"object"}function F(t){return"function"==$(t)}function k(t){return null!=t&&t==t.window}function M(t){return null!=t&&t.nodeType==t.DOCUMENT_NODE}function R(t){return"object"==$(t)}function Z(t){return R(t)&&!k(t)&&Object.getPrototypeOf(t)==Object.prototype}function z(t) {var e=!!t&&"length"in t&&t.length,n=r.type(t);return"function"!=n&&!k(t)&&("array"==n||0===e||"number"==typeof e&&e>0&&e-1 in t)}function q(t){return a.call(t,function(t){r eturn null!=t})}function H(t){return t.length>0?r.fn.concat.apply([],t):t}function I(t){return t.replace(/::/g,"/").replace(/([A-Z]+)([A-Z][a-z])/g,"$1_$2").replace(/([a-z\d])([A-Z])/g,"$1_$2").replace(/_/g,"-").toLowerCase()}function V(t){return t in l?l[t]:l[t]=new RegExp("(^\|\\s)"+t+"(\\s\|$)")}function _(t

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\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:	BF9211CB4EB1D8EE2C5DA099044D2911A647958D5DC4215B651C84D721919B5B9427767704651145345F5231FE5D918F9FEA1DD955CBCE9F53024FCD3B9D535
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..;|....*.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\Temporary Internet Files\Content.IE5\T4O403JZ\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\Temporary Internet Files\Content.IE5\T4O403JZ\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**
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\Temporary Internet Files\Content.IE5\T4O403JZ\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\Temporary Internet Files\Content.IE5\T4O403JZ\642100862[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\Temporary Internet Files\Content.IE5\T4O403JZ\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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\67da9da8-4b53-4407-9184-abce69bfc8b5[1].woff	
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\Temporary Internet Files\Content.IE5\T4O403JZ\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\Temporary Internet Files\Content.IE5\T4O403JZ\9362bca5-b362-4543-a051-2129e2def911[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 22131, version 1.0
Category:	downloaded
Size (bytes):	22131
Entropy (8bit):	7.980068465474638
Encrypted:	false
SSDEEP:	384:q54PVqnInDbWa1qhWI5m/fCatLxU/eBzqWOMKjCT2D2h7NKyVaEPzJJNmh:qbInDP1qhfm/f3UWOWOMG2dVzVmh
MD5:	C79267643FBCE46F7FE3B1A1A390B5E5
SHA1:	946A77EA7F1DFD9990A448087A93367D311C618D
SHA-256:	734C66A2EBF94202AB98FA4F2AE3874FA5582E5579114D2567FBD85012916365
SHA-512:	DF034623BB76454EC1B3C740662AE59957A10B83CD6CCE660063FF646A2AF86197D5ED7B4972695C54A5CF24AA64CB0F4D08A3E8ECB7D6C4645BE52A8A73B42
Malicious:	false
IE Cache URL:	http://https://static.parastorage.com/services/third-party/fonts/user-site-fonts/fonts/9362bca5-b362-4543-a051-2129e2def911.woff
Preview:	wOFF.....Vs.....S.....LINO...X.....OS/2...I...Z...`\O\.cmap.....pA...cvt .....J.....z.mfpgm.....c...gasp.....glyf.....@x..vTv.w-head..Jp...6...6 ..r.hhea..J.... ...$.G..hmtx..J....I.....7+Ploca..M....]....5..maxp..Ot... ... ....name..O....&...pTU..post..Q..... ...2prep..Q.....2..Y[..20131023165841....x.c`f.....B3.e0b ....fffbbfcbj``...s1@.G.....W..3.)h0.:...'0..R.....o....x.M..o.e.....V.j...m. ..b+ 2.d.-C.j.Ee8@.... eFq ..D..".@.. .P..Tl.K...7.....$7..s.D...1i.....K.RB.....8*.VD.....8+....yq.xP\....kl... G.?V..EQi.n.g....8N.....zPi,I.....5.%..B.2Y.\..[.r.....v.....f..aR.....*.C..\..,.laF..Jkm..)K;.u.Q'.=.[.9.....t.].=..{..'....h.|Oz.`O{...*P.9C.3..Fx.H..6.^2.8/.o..&y.dS.)6.4...^.Yf+.....#.:. ...v...,.v..N..[.)Uf.....B...].y...[...Zj..,..*..O..=>.....z.6.d.-.....F_.....i.*.U..^5V..#.}..O....N8.s....Y.....x.c:..... .....(.q.P|>..H.2...P|..} ....X...a.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\F2MQQRVE.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
MD5:	612F638153331AFEBAEBBD3342A1113F
SHA1:	DFA74B975063102F7C6F4DC35E811722697655F3
SHA-256:	A5A2C8167B9F85AD1C47C9F89337CA2F179EBCC642303963E17E22A029F8E8AA
SHA-512:	3D3A01CA75B21DDE0ABECC7BB6C9492E291F31D71657176D1D2DE8E396CD6CE819EC532628C838E6E2F2AB282E318E004CF32ACBE24510160EDA87BC34B79F4
Malicious:	false
IE Cache URL:	http://https://www.artsenvoorwaarheid.nl/

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\F2MQQRVE.htm	
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\Temporary Internet Files\Content.IE5\T4O403JZ\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\Temporary Internet Files\Content.IE5\T4O403JZ\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..:..... I.(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\Temporary Internet Files\Content.IE5\T4O403JZ\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:	29D61DEA50E8D5175DB587C7CAE7AC703BA114C04161870C9BE5A175232252E44C7E1AF07BDA66D80851BBFB1DCB45A71EF307F14AFFD3796EE24F7A4E1AB66F
Malicious:	false
IE Cache URL:	http://https://static.parastorage.com/services/promote-analytics-adapter/2.759.0/analytics-event-adapter.bundle.min.js

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\analytics-event-adapter.bundle.min[1].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\Temporary Internet Files\Content.IE5\T4O403JZ\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
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\Temporary Internet Files\Content.IE5\T4O403JZ\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
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\Temporary Internet Files\Content.IE5\T4O403JZ\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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\coreUtils[1].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\Temporary Internet Files\Content.IE5\T4O403JZ\dataRefs.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):	2041
Entropy (8bit):	5.187939890064941
Encrypted:	false
SSDEEP:	48:xoznSHGdLNSxyAUwugTLHAqdLk0HBmh0hC:4nrsUA/jjg0HcYC
MD5:	9A2AD0B81CF5F46469435545EC3B7104
SHA1:	268225661D68496F35E6B349DCA76EA33AE34EFC
SHA-256:	6C36B17EEF5EF3AA7F1086E689A34C0FB765F6764B2CDEE97975DE049CA70AF6
SHA-512:	0F9DFE334FC562C3E9EC062005DFD7FE8BE36340DA035D17829E15DA7277F3C4CCF293FFE1809A9D0FECF21F7D4A07B542C5276A93AFE2AAD8F5CC5FB9174C E0
Malicious:	false
IE Cache URL:	http://https://static.parastorage.com/unpkg/@wix/wix-ui-santa@2.0.294/dist/statics/dataRefs.bundle.min.js
Preview:	!function webpackUniversalModuleDefinition(e,r){"object"==typeof exports&&"object"==typeof module?module.exports=r():"function"==typeof define&&define.amd?define([],r):"object"==typeof exports?exports.dataRefs=r():e.dataRefs=r()}("undefined"!=typeof self?self:this,(function(){return function(e){var r={};function __webpack_require__(t){if(r[t])return r[t].exports;var _=r[t]={i:t,l:!1,exports:{}};return e[t].call(_.exports,_,_.exports,__webpack_require__),_.l=!0,_.exports}return __webpack_require__.m=e,__webpack_require__.c=r,__webpack_require__.d=function(e,r,t){__webpack_require__.o(e,r)||Object.defineProperty(e,r,{enumerable:!0,get:t})},__webpack_require__.r=function(e){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(e,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(e,"__esModule",{value:!0})},__webpack_require__.t=function(e,r){if(1&r&&(e=__webpack_require__(e)),8&r)return e;if(4&r&&"object"==typeof e&&e&&e.__esModule)return e;var t=Object.create(null

