ID: 412519
Cookbook: browseurl.jbs
Time: 18:44:22
Date: 12/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

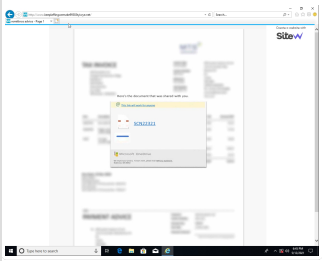
Analysis Report http://keeplaffingwemake99383tyiwye.n…

Overview

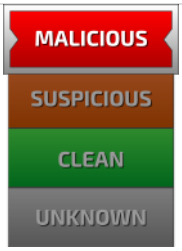
General Information

Sample URL:	http://keeplaffingwemake99383tyiwye.net/
Analysis ID:	412519
Infos:	

Most interesting Screenshot:



Detection



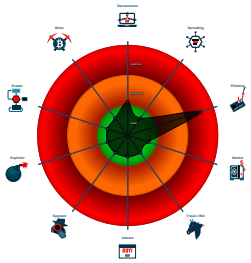
HTMLPhisher

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: 6396 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6484 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6396 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

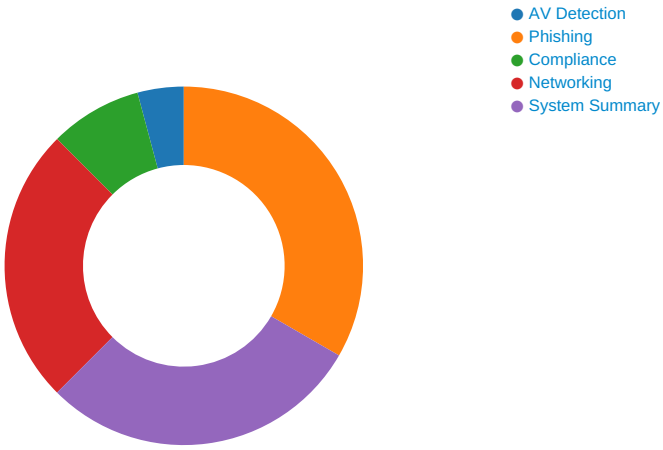
Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1_____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