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\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):	2583
Entropy (8bit):	5.720570244871379
Encrypted:	false
SSDEEP:	48:0VUUIqzPrqTnJcgVhkGQPt11WOIp7Fv7RZtqebq11WOIp7Fv7RZtqe06:+UURWTCgVhkFt1ql0ee1ql0eN
MD5:	BD2DB6BB122E3A08F4FA8435FC4B47D4
SHA1:	3702481D984D9F303F76F451F6DFDFAB46A1DF5A
SHA-256:	57FDBEA2496F74AA186E1106D698E9005DEFF40B266474C872DBB004DBD5256A
SHA-512:	A33514E6F4FE7645C7631E2F0049FC8110849C2E194AF199E15D0E29930F10E7F187AC1A20F2370BA37AC7B38231EE3B780F9B2E2A21BDE1CF544CFA1DF2073E
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\Temporary Internet Files\Content.IE5\T4O403JZ\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):	2583
Entropy (8bit):	5.709561056084228
Encrypted:	false
SSDEEP:	48:0VUUIqzPrqTnJcgVhkG2Pbh5WOIp7Fv7RZtqgbqh5WOIp7Fv7RZtqg06:+UURWTCgVhkzbhWl0gehWl0gN
MD5:	B05F16DD239CCCF2C618B75656046D36
SHA1:	6D267295BA5828DB5A1AFB06AC1FA82D6FF36833
SHA-256:	24673FA988F4E9A5167816D9D8913903372DA1E43D8DC36B1DE8B329BC77AC28
SHA-512:	5FB97D3D77697F67B82E56DDA2D0EFDD87991B7DC21316A45E7F01448DF40401210F6FF9CC563CC729723964C4D58087FB4F2A7B8C0E2152DE568EFD204DD26
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\f[2].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\Temporary Internet Files\Content.IE5\T4O403JZ\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 Objec t.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){i f(!(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\Temporary Internet Files\Content.IE5\T4O403JZ\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\Temporary Internet Files\Content.IE5\T4O403JZ\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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\lodash.min[1].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 true;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\Temporary Internet Files\Content.IE5\T4O403JZ\overrides.bundle[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	5389
Entropy (8bit):	4.9544519995864
Encrypted:	false
SSDEEP:	96:UpM8C8dtyEvEWlEmcfXGunhXWiIrKBK9v4s//XeHCk:S1lfyEvEW6mcfXGunhXPIrvd4s/feik
MD5:	2E3F3B6393C59BC6AB16AAFC53E537B4
SHA1:	0E541D34E050FF4CEDE41D94CF3AA4E02DE2B5B0
SHA-256:	D0EA72D47CE376B628257394F8ACB5DED4A33B1FFB73EF9F1A023C8C972D52DD
SHA-512:	187A7A3539E54CE3A4BFCF5F1C1C5506C7ABA12041E310CA1935B17745EE76F53026EB4C1F3794AF83B7CB7840A5C9943ED0628DF2E4288D76800416C0122C47
Malicious:	false
IE Cache URL:	http://https://static.parastorage.com/unpkg/@wix/wix-ui-santa@2.0.294/dist/statics/overrides.bundle.js
Preview:	(function webpackUniversalModuleDefinition(root, factory) {..if(typeof exports === 'object' && typeof module === 'object')...module.exports = factory();..else if(typeof define === 'function' && define.amd)...define([], factory);..else if(typeof exports === 'object')...exports["overrides"] = factory();..else...root["overrides"] = factory();.})((typeof self !== 'undefined' ? self : this), function() {.return /******/ (function(modules) { // webpackBootstrap./******/ .// The module cache./******/ .var installedModules = {};./******/./******/ .// The require function./******/ .function __webpack_require__(moduleId) {./******/./******/ ..// Check if module is in cache./******/ ..if(installedModules[moduleId]) {./******/ ...return installedModules[moduleId].exports;./******/ ..}./******/ ..// Create a new module (and put it into the cache)./******/ ..var module = installedModules[moduleId] = {./******/ ...i: moduleId,./******/ ...l: false,./******/ ...exports: {}./******/ ..};./******/./****

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\siteTags.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):	11216
Entropy (8bit):	5.386898826630416
Encrypted:	false
SSDEEP:	192:tQR4THPSrVjQivOXjCkK8NRgj6MNPPzHex/PobdrgtDo1M6rEgdB3:tQOTvoVMFWPzH8HiKWf
MD5:	74B64900831A2E814A8FF0CDEDCF80CB
SHA1:	AF47310E4A322F6CA516C97BD6DF09C38C36177E
SHA-256:	A055462E069AB37C3C269BF8B80C7C1AAFA72B7D2F0B7699833F87558B06A0CC
SHA-512:	770665074CD4B5629D3260325E8BB156A9DFA36A50BE813BEDA950CCA9B066DB2EEE62EAA9F7B35C563A77D741AE2A52013499BADBCAF8DC90E5546CE1619566
Malicious:	false
IE Cache URL:	http://https://static.parastorage.com/services/tag-manager-client/1.427.0/siteTags.bundle.min.js
Preview:	!function(t){var n={};function e(o){if(n[o])return n[o].exports;var r=n[o]={i:o,l:!1,exports:{}};return t[o].call(r.exports,r,r.exports,e),r.l=!0,r.exports}e.m=t,e.c=n,e.d=function(t,n,o){e.o(t,n)||Object.defineProperty(t,n,{enumerable:!0,get:o})},e.r=function(t){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(t,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(t,"__esModule",{value:!0})},e.t=function(t,n){if(1&n&&(t=e(t)),8&n)return t;if(4&n&&"object"==typeof t&&t&&t.__esModule)return t;var o=Object.create(null);if(e.r(o),Object.defineProperty(o,"default",{enumerable:!0,value:t}),2&n&&"string"!=typeof t)for(var r in t)e.d(o,r,function(n){return t[n]}.bind(null,r));return o},e.n=function(t){var n=t&&t.__esModule?function(){return t.default}:function(){return t};return e.d(n,"a",n),n},e.o=function(t,n){return Object.prototype.hasOwnProperty.call(t,n)},e.p="https://static.parastorage.com/services/tag-manager-client/1.427.0/",e(e.s=7)}([function(t,n,e){"use

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\skin-utils[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	14366
Entropy (8bit):	5.4197064005160005
Encrypted:	false
SSDEEP:	384:yhKJjpTZnylu65VVK65oThXdHEtC7UFst9qgro+HSyJ:tZIu1XdktCpZfJ
MD5:	A14782F687921049A8B790DDD8585B03
SHA1:	4F931B2C0F446FAB96CBC029EF87E0E8187A8FDA
SHA-256:	73DB5B78DBB98A5758A9FCC7FE9B381678375B287341D7638EB8915ACB3B4997
SHA-512:	406D5AAAE0E7214F760B00E4799A5C002CA7075750A96D49EEF25E20EF3608B197FF0CAF0B1352489FCEA085F35CD7117F31386FC3278840F807C7E21F55D13F
Malicious:	false
IE Cache URL:	http://https://static.parastorage.com/unpkg/@wix/santa-skin-utils@1.1686.0/dist/skin-utils.js

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\skin-utils[1].js	
Preview:	!function(r,t){"object"==typeof exports&&"object"==typeof module?module.exports=t(require("lodash"),require("color"),require("coreUtilsLib")):"function"==typeof define&&define.amd?define(["lodash","color","coreUtilsLib"],t):"object"==typeof exports?exports["skin-utils"]=t(require("lodash"),require("color"),require("coreUtilsLib")):r["skin-utils"]=t(r.lodash,r.color,r.coreUtilsLib)}(this,(function(r,t,n){return function(r){var t={};function n(e){if(t[e])return t[e].exports;var i=t[e]={i:e,l:!1,exports:{}};return r[e].call(i.exports,i,i.exports,n),i.l=!0,i.exports}return n.m=r,n.c=t,n.d=function(r,t,e){n.o(r,t)||Object.defineProperty(r,t,{enumerable:!0,get:e})},n.r=function(r){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(r,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(r,"__esModule",{value:!0})},n.t=function(r,t){if(1&t&&(r=n(r)),8&t)return r;if(4&t&&"object"==typeof r&&r&&r.__esModule)return r;var e=Object.create(null);if(n.r(e),Object.defineProperty

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\skins.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):	394510
Entropy (8bit):	5.370227828032885
Encrypted:	false
SSDEEP:	12288:j4WQCBH8AAULsDm10EtpJe5jTK9EDNHWKOzVpSbKu1wqryUJ+0CyBe9zR6Y5b+AA:j4+yBe9zRMA3Q
MD5:	970A5A90DD7AEB73F403E86EE4849B87
SHA1:	92A921A29F5761C1F0E4C2D39779CED837A9D18B
SHA-256:	B9362DD9B9D3272E10799E1B366D08279BA21E45766E15E994597131B4D87526
SHA-512:	915F92F97ABD17C1494F89152789617030B50BD494ECF24741ECC223F354708C244C2CBDEA2DAF6A3DFE62967C524F7D66C82C178829BB61566F44D08E9A8AC
Malicious:	false
IE Cache URL:	http://https://static.parastorage.com/services/wix-bolt/1.7264.0/node_modules/wix-santa/dist/packages-bin/skins/skins.min.js
Preview:	define("skins",["lodash","santa-components","santa-core-utils","skinUtils"],(function(t,e,o,r){return function(t){var e={};function o(r){if(e[r])return e[r].exports;var a=e[r]={i:r,l:!1,exports:{}};return t[r].call(a.exports,a,a.exports,o),a.l=!0,a.exports}return o.m=t,o.c=e,o.d=function(t,e,r){o.o(t,e)||Object.defineProperty(t,e,{enumerable:!0,get:r})},o.r=function(t){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(t,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(t,"__esModule",{value:!0})},o.t=function(t,e){if(1&e&&(t=o(t)),8&e)return t;if(4&e&&"object"==typeof t&&t&&t.__esModule)return t;var r=Object.create(null);if(o.r(r),Object.defineProperty(r,"default",{enumerable:!0,value:t}),2&e&&"string"!=typeof t)for(var a in t)o.d(r,a,function(e){return t[e]}.bind(null,a));return r},o.n=function(t){var e=t&&t.__esModule?function(){return t.default}:function(){return t};return o.d(e,"a",e),e},o.o=function(t,e){return Object.prototype.hasOwnProperty.call(t,e)

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\src=4382365;type=count;cat=websi0;ord=1;num=4397511000816;gtm=2wg6n0;u1=undefined;~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:	dropped
Size (bytes):	524
Entropy (8bit):	5.398342281693514
Encrypted:	false
SSDEEP:	12:hnMQbwuOaxyCkv4A1ZtlwV7eoswb03AEIAgKWw1vR/a2W2KD:hMiRO9N60VPqAgKvvhyl
MD5:	F84C21E13587FA410F294A5FFC07105A
SHA1:	9271766F54253750F6059B8CAD1875F71C3B5654
SHA-256:	12AFD579411EF1A7E88BB2C74B39B68E90A4DCFB1E273450A863C8DABCD9CD64
SHA-512:	801686D1E27AFB4CEE5049EA66B0B8CA08D701BF3ADDA8BF7C7739CE62E113F192950864245B14B2280308B71EF1BFEA2749434B954E5618F9EDCD89BB47006
Malicious:	false
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="background-color: transparent"><iframe src="https://adservice.google.de/ddm/fls/i/src=4382365;type=count;cat=websi0;ord=1;num=4397511000816;gtm=2wg6n0;u1=undefined;~oref=https%3A%2F%2Fwww.wix.com%2Foutdated-browser%2Finternet-explorer%3FforceBolt%3D%26ssrIndicator%3Dfalse%26suppressbi%3Dtrue" width="1" height="1" frameborder="0" style="display:none"></iframe></body></html>

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\src=4382365;type=count;cat=websi0;ord=1;num=4397511000816;gtm=2wg6n0;u1=undefined;~oref=https___www.wix[2].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	194
Entropy (8bit):	5.144203472842556
Encrypted:	false
SSDEEP:	6:hn8FQiowadCc4svmzw9xUpCX96v6OqPbRm9:hnMQbwuOaxyCkv4A9
MD5:	5EDEA4CDE2C1A9C8E8150DEAF71CE73D
SHA1:	725019DAAF24DED79DCAAC96C897CC4727CC8B35
SHA-256:	05978957C6C8B028F2785DC77271C286BFAC76E30B7BCD7E835C2927FBE897CF
SHA-512:	E55349AB79FEF70C5DF45009E9EA2E4CA57678305A25B3279CFFAD472192654FE86E30B9471313243FB081D7B2C2958E8F888F87C648AAE5FF00E289C69B615E
Malicious:	false
IE Cache URL:	http://https://adservice.google.de/ddm/fls/i/src=4382365;type=count;cat=websi0;ord=1;num=4397511000816;gtm=2wg6n0;u1=undefined;~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="background-color: transparent"></body></html>

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\thirdPartyAnalytics.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	C source, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	9873
Entropy (8bit):	5.205156652219834
Encrypted:	false
SSDEEP:	192:jcvj1yLBPBT2nQc94VE9Mz9hrbZ4iDwwpzH1AKyfCpsJ+W4:g1ymnXWV6OdPDllH1ECmJ+W4
MD5:	907C5062AE2E2C1732B12348708E30A0
SHA1:	832E34675A984610BF11BE4810D0ECEEF30FE240
SHA-256:	32567FEC7314C675F45B50A968C9B6AB076AB459C00362CFE7EC8CFD08A18D1A
SHA-512:	68A85A9558E42AAF2BF2475FC2D8A435B98EA5AB50A6B465A2BE895180EA0AF52FB740D68EE452B2AE39B53C48018EB38A2EEF654F7AD2D062A4ED14BA05792F
Malicious:	false
IE Cache URL:	http://https://static.parastorage.com/services/wix-bolt/1.7264.0/node_modules/wix-santa/dist/packages-bin/thirdPartyAnalytics/thirdPartyAnalytics.min.js
Preview:	define("thirdPartyAnalytics",["lodash","warmupUtils","santa-core-utils"],(function(n,e,t){return function(n){var e={};function t(i){if(e[i])return e[i].exports;var r=e[i]={i:i,l:!1,exports:{}};return n[i].call(r.exports,r,r.exports,t),r.l=!0,r.exports}return t.m=n,t.c=e,t.d=function(n,e,i){t.o(n,e)||Object.defineProperty(n,e,{enumerable:!0,get:i})},t.r=function(n){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(n,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(n,"__esModule",{value:!0})},t.t=function(n,e){if(1&e&&(n=t(n)),8&e)return n;if(4&e&&"object"==typeof n&&n&&n.__esModule)return n;var i=Object.create(null);if(t.r(i),Object.defineProperty(i,"default",{enumerable:!0,value:n}),2&e&&"string"!=typeof n)for(var r in n)t.d(i,r,function(e){return n[e]}.bind(null,r));return i},t.n=function(n){var e=n&&n.__esModule?function(){return n.default}:function(){return n};return t.d(e,"a",e),e},t.o=function(n,e){return Object.prototype.hasOwnProperty.call(n,e)},t.p

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\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=Microdata&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=1624916899967&cd[DataLayer]=%5B%5D&cd[Meta]=%7B%22title%22%3A%22Internet%20Explorer%20Web%20Browser%20Is%20Ending%20Support%20Soon%22%2C%22meta%3Adescription%22%3A%22To%20get%20a%20better%20browsing%20experience%2C%20download%20a%20new%20browser%20for%20free%20onto%20your%20desktop.%20Learn%20more%20about%20how%20to%20download%20a%20new%20browser%20today.%22%7D&cd[OpenGraph]=%7B%22og%3Atitle%22%3A%22Internet%20Explorer%20Web%20Browser%20Is%20Ending%20Support%20Soon%22%2C%22og%3Adescription%22%3A%22To%20get%20a%20better%20browsing%20experience%2C%20download%20a%20new%20browser%20for%20free%20onto%20your%20desktop.%20Learn%20more%20about%20how%20to%20download%20a%20new%20browser%20today.%22%2C%22og%3Aimage%22%3A%22https%3A%2F%2Fstatic.wixstatic.com%2Fmedia%2F311dce_77ca1007cf83485da0b7e16ffb9735ac~mv2.png%2Fv1%2Ffill%2Fw_1200%2Ch_630%2Cal_c%2F311dce_77ca1007cf83485da0b7e16ffb9735ac~mv2.png%22%2C%22og%3Aimage%3Awidth%22%3A%221200%22%2C%22og%3Aimage%3Aheight%22%3A%22630%22%2C%22og%3Aurl%22%3A%22https%3A%2F%2Fwww.wix.com%2Foutdated-browser%2Finternet-explorer%22%2C%22og%3Asite_name%22%3A%22Report%20Spam%22%2C%22og%3Atype%22%3A%22website%22%7D&cd[Schema.org]=%5B%5D&cd[JSON-LD]=%5B%5D&sw=1280&sh=1024&v=2.9.42&r=stable&ec=1&o=14&it=1624916899179&coo=false&es=automatic&tm=3&rqm=GET
Preview:	GIF89a.....!.....,.....D..;.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\urlblockindex[1].bin	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	data
Category:	downloaded
Size (bytes):	16
Entropy (8bit):	1.6216407621868583
Encrypted:	false
SSDEEP:	3:PF/l:
MD5:	FA518E3DFAE8CA3A0E495460FD60C791
SHA1:	E4F30E49120657D37267C0162FD4A08934800C69
SHA-256:	775853600060162C4B4E5F883F9FD5A278E61C471B3EE1826396B6D129499AA7
SHA-512:	D21667F3FB081D39B579178E74E9BB1B6E9A97F2659029C165729A58F1787DC0ADADD980CD026C7A601D416665A81AC13A69E49A6A2FE2FDD0967938AA645C0
Malicious:	false
IE Cache URL:	http://https://r20swj13mr.microsoft.com/ieblocklist/v1/urlblockindex.bin
Preview:	.p.J2.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\v3[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\Temporary Internet Files\Content.IE5\T4O403JZ\v3[1].gif	
Category:	dropped
Size (bytes):	35
Entropy (8bit):	2.97020783365077
Encrypted:	false
SSDEEP:	3:CUU0/rllHh/:S0TJ/
MD5:	9B8D19F4310C758344E40BF17FBC7E85
SHA1:	2290EF058812D5F5E398736E2316CBA8CF8093CF
SHA-256:	37B17C5135A176A9474521AF147D96DFA1FB4CA0F43F00D1400BD1885BE3AB9B
SHA-512:	793F00C21FE332ED3CC1C1B17B4EBB115379D6468C6CC3668D6E99DA0FF73C52E8E023FDA8786193F8B256C7AD6E1415378969602C72BA3206DA6FD46470CEA
Malicious:	false
Preview:	GIF89a.....,.....D..;

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\v3[2].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped
Size (bytes):	35
Entropy (8bit):	2.97020783365077
Encrypted:	false
SSDEEP:	3:CUU0/rllHh/:S0TJ/
MD5:	9B8D19F4310C758344E40BF17FBC7E85
SHA1:	2290EF058812D5F5E398736E2316CBA8CF8093CF
SHA-256:	37B17C5135A176A9474521AF147D96DFA1FB4CA0F43F00D1400BD1885BE3AB9B
SHA-512:	793F00C21FE332ED3CC1C1B17B4EBB115379D6468C6CC3668D6E99DA0FF73C52E8E023FDA8786193F8B256C7AD6E1415378969602C72BA3206DA6FD46470CEA
Malicious:	false
Preview:	GIF89a.....,.....D..;

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\viewerComponentService.bundle[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	37928
Entropy (8bit):	5.041535174878363
Encrypted:	false
SSDEEP:	384:SL+FVpPyyVJpP1HmxGfaweb3yXvwjpbbAj5JFHnGrQna8ZjO2lneiL3ynWokUVR:HjlP1HmxGfawebiYj9bA9vGrQnaysou
MD5:	5F3E9DF0BD2ABB3656165C971DEDAF4D
SHA1:	B09C2DF939E0AFB70A1BBEC93357D4CFC47E10DA
SHA-256:	B0522077490AFBABD5D4F924A89FE89E842EFEB98822526294D3D1CEF33B6EB1
SHA-512:	1938D5D603052A567D51C58A3659D764363C54E5A2028E4552ECD08EFB64547BC4C9E897711C2495197ABCFF345FC6FC33707C26677229B30AD4DC2D7D72470A
Malicious:	false
IE Cache URL:	http://https://static.parastorage.com/unpkg/@wix/wix-ui-santa@2.0.294/dist/statics/viewerComponentService.bundle.js
Preview:	(function webpackUniversalModuleDefinition(root, factory) {..if(typeof exports === 'object' && typeof module === 'object')...module.exports = factory(require("react"), require("prop-types"), require("lodash"), require("santa-components"), require("react-dom"));..else if(typeof define === 'function' && define.amd)...define(["react", "prop-types", "lodash", "santa-components", "reactDOM"], factory);..else if(typeof exports === 'object')...exports["viewerComponentService"] = factory(require("react"), require("prop-types"), require("lodash"), require("santa-components"), require("react-dom"));..else...root["viewerComponentService"] = factory(root["React"], root["prop-types"], root["_"], root["santaComponents"], root["ReactDOM"]);.})((typeof self !== 'undefined' ? self : this), function(__WEBPACK_EXTERNAL_MODULE__0__, __WEBPACK_EXTERNAL_MODULE__1__, __WEBPACK_EXTERNAL_MODULE__3__, __WEBPACK_EXTERNAL_MODULE__4__, __WEBPACK_EXTERNAL_MODULE__33__) {.return /******/ (function(modules) { // webp

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\viewerScript.bundle.min[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.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\Temporary Internet Files\Content.IE5\T4O403JZ\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
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\Temporary Internet Files\Content.IE5\T4O403JZ\wix-resize-observer-polyfill.56f8c1c1.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):	8150
Entropy (8bit):	5.083726556129888
Encrypted:	false
SSDEEP:	96:2DB9cWX6WuQvTlEvroUiLhaKxMcP1hTjyzcAIJqSVy3tNSAMDje8O5Z2/eEj9ipr:q9pvTxJiQDjyzzIJu8rN9ibSwv
MD5:	41F8238C3628CF2F1006CEA34CCF3231
SHA1:	5801EA10823609B8E835716A030EC6AF7A08BAC4
SHA-256:	5075CD8D885EEEE885C19B24251B671E81F1D542E5C810397E5DAE49A124F7D0
SHA-512:	4B71E763AE93C1E856CD1E005DFFBBBEE8D0B1BE9948AF1D9BA584988FBA2A15D97533CED111E5974AFC8E8FE65F92C84256254697CACCEF8E7762C225B191DC
Malicious:	false
IE Cache URL:	http://https://static.parastorage.com/services/wix-thunderbolt/dist/wix-resize-observer-polyfill.56f8c1c1.chunk.min.js
Preview:	(self.webpackJsonp__wix_thunderbolt_app=self.webpackJsonp__wix_thunderbolt_app||[]).push([[7971],{5653:function(t,e,n){"use strict";n.r(e);var i=function(){if("undefined"!=typeof Map)return Map;function t(t,e){var n=-1;return t.some((function(t,i){return t[0]===e&&(n=i,!0)})),n}return function(){function e(){this.__entries__=[]}return Object.defineProperty(e.prototype,"size",{get:function(){return this.__entries__.length},enumerable:!0,configurable:!0}),e.prototype.get=function(e){var n=t(this.__entries__,e),i=this.__entries__[n];return i&&i[1]},e.prototype.set=function(e,n){var i=t(this.__entries__,e);~i?this.__entries__[i][1]=n:this.__entries__.push([e,n])},e.prototype.delete=function(e){var n=this.__entries__,i=t(n,e);~i&&n.splice(i,1)},e.prototype.has=function(e){return!!~t(this.__entries__,e)},e.prototype.clear=function(){this.__entries__.splice(0)},e.prototype.forEach=function(t,e){void 0===e&&(e=null);for(var n=0,i=this.__entries__;n<i.length;n++){var r=i[n];t.call(e,r[1],r[0])}

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\xss.min[1].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].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){var FilterCSS=require("cssfilter").FilterCSS;var getDefaultCSSWhiteList=require("cssfilter").getDefaultWhiteList;var _=require("./util");function getDefaultWhiteList(){return{a:["target","href","title"],abbr:["title"],address:[],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\Temporary Internet Files\Content.IE5\XNHC0JWC\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:7jhrmUyj3rNIth1q7Nxt824dQ3F
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\Temporary Internet Files\Content.IE5\XNHC0JWC\704136006388169[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	269361
Entropy (8bit):	5.4837080909282445
Encrypted:	false
SSDEEP:	6144:Rk1HgCSntDV/HaK8V/Ha8NEPjQHguH3HpQrwz8GW/:kNE7F
MD5:	7D7A91C5FB82395B67E33FB5F283A68D
SHA1:	AAB171A1DDAFF79719B87844909E0E6EE6C54431
SHA-256:	D1284DE679390F5B2E27DBAB52AD23761F66996A58425929E44C9AEE1EAED5B8
SHA-512:	0140426BB3567893946A59587D32EAF4949004A2ED94AC983B26B96EA5484897FAB02B86701B940234AAD5A69A25EEEE412C002A32A915ED3540309254F2DD57
Malicious:	false
IE Cache URL:	http://https://connect.facebook.net/signals/config/704136006388169?v=2.9.42&r=stable
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\Temporary Internet Files\Content.IE5\XNHC0JWC\ProfileCardController.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):	312244
Entropy (8bit):	5.360346241576116
Encrypted:	false
SSDEEP:	1536:F9P1ZBSSIa5XJPvPvGITTX+k+Kaa386soFMykgqTirluFcjDcGu59bF9a/7MB/MG:0SXLTeKt8EaRwHEQvH9KyijcsnCvPZb
MD5:	DE322298E943CF779F4CB282D2F369B4
SHA1:	768894FB2B1FF1160082228075F36CF6AE792587
SHA-256:	C0F2B17933B579AC121A4A02C50A30E18DF4865DA27693C6EC8AD2341EFA73D2
SHA-512:	E25CE94A20198B72D721641874656CD37CC1C30F372F9FC08DDFFF714AB8DBA315D48C3C760FA9CE881D05A56EF03D37B2C27B6993B7A41939D43D261E95D7
Malicious:	false
IE Cache URL:	http://https://static.parastorage.com/services/profile-card-tpa-ooi/1.277.0/ProfileCardController.bundle.min.js

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\ProfileCardController.bundle.min[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.ProfileCardController=t():e.ProfileCardController=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.__esM

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\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\Temporary Internet Files\Content.IE5\XNHC0JWC\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.gl..h...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\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
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....I....~.=.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\Temporary Internet Files\Content.IE5\XNHC0JWC\WixMadeforText_W_Rg[1].woff	

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\activityi;src=4382365;type=count;cat=websi0;ord=1;num=4397511000816;gtm=2wg6n0;u1=undefined;~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:	dropped
Size (bytes):	525
Entropy (8bit):	5.401151143591865
Encrypted:	false
SSDEEP:	12:hnMQbwuOaxyCkv4A1ZHwV7eoswb03AEIAgKWw1vR/a2W2KD:hMiRO9w0VPqAgKvvhyl
MD5:	D79A4A451F7EC7C544DBF9D73C45C03D
SHA1:	A69F4ABB11D564D7FB5E26A5FA491743BD475247
SHA-256:	C477B0D9C6A1A2F32EAAE814521DF22B96FEB7C0F8EDA74B6267BB2C152CF47C
SHA-512:	491D25B1886DFFFCADE490BE37B480738BD1BE76BD864DA4E5A5E32D93F10DD7F1D9B4A7235ACBA9CD3094762D523794519F24F2AEFD8FE4F02E25335A60EBE0
Malicious:	false
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="background-color: transparent"><iframe src="https://adservice.google.com/ddm/fls/i/src=4382365;type=count;cat=websi0;ord=1;num=4397511000816;gtm=2wg6n0;u1=undefined;~oref=https%3A%2F%2Fwww.wix.com%2Foutdated-browser%2Finternet-explorer%3FforceBolt%3D%26ssrIndicator%3Dfalse%26suppressbi%3Dtrue" width="1" height="1" frameborder="0" style="display:none"></iframe></body></html>

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\backgroundCommon.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	60491
Entropy (8bit):	5.275391112179184
Encrypted:	false
SSDEEP:	768:TjaZ7aN3TRXcGr6L3qBuOkTKVZCqClT3gN1FR/7NgZFbz8Smz9PGIuIYI46R:Tje8ZcGeL3qB4TK0T3gNDNI8bGIuW4c
MD5:	D80649607043BFA952989CCA71197D59
SHA1:	E6EC186A15B37B4F33AC8886B184A9D0305C6F56
SHA-256:	59C24AC72D1B4C54D7D470C8F48EE7116CBD4E924DBF5D5D05FD4D30575B6577
SHA-512:	4A812818AC669B0935221BE223A4B2DFAE6D8E2E0CD2E6FB7B46E3D03F476DB5A3E92A55CF8B7B438E3A795024EEBEAF9CE77255B256AAF3F5E67E913A2E6CBF
Malicious:	false
IE Cache URL:	http://https://static.parastorage.com/services/wix-bolt/1.7264.0/node_modules/wix-santa/dist/packages-bin/backgroundCommon/backgroundCommon.min.js
Preview:	define("backgroundCommon",["lodash","coreUtils","santa-components","componentsCore","prop-types","skins","warmupUtils","image-client-api","color","pmrpc"],(function(e,t,i,o,n,a,r,s,p,d){return function(e){var t={};function i(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,i),n.l=!0,n.exports}return i.m=e,i.c=t,i.d=function(e,t,o){i.o(e,t)||Object.defineProperty(e,t,{enumerable:!0,get:o})},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 o=Object.create(null);if(i.r(o),Object.defineProperty(o,"default",{enumerable:!0,value:e}),2&t&&"string"!=typeof e)for(var n in e)i.d(o,n,function(t){return e[t]}.bind(null,n));return o},i.n=function(e){var t=e&&e.__esModule?function(){return e.default}:function(){return e

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\bat[1].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}$/,error:"{p} value must be ISO standard currency code"},number:{type:"num",digits:3,max:9999999999999},integer:{type:"num",digits:0,max:9999999999999},hct_los:{type:"num",digits:0,max:30},date:{type:"regex",regex:/^\d{4}-\d{2}-\d{2}$/,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\Temporary Internet Files\Content.IE5\XNHC0JWC\bc176270-17fa-4c78-a343-9fe52824e501[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 30192, version 1.0
Category:	downloaded
Size (bytes):	30192
Entropy (8bit):	7.97938449205579
Encrypted:	false
SSDEEP:	768:zKTyKQfjvSP7I5zwRPw+ku8KOV2YsBnkRSAHq:OTGfjC7I5z8P18vV+eSAK
MD5:	4DC77F0FF1474412272BA230B085D035
SHA1:	E2558F88D8F2878B4A5510967D107223B6C29BD1
SHA-256:	C629B3CE163A14DF3B642F01044A989647EBBDB0F7D5D1D95783BDCE89A8A666
SHA-512:	9A7B656A56D652E4BB6E7BAAA8B8AFA3C684CF1B5292EB1BF3EFB9254BF7384164B315289A2AB8C96B93E410E63747357E3670CFABB395A69551810C5776CCD5
Malicious:	false
IE Cache URL:	http://https://static.parastorage.com/services/third-party/fonts/user-site-fonts/fonts/bc176270-17fa-4c78-a343-9fe52824e501.woff
Preview:	wOFF.....u.....(.....OS/2...X...X...`g).gcmap.....L.....cvt .....&...&...~fpgm...$.....s.Y.7gasp...(.....glyf...0..JB....E3.{head..Nt...6...6....hhea..N.... ...$ ...)hmtx..N.....;.kern..P.....:&....loca..j.....~N..maxp..l`... ... .name..l.....b...post..uh..... ...2prep..u|...r....}...x.c`f|.8.....i.S...C..f..`.....a=P....|.....l.'....|F...]..@.....x.E../.a...o..{[|V.z.m....(....W.77.9:..Hl.....3Ym.wf.&Of^@.!....B.....1T.*T.jN.Cud.1=..=.t.....M.u.>K.....7.P.B..q.C...m..MT...qo\.)...V..q.~..]..g....'..h.vy.M....Y\.{s.y.aL..'^x./~.K.@.....N..D.M.....I.<.XI!.4.. .,..!.<.)...)...J)...*.SE55.RG=.4.D3-..F;.t.E7=..G?.8.d.aF.e.q&.d.ifXe.evXc.%^Yg.Y6.b....f../.^P%...4.+./.6.:.1.....L.....x.].=N.0...8,..H..-+.+..R8.P.@(<.?.D..Hih\p..3]..`.....3.....k..m.....L.. ...I ..U.I..8sl..w..dQ?..:.x.....o[...`..V.t...).*Q.....s.....L./..L`.//..F..i.C..+*=*ctEc.h.. ....G..d...57

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\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\Temporary Internet Files\Content.IE5\XNHC0JWC\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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\bundle.min[1].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\Temporary Internet Files\Content.IE5\XNHC0JWC\ca003289-5ee3-45c2-94ad-36c743c35fc1[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 31147, version 1.0
Category:	downloaded
Size (bytes):	31147
Entropy (8bit):	7.987396350283174
Encrypted:	false
SSDEEP:	768:C9IfZeyachSjRMkny9BzuEUnCQJbPaZ3kI1irZQo:C9MqjRj8Qn1pak0iio
MD5:	F3471862C553872A8A36648B3D1F55D4
SHA1:	FD60A4A0674CFCB218C2CC425222501D78815087
SHA-256:	8177D7B57C7E74E786593452C92DCCE54B2610766530F30E856848E56A603E46
SHA-512:	3A5073177947A16028012E6571EEE0CCA99E7B908FDD9EFDEF06F2C1555A5BED784EF610E2C645BD463FD712F59BB9C7B0E46D0A67F78ED03701F385047FBB0A
Malicious:	false
IE Cache URL:	http://https://static.parastorage.com/services/santa-resources/resources/viewer/user-site-fonts/fonts/Helvetica/v2/ca003289-5ee3-45c2-94ad-36c743c35fc1.woff
Preview:	wOFF.....y.....t.....GPOS.....GSUB...(.....OS/2.....S...`eDz.VDMX...P...Z....r.y.cmap.....'cvt ...|...K.....fpgm.....,...gasp...T.....glyf...\..P.....head..fH...6...6.z}.hhea..f....!...$.>.Lhmtx..f.....(.G3sloca..i`.....,.j.maxp..m`... ... .Y.Mname..m.....!l..$post..sL..... ...2prep..s`.....y..x..TMOSQ.=.J.mi-Vl..Q..hLP.".4iSQ.jD..qc.QKX...\.A..4Q.....[....a.....y...E}'w.w./.B..0.W.....C.b8.>....B&.C|....R.#.....W.R.V.*....s...qP.Q..jO.M.M.....:U...C..J;,..F+u....pM.....!.B.6i.9.+.Tp..V.@.....W[&99..+.Zm.....k...c....|.....P.T|.<.....I..oo.....*.y....".1....o|.5j/..(.....2..n..w.l.3.9..._...\.,..,...S].r...o..6,...A?.%..!8.NF...E..q..ad1.[.'&p.....f..O../0.y,.%....x..A$...X...@.a.n.Yz.z....OX..K....a.E.,.,:.?.s.0K6.|s.'..|..Z".....rF.....8.D.....Du.U....Q.Q.Ji.."Zp..3D..k.....KD+F.z\&.0J.U..\!..J.p...:.]5...coS.....~".O...%| .2>

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\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\Temporary Internet Files\Content.IE5\XNHC0JWC\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\Temporary Internet Files\Content.IE5\XNHC0JWC\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:	0AD23B1D6E46D4E7090EFEA9D7A5EE621D1A21F2AB7EC0D403C65365337178F6AC76E8F2E6CB20313AC4FB6B9CEE94115BF2833F0EE78A980CB669E80A7403 1
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.Documen t.prototype.createElement,e=window.Document.prototype.createElementNS,n=window.Document.prototype.importNode,o=window.Document.prototype.prepend,r=win dow.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=O bject.getOwnPropertyDescriptor(window.Node.prototype,"textContent"),d=window.Element.prototype.attachShadow,p=Object.getOwnPropertyDescriptor(window.E lement.prototype,"innerHTML"),m=window.Element.prototype.getAttribute,w=window.Element.prototype.setAttribute,y=window.Element.prototype.removeAttribute,v=windo w.Element.prototype.getAttributeNS,E=window.Element.prototype.setAttributeNS,b=w

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\displayer.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	67102
Entropy (8bit):	5.352197088503686
Encrypted:	false
SSDEEP:	768:+IxFGqv1Wt2j1K7CZrE6QceQxjlEG4jvavNrk/j0YN9uKn3C9u0mslzaGwlcF:+Ixi2jRmwxjl34jcNw9IKkOGWcF
MD5:	978C38A84D041B8081A7E7C7AC37AA3D
SHA1:	39E070B520F2475E7DF8C69DAC7BE8F806BFEA84
SHA-256:	A57295E4D49D2ACE0D529E2EABDFC2B9957F7986116CE3079B6397DAD0CB0F72
SHA-512:	AFE81D1C11C29663304700E8B49CD7A02F6AFF882DA564FB8BFA417CDDC85C89C477E1C7B92B312C62304CCE0AF43E29ECC061A66607FD9EF6DEF118806FBF E3
Malicious:	false
IE Cache URL:	http://https://static.parastorage.com/services/wix-bolt/1.7264.0/node_modules/wix-santa/dist/packages-bin/displayer/displayer.min.js
Preview:	define("displayer",["lodash","coreUtils","santa-components","componentsCore","prop-types","skins","reactDOM","image-client-api"],(function(t,e,i,r,o,a,p,n){return function(t) {var e={};function i(r){if(e[r])return e[r].exports;var o=e[r]={i:r,l:!1,exports:{}};return t[r].call(o.exports,o,o.exports,i),o.l=!0,o.exports}return i.m=t,i.c=e,i.d=function(t,e,r){i.o (t,e)||Object.defineProperty(t,e,{enumerable:!0,get:r})},i.r=function(t){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(t,Symbol.toStringTag, {value:"Module"}),Object.defineProperty(t,"__esModule",{value:!0})},i.t=function(t,e){if(1&e&&(t=i(t)),8&e)return t;if(4&e&&"object"==typeof t&&t&&t.__esModule)return t;var r=Object.create(null);if(i.r(r),Object.defineProperty(r,"default",{enumerable:!0,value:t}),2&e&&"string"!=typeof t)for(var o in t)i.d(r,o,function(e){return t[e]}.bind(null,o));return r},i.n=function(t){var e=t&&t.__esModule?function(){return t.default}:function(){return t};return i.d(e,"a",e),e},i.o=f

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\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
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\Temporary Internet Files\Content.IE5\XNHC0JWC\galleriesCommon.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\galleriesCommon.min[1].js	
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	4129
Entropy (8bit):	5.210747730963494
Encrypted:	false
SSDEEP:	96:YJFqr6XHhbEVLBcd9wSiyUsOD7klj/3aTqEU5CemUYu0E:YJ1RcWoSKsOD7klj/oqj5CemU70E
MD5:	01D80E46A9B39435AC06B3C210BDF2C8
SHA1:	9BD64459F8CC105C84779C5E25912174437CD2C2
SHA-256:	22B1E0568CFC5107C5D59C07056BA7C03F39C9666F1D70701FC89B9FFFC2AF3B
SHA-512:	11B3606F3CFD1ECD7461CBB83204B2806A0DC8909DA60429C25F7E3415E65A300C1EA8EBD044B45261F1AEF9FC6746199215DA6307DCD59A6EDC6C768785AF
Malicious:	false
IE Cache URL:	http://https://static.parastorage.com/services/wix-bolt/1.7264.0/node_modules/wix-santa/dist/packages-bin/galleriesCommon/galleriesCommon.min.js
Preview:	define("galleriesCommon",["lodash","coreUtils","santa-components","skinExports"],(function(t,e,o,i){return function(t){var e={};function o(i){if(e[i])return e[i].exports;var n=e[i]={i:i,l:!1,exports:{}};return t[i].call(n.exports,n,n.exports,o),n.l=!0,n.exports}return o.m=t,o.c=e,o.d=function(t,e,i){o.o(t,e)||Object.defineProperty(t,e,{enumerable:!0,get:i})},o.r=function(t){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(t,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(t,"__esModule",{value:!0})},o.t=function(t,e){if(1&e&&(t=o(t)),8&e)return t;if(4&e&&"object"==typeof t&&t&&t.__esModule)return t;var i=Object.create(null);if(o.r(i),Object.defineProperty(i,"default",{enumerable:!0,value:t}),2&e&&"string"!=typeof t)for(var n in t)o.d(i,n,function(e){return t[e]}.bind(null,n));return i},o.n=function(t){var e=t&&t.__esModule?function(){return t.default}:function(){return t};return o.d(e,"a",e),e},o.o=function(t,e){return Object.prototype.hasOwnProperty.call

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\identity[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	11633
Entropy (8bit):	5.7883624283841515
Encrypted:	false
SSDEEP:	192:sCQHyB0Qt5BeeOvnJdTQn8dMf2IUiVIgqgxdbYpH380QtKgSbq8kjMc9Ix0vvOuG:sCJBTMMf2IUiGUU8QgSbqRFy0vvpi
MD5:	A4B4E2FB56CBAC0AA769F30236149A3B
SHA1:	2B80252D14157774F2F06A65EE9B55B66CF4D8DB
SHA-256:	3BEA34F20C813024F046166FB0AD98A8EB93D5AB93052CEB993EEE238ECE5B66
SHA-512:	46D1C72B70B054EAC2B6C511F7C09ECC176566037322AC0FAEA7FFC10071503CD71903EB514D6C482A21185BB53571400359EC2B2080BB1DCA9AD6146566E79
Malicious:	false
IE Cache URL:	http://https://connect.facebook.net/signals/plugins/identity.js?v=2.9.42
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.* IM PLIED, 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 C ONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN.* CONNECTION WI

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\imageZoom.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	38750
Entropy (8bit):	5.269496272384624
Encrypted:	false
SSDEEP:	768:oe2dO+ffpuRdEtv//FBzCqGlCmdqUEP38p8dWJxhAcSv:oezRdEp//FBzCqGlCmdqUEP38qwb+
MD5:	40BFEEEE9DB56B7C198C3FC40F037C96
SHA1:	2DB70EA24C760A0BFCE5E0747312D2416CDA9A4D
SHA-256:	6AFE17ED07B060DCFBF39804D0ABC5F9B6514C57B956ED29FD51021E67286128
SHA-512:	BB4D1A150EB315520CA65D91CED089CBCDC1BC798DFE870B2A2CC5339296DD41417D3D1571956659F3B986478DF31A1578EC664A914C0A3C938204D971A1D8
Malicious:	false
IE Cache URL:	http://https://static.parastorage.com/services/wix-bolt/1.7264.0/node_modules/wix-santa/dist/packages-bin/imageZoom/imageZoom.min.js
Preview:	define("imageZoom",["lodash","coreUtils","santa-components","componentsCore","prop-types","skins","reactDOM","zepto","image-client-api"],(function(t,e,i,n,o,s,a,r,p){return function(t){var e={};function i(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,i),o.l=!0,o.exports}return i.m=t,i.c=e,i.d=function(t,e,n){i.o(t,e)||Object.defineProperty(t,e,{enumerable:!0,get:n})},i.r=function(t){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(t,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(t,"__esModule",{value:!0})},i.t=function(t,e){if(1&e&&(t=i(t)),8&e)return t;if(4&e&&"object"==typeof t&&t&&t.__esModule)return t;var n=Object.create(null);if(i.r(n),Object.defineProperty(n,"default",{enumerable:!0,value:t}),2&e&&"string"!=typeof t)for(var o in t)i.d(n,o,function(e){return t[e]}.bind(null,o));return n},i.n=function(t){var e=t&&t.__esModule?function(){return t.default}:function(){return t};return i.d(e,"a",e

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\intersection-observer-polyfill.67fb87dd.chunk.min[1].js	
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.intersectionRatio>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_OBSERVER=!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._checkForIntersections()}))},n},r._resetCrossOriginUpdater=function(){n=null,o=null},r.prototype.observe=function(t){if(!this._observationTargets.some((function(e){return e.element==t}))){if(!t||1!

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\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:4ODFkXzE3d8YBmH1KIAq3
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\Temporary Internet Files\Content.IE5\XNHC0JWC\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
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\Temporary Internet Files\Content.IE5\XNHC0JWC\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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\pm-rpc.min[1].js	
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?a:c:s&&s in Object(t)?i(t):u(t)}var o=e(8),i=e(

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\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\Temporary Internet Files\Content.IE5\XNHC0JWC\skinExports.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
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

Static File Info

General

File type:	Microsoft Word 2007+

General

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

File Icon

Icon Hash:	e4e6a2a2a4b4b4a4

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 14:48:44.879158020 CEST	192.168.2.22	8.8.8.8	0xdeb5	Standard query (0)	www.artsenvoorwaarheid.nl	A (IP address)	IN (0x0001)
Jun 28, 2021 14:48:48.892786026 CEST	192.168.2.22	8.8.8.8	0x1e66	Standard query (0)	polyfill.io	A (IP address)	IN (0x0001)
Jun 28, 2021 14:48:48.895061016 CEST	192.168.2.22	8.8.8.8	0xe124	Standard query (0)	static.parastorage.com	A (IP address)	IN (0x0001)
Jun 28, 2021 14:48:49.034324884 CEST	192.168.2.22	8.8.8.8	0xe10c	Standard query (0)	static.wixstatic.com	A (IP address)	IN (0x0001)
Jun 28, 2021 14:48:49.668648005 CEST	192.168.2.22	8.8.8.8	0x5fc5	Standard query (0)	frog.wix.com	A (IP address)	IN (0x0001)
Jun 28, 2021 14:48:50.190984011 CEST	192.168.2.22	8.8.8.8	0x5437	Standard query (0)	en.wix.com	A (IP address)	IN (0x0001)
Jun 28, 2021 14:48:50.252559900 CEST	192.168.2.22	8.8.8.8	0xba95	Standard query (0)	browser.sentry-cdn.com	A (IP address)	IN (0x0001)
Jun 28, 2021 14:48:50.636857033 CEST	192.168.2.22	8.8.8.8	0xae1a	Standard query (0)	www.wix.com	A (IP address)	IN (0x0001)
Jun 28, 2021 14:48:50.870846987 CEST	192.168.2.22	8.8.8.8	0x471	Standard query (0)	sentry.wixpress.com	A (IP address)	IN (0x0001)
Jun 28, 2021 14:48:51.951693058 CEST	192.168.2.22	8.8.8.8	0xa0f9	Standard query (0)	fast.fonts.com	A (IP address)	IN (0x0001)
Jun 28, 2021 14:48:52.601972103 CEST	192.168.2.22	8.8.8.8	0x11f1	Standard query (0)	siteassets.parastorage.com	A (IP address)	IN (0x0001)
Jun 28, 2021 14:48:56.718661070 CEST	192.168.2.22	8.8.8.8	0xa3b8	Standard query (0)	4382365.fls.doubleclick.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 28, 2021 14:48:56.741353035 CEST	192.168.2.22	8.8.8.8	0x5a67	Standard query (0)	s.pinimg.com	A (IP address)	IN (0x0001)
Jun 28, 2021 14:48:56.744472027 CEST	192.168.2.22	8.8.8.8	0x4ea8	Standard query (0)	snap.licdn.com	A (IP address)	IN (0x0001)
Jun 28, 2021 14:48:56.752595901 CEST	192.168.2.22	8.8.8.8	0x6f91	Standard query (0)	connect.facebook.net	A (IP address)	IN (0x0001)
Jun 28, 2021 14:48:57.068099022 CEST	192.168.2.22	8.8.8.8	0x57ce	Standard query (0)	googleads.g.doubleclick.net	A (IP address)	IN (0x0001)
Jun 28, 2021 14:48:57.111110926 CEST	192.168.2.22	8.8.8.8	0xb462	Standard query (0)	px.ads.linkedin.com	A (IP address)	IN (0x0001)
Jun 28, 2021 14:48:57.215729952 CEST	192.168.2.22	8.8.8.8	0x6bb3	Standard query (0)	ct.pinterest.com	A (IP address)	IN (0x0001)
Jun 28, 2021 14:48:57.355221033 CEST	192.168.2.22	8.8.8.8	0x41e1	Standard query (0)	www.google.de	A (IP address)	IN (0x0001)
Jun 28, 2021 14:48:57.464163065 CEST	192.168.2.22	8.8.8.8	0x5bbd	Standard query (0)	adservice.google.de	A (IP address)	IN (0x0001)
Jun 28, 2021 14:48:58.115175962 CEST	192.168.2.22	8.8.8.8	0x9ae3	Standard query (0)	www.linkedin.com	A (IP address)	IN (0x0001)
Jun 28, 2021 14:49:00.042639017 CEST	192.168.2.22	8.8.8.8	0xe623	Standard query (0)	www.facebook.com	A (IP address)	IN (0x0001)
Jun 28, 2021 14:49:54.506321907 CEST	192.168.2.22	8.8.8.8	0x7df6	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 14:48:44.961555004 CEST	8.8.8.8	192.168.2.22	0xdeb5	No error (0)	www.artsenvoorwaarheid.nl	www179.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Jun 28, 2021 14:48:44.961555004 CEST	8.8.8.8	192.168.2.22	0xdeb5	No error (0)	www179.wixdns.net	balancer.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Jun 28, 2021 14:48:44.961555004 CEST	8.8.8.8	192.168.2.22	0xdeb5	No error (0)	balancer.wixdns.net	5f36b111-balancer.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Jun 28, 2021 14:48:44.961555004 CEST	8.8.8.8	192.168.2.22	0xdeb5	No error (0)	5f36b111-balancer.wixdns.net	td-balancer-euw2-6-109.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Jun 28, 2021 14:48:44.961555004 CEST	8.8.8.8	192.168.2.22	0xdeb5	No error (0)	td-balancer-euw2-6-109.wixdns.net		35.246.6.109	A (IP address)	IN (0x0001)
Jun 28, 2021 14:48:48.941302061 CEST	8.8.8.8	192.168.2.22	0x1e66	No error (0)	polyfill.io		151.101.129.26	A (IP address)	IN (0x0001)
Jun 28, 2021 14:48:48.941302061 CEST	8.8.8.8	192.168.2.22	0x1e66	No error (0)	polyfill.io		151.101.1.26	A (IP address)	IN (0x0001)
Jun 28, 2021 14:48:48.941302061 CEST	8.8.8.8	192.168.2.22	0x1e66	No error (0)	polyfill.io		151.101.193.26	A (IP address)	IN (0x0001)
Jun 28, 2021 14:48:48.941302061 CEST	8.8.8.8	192.168.2.22	0x1e66	No error (0)	polyfill.io		151.101.65.26	A (IP address)	IN (0x0001)
Jun 28, 2021 14:48:48.957878113 CEST	8.8.8.8	192.168.2.22	0xe124	No error (0)	static.parastorage.com	td-static-34-96-106-200.parastorage.com		CNAME (Canonical name)	IN (0x0001)
Jun 28, 2021 14:48:48.957878113 CEST	8.8.8.8	192.168.2.22	0xe124	No error (0)	td-static-34-96-106-200.parastorage.com		34.96.106.200	A (IP address)	IN (0x0001)
Jun 28, 2021 14:48:49.104295969 CEST	8.8.8.8	192.168.2.22	0xe10c	No error (0)	static.wixstatic.com	gcp.media-router.wixstatic.com		CNAME (Canonical name)	IN (0x0001)
Jun 28, 2021 14:48:49.104295969 CEST	8.8.8.8	192.168.2.22	0xe10c	No error (0)	gcp.media-router.wixstatic.com		34.102.176.152	A (IP address)	IN (0x0001)
Jun 28, 2021 14:48:49.724184990 CEST	8.8.8.8	192.168.2.22	0x5fc5	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 14:48:49.724184990 CEST	8.8.8.8	192.168.2.22	0x5fc5	No error (0)	bi-flogger-alb-ext-343643057.us-east-1.elb.amazonaws.com		34.231.78.0	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 28, 2021 14:48:49.724184990 CEST	8.8.8.8	192.168.2.22	0x5fc5	No error (0)	bi-flogger-alb-ext-343643057.us-east-1.elb.amazonaws.com		54.205.21.19	A (IP address)	IN (0x0001)
Jun 28, 2021 14:48:49.724184990 CEST	8.8.8.8	192.168.2.22	0x5fc5	No error (0)	bi-flogger-alb-ext-343643057.us-east-1.elb.amazonaws.com		34.202.88.78	A (IP address)	IN (0x0001)
Jun 28, 2021 14:48:49.724184990 CEST	8.8.8.8	192.168.2.22	0x5fc5	No error (0)	bi-flogger-alb-ext-343643057.us-east-1.elb.amazonaws.com		35.169.58.31	A (IP address)	IN (0x0001)
Jun 28, 2021 14:48:49.724184990 CEST	8.8.8.8	192.168.2.22	0x5fc5	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 14:48:49.724184990 CEST	8.8.8.8	192.168.2.22	0x5fc5	No error (0)	bi-flogger-alb-ext-343643057.us-east-1.elb.amazonaws.com		34.202.131.150	A (IP address)	IN (0x0001)
Jun 28, 2021 14:48:49.724184990 CEST	8.8.8.8	192.168.2.22	0x5fc5	No error (0)	bi-flogger-alb-ext-343643057.us-east-1.elb.amazonaws.com		34.193.74.105	A (IP address)	IN (0x0001)
Jun 28, 2021 14:48:49.724184990 CEST	8.8.8.8	192.168.2.22	0x5fc5	No error (0)	bi-flogger-alb-ext-343643057.us-east-1.elb.amazonaws.com		52.21.48.132	A (IP address)	IN (0x0001)
Jun 28, 2021 14:48:50.265002012 CEST	8.8.8.8	192.168.2.22	0x5437	No error (0)	en.wix.com	username.wix.com		CNAME (Canonical name)	IN (0x0001)
Jun 28, 2021 14:48:50.265002012 CEST	8.8.8.8	192.168.2.22	0x5437	No error (0)	username.wix.com	5f36b111-username.wix.com		CNAME (Canonical name)	IN (0x0001)
Jun 28, 2021 14:48:50.265002012 CEST	8.8.8.8	192.168.2.22	0x5437	No error (0)	5f36b111-username.wix.com	td-username-euw2-6-109.wix.com		CNAME (Canonical name)	IN (0x0001)
Jun 28, 2021 14:48:50.265002012 CEST	8.8.8.8	192.168.2.22	0x5437	No error (0)	td-username-euw2-6-109.wix.com		35.246.6.109	A (IP address)	IN (0x0001)
Jun 28, 2021 14:48:50.298788071 CEST	8.8.8.8	192.168.2.22	0xba95	No error (0)	browser.sentry-cdn.com		151.101.194.217	A (IP address)	IN (0x0001)
Jun 28, 2021 14:48:50.298788071 CEST	8.8.8.8	192.168.2.22	0xba95	No error (0)	browser.sentry-cdn.com		151.101.66.217	A (IP address)	IN (0x0001)
Jun 28, 2021 14:48:50.298788071 CEST	8.8.8.8	192.168.2.22	0xba95	No error (0)	browser.sentry-cdn.com		151.101.2.217	A (IP address)	IN (0x0001)
Jun 28, 2021 14:48:50.298788071 CEST	8.8.8.8	192.168.2.22	0xba95	No error (0)	browser.sentry-cdn.com		151.101.130.217	A (IP address)	IN (0x0001)
Jun 28, 2021 14:48:50.695804119 CEST	8.8.8.8	192.168.2.22	0xae1a	No error (0)	www.wix.com	wwworigin.wix.com		CNAME (Canonical name)	IN (0x0001)
Jun 28, 2021 14:48:50.695804119 CEST	8.8.8.8	192.168.2.22	0xae1a	No error (0)	wwworigin.wix.com	163.www.sv5.wix.com		CNAME (Canonical name)	IN (0x0001)
Jun 28, 2021 14:48:50.695804119 CEST	8.8.8.8	192.168.2.22	0xae1a	No error (0)	163.www.sv5.wix.com		185.230.61.163	A (IP address)	IN (0x0001)
Jun 28, 2021 14:48:50.918550014 CEST	8.8.8.8	192.168.2.22	0x471	No error (0)	sentry.wixpress.com	sentry-nlb-e70282e8a06dcc98.elb.us-east-1.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jun 28, 2021 14:48:50.918550014 CEST	8.8.8.8	192.168.2.22	0x471	No error (0)	sentry-nlb-e70282e8a06dcc98.elb.us-east-1.amazonaws.com		52.2.188.208	A (IP address)	IN (0x0001)
Jun 28, 2021 14:48:52.015191078 CEST	8.8.8.8	192.168.2.22	0xa0f9	No error (0)	fast.fonts.com		104.17.71.188	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 28, 2021 14:48:52.015191078 CEST	8.8.8.8	192.168.2.22	0xa0f9	No error (0)	fast.fonts.com		104.17.70.188	A (IP address)	IN (0x0001)
Jun 28, 2021 14:48:52.690316916 CEST	8.8.8.8	192.168.2.22	0x11f1	No error (0)	siteassets.parastorage.com	static.parastorage.com		CNAME (Canonical name)	IN (0x0001)
Jun 28, 2021 14:48:52.690316916 CEST	8.8.8.8	192.168.2.22	0x11f1	No error (0)	static.parastorage.com	td-static-34-96-106-200.parastorage.com		CNAME (Canonical name)	IN (0x0001)
Jun 28, 2021 14:48:52.690316916 CEST	8.8.8.8	192.168.2.22	0x11f1	No error (0)	td-static-34-96-106-200.parastorage.com		34.96.106.200	A (IP address)	IN (0x0001)
Jun 28, 2021 14:48:56.784737110 CEST	8.8.8.8	192.168.2.22	0xa3b8	No error (0)	4382365.fls.doubleclick.net	dart.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Jun 28, 2021 14:48:56.784737110 CEST	8.8.8.8	192.168.2.22	0xa3b8	No error (0)	dart.l.doubleclick.net		142.250.185.198	A (IP address)	IN (0x0001)
Jun 28, 2021 14:48:56.800708055 CEST	8.8.8.8	192.168.2.22	0x4ea8	No error (0)	snap.licdn.com	wildcard.licdn.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jun 28, 2021 14:48:56.803028107 CEST	8.8.8.8	192.168.2.22	0x5a67	No error (0)	s.pinimg.com	s-pinimg-com.gslb.pinterest.com		CNAME (Canonical name)	IN (0x0001)
Jun 28, 2021 14:48:56.803028107 CEST	8.8.8.8	192.168.2.22	0x5a67	No error (0)	s-pinimg-com.gslb.pinterest.com	2-01-37d2-0006.cdx.cedexis.net		CNAME (Canonical name)	IN (0x0001)
Jun 28, 2021 14:48:56.812841892 CEST	8.8.8.8	192.168.2.22	0x6f91	No error (0)	connect.facebook.net	scontent.xx.fbcdn.net		CNAME (Canonical name)	IN (0x0001)
Jun 28, 2021 14:48:56.812841892 CEST	8.8.8.8	192.168.2.22	0x6f91	No error (0)	scontent.xx.fbcdn.net		157.240.17.15	A (IP address)	IN (0x0001)
Jun 28, 2021 14:48:57.124691963 CEST	8.8.8.8	192.168.2.22	0x57ce	No error (0)	googleads.g.doubleclick.net		216.58.212.162	A (IP address)	IN (0x0001)
Jun 28, 2021 14:48:57.170702934 CEST	8.8.8.8	192.168.2.22	0xb462	No error (0)	px.ads.linkedin.com	mix.linkedin.com		CNAME (Canonical name)	IN (0x0001)
Jun 28, 2021 14:48:57.170702934 CEST	8.8.8.8	192.168.2.22	0xb462	No error (0)	mix.linkedin.com	glb-na.mix.linkedin.com		CNAME (Canonical name)	IN (0x0001)
Jun 28, 2021 14:48:57.170702934 CEST	8.8.8.8	192.168.2.22	0xb462	No error (0)	glb-na.mix.linkedin.com	pop-esv5.mix.linkedin.com		CNAME (Canonical name)	IN (0x0001)
Jun 28, 2021 14:48:57.170702934 CEST	8.8.8.8	192.168.2.22	0xb462	No error (0)	pop-esv5.mix.linkedin.com		108.174.11.37	A (IP address)	IN (0x0001)
Jun 28, 2021 14:48:57.300431967 CEST	8.8.8.8	192.168.2.22	0x6bb3	No error (0)	ct.pinterest.com	www.pinterest.com		CNAME (Canonical name)	IN (0x0001)
Jun 28, 2021 14:48:57.300431967 CEST	8.8.8.8	192.168.2.22	0x6bb3	No error (0)	www.pinterest.com	www-pinterest-com.gslb.pinterest.com		CNAME (Canonical name)	IN (0x0001)
Jun 28, 2021 14:48:57.300431967 CEST	8.8.8.8	192.168.2.22	0x6bb3	No error (0)	www-pinterest-com.gslb.pinterest.com	2-01-37d2-0018.cdx.cedexis.net		CNAME (Canonical name)	IN (0x0001)
Jun 28, 2021 14:48:57.419599056 CEST	8.8.8.8	192.168.2.22	0x41e1	No error (0)	www.google.de		142.250.186.35	A (IP address)	IN (0x0001)
Jun 28, 2021 14:48:57.532418966 CEST	8.8.8.8	192.168.2.22	0x5bbd	No error (0)	adservice.google.de	pagead46.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Jun 28, 2021 14:48:57.532418966 CEST	8.8.8.8	192.168.2.22	0x5bbd	No error (0)	pagead46.l.doubleclick.net		142.250.185.194	A (IP address)	IN (0x0001)
Jun 28, 2021 14:48:58.163173914 CEST	8.8.8.8	192.168.2.22	0x9ae3	No error (0)	www.linkedin.com	www-linkedin-com.l-0005.l-msedge.net		CNAME (Canonical name)	IN (0x0001)
Jun 28, 2021 14:49:00.104525089 CEST	8.8.8.8	192.168.2.22	0xe623	No error (0)	www.facebook.com	star-mini.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)
Jun 28, 2021 14:49:00.104525089 CEST	8.8.8.8	192.168.2.22	0xe623	No error (0)	star-mini.c10r.facebook.com		157.240.17.35	A (IP address)	IN (0x0001)
Jun 28, 2021 14:49:54.563241959 CEST	8.8.8.8	192.168.2.22	0x7df6	No error (0)	static.parastorage.com	td-static-34-96-106-200.parastorage.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 28, 2021 14:49:54.563241959 CEST	8.8.8.8	192.168.2.22	0x7df6	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	192.168.2.22	49165	35.246.6.109	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jun 28, 2021 14:48:45.601022959 CEST	1	OUT	GET / HTTP/1.1 Accept: text/html, application/xhtml+xml, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: www.artsenvoorwaarheid.nl DNT: 1 Connection: Keep-Alive
Jun 28, 2021 14:48:45.678210974 CEST	2	IN	HTTP/1.1 301 Moved Permanently Date: Mon, 28 Jun 2021 12:48:45 GMT Content-Length: 0 Connection: keep-alive location: https://www.artsenvoorwaarheid.nl/ strict-transport-security: max-age=120 Age: 5279 Server-Timing: cache;desc=hit, varnish;desc=hit, dc;desc=euw2 X-Seen-By: sHU62EDOGnH2FBkJkG/Wx8EeXWsWdHrhlvbxtlynkVh6aqXNQlfs1DVxLIoL9NTV,qquldgcFrj2n04 6g4RNSVJWsHd48QfxhscEwgNQIOKxYgeUJqUXtid+86vZww+nL,2d58ifebGbosy5xc+FRali8T5T5cmIo0vofyNYy rb+RrXfz1Q7kr3TTe9b/3mmKBz0YAkIZfvLTU62dP8Trm7wsESVK8cilF8hHIhzK9mL8=,2UNV7KOq4oGjA5+PKsX4 7JpxpkqGEXQxSEKO4wY/fJs= Cache-Control: no-cache X-Wix-Request-Id: 1624884525.647535788012131730 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 14:48:45.851372004 CEST	35.246.6.109	443	192.168.2.22	49167	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	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					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 14:48:49.036014080 CEST	151.101.129.26	443	192.168.2.22	49169	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	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					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 14:48:49.041692019 CEST	34.96.106.200	443	192.168.2.22	49172	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	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					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 14:48:49.041897058 CEST	34.96.106.200	443	192.168.2.22	49171	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	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					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 14:48:49.043240070 CEST	34.96.106.200	443	192.168.2.22	49173	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	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					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 14:48:49.050586939 CEST	34.96.106.200	443	192.168.2.22	49176	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	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					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 14:48:49.050776958 CEST	34.96.106.200	443	192.168.2.22	49174	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	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					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 14:48:49.052115917 CEST	34.96.106.200	443	192.168.2.22	49175	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	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					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 14:48:49.053569078 CEST	151.101.129.26	443	192.168.2.22	49170	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	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					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 14:48:49.193346024 CEST	34.102.176.152	443	192.168.2.22	49178	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	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					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 14:48:49.206100941 CEST	34.102.176.152	443	192.168.2.22	49177	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	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					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 14:48:50.005373955 CEST	35.246.6.109	443	192.168.2.22	49183	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	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					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		
Jun 28, 2021 14:48:50.036062956 CEST	34.231.78.0	443	192.168.2.22	49181	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	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					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 14:48:50.039561033 CEST	34.231.78.0	443	192.168.2.22	49182	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	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					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 14:48:50.390137911 CEST	151.101.194.217	443	192.168.2.22	49186	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	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					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 14:48:50.392808914 CEST	151.101.194.217	443	192.168.2.22	49187	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	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					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 14:48:50.401460886 CEST	35.246.6.109	443	192.168.2.22	49185	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	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					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 14:48:50.404387951 CEST	35.246.6.109	443	192.168.2.22	49184	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	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					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 14:48:51.078758001 CEST	185.230.61.163	443	192.168.2.22	49188	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	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					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 14:48:51.121784925 CEST	185.230.61.163	443	192.168.2.22	49189	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	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					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 14:48:51.242650986 CEST	52.2.188.208	443	192.168.2.22	49190	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=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	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					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 14:48:51.243237019 CEST	52.2.188.208	443	192.168.2.22	49191	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	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					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 14:48:51.356890917 CEST	52.2.188.208	443	192.168.2.22	49192	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	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					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 14:48:52.107820034 CEST	104.17.71.188	443	192.168.2.22	49193	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	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					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 14:48:52.116864920 CEST	104.17.71.188	443	192.168.2.22	49194	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	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					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 14:48:52.808414936 CEST	34.96.106.200	443	192.168.2.22	49196	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	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					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 14:48:52.810754061 CEST	34.96.106.200	443	192.168.2.22	49197	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	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					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
					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 14:48:56.891537905 CEST	142.250.185.198	443	192.168.2.22	49202	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	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					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 14:48:56.891802073 CEST	157.240.17.15	443	192.168.2.22	49211	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	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					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 14:48:56.893003941 CEST	142.250.185.198	443	192.168.2.22	49204	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	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					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 14:48:56.893078089 CEST	157.240.17.15	443	192.168.2.22	49212	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	Wed Aug 25 01:59:59 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					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 14:48:57.211492062 CEST	216.58.212.162	443	192.168.2.22	49214	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	Mon Aug 23 03:33:25 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					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 14:48:57.222887993 CEST	216.58.212.162	443	192.168.2.22	49215	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	Mon Aug 23 03:33:25 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					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 14:48:57.223644018 CEST	216.58.212.162	443	192.168.2.22	49216	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	Mon Aug 23 03:33:25 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					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		

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 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 14:48:57.525665998 CEST	142.250.186.35	443	192.168.2.22	49227	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	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					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 14:48:57.526021957 CEST	142.250.186.35	443	192.168.2.22	49228	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	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					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 14:48:57.596683979 CEST	108.174.11.37	443	192.168.2.22	49218	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	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					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 14:48:57.609415054 CEST	108.174.11.37	443	192.168.2.22	49217	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	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					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		

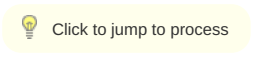
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jun 28, 2021 14:48:57.639417887 CEST	142.250.185.194	443	192.168.2.22	49230	CN=*.google.de CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust 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 07:18:47 CEST 2021 Thu Aug 13 02:00:42 CEST 2020 Fri Jun 19 02:00:42 CEST 2020	Mon Aug 23 07:18:46 CEST 2021 Thu Sep 30 02:00:42 CEST 2027 Fri Jan 28 01:00:42 CET 2028	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					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 14:48:57.642172098 CEST	142.250.185.194	443	192.168.2.22	49229	CN=*.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 07:18:47 CEST 2021 Thu Aug 13 02:00:42 CEST 2020 Fri Jun 19 02:00:42 CEST 2020	Mon Aug 23 07:18:46 CEST 2021 Thu Sep 30 02:00:42 CEST 2027 Fri Jan 28 01:00:42 CET 2028	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					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 14:49:00.175213099 CEST	157.240.17.35	443	192.168.2.22	49234	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	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					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 14:49:00.177207947 CEST	157.240.17.35	443	192.168.2.22	49235	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	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					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 14:49:54.652025938 CEST	34.96.106.200	443	192.168.2.22	49238	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	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					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



System Behavior

Analysis Process: WINWORD.EXE PID: 2480 Parent PID: 584

General

Start time:	14:47:32
Start date:	28/06/2021
Path:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding
Imagebase:	0x13f730000
File size:	1424032 bytes
MD5 hash:	95C38D04597050285A18F66039EDB456
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: 3044 Parent PID: 584

General

Start time:	14:48:01
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:	0x13f6a0000
File size:	814288 bytes
MD5 hash:	4EB098135821348270F27157F7A84E65
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Analysis Process: iexplore.exe PID: 3032 Parent PID: 3044

General

Start time:	14:48:02
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:3044 CREDAT:275457 /prefetch:2
Imagebase:	0x1230000
File size:	815304 bytes
MD5 hash:	8A590F790A98F3D77399BE457E01386A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities — Show Windows behavior

Registry Activities — Show Windows behavior

Disassembly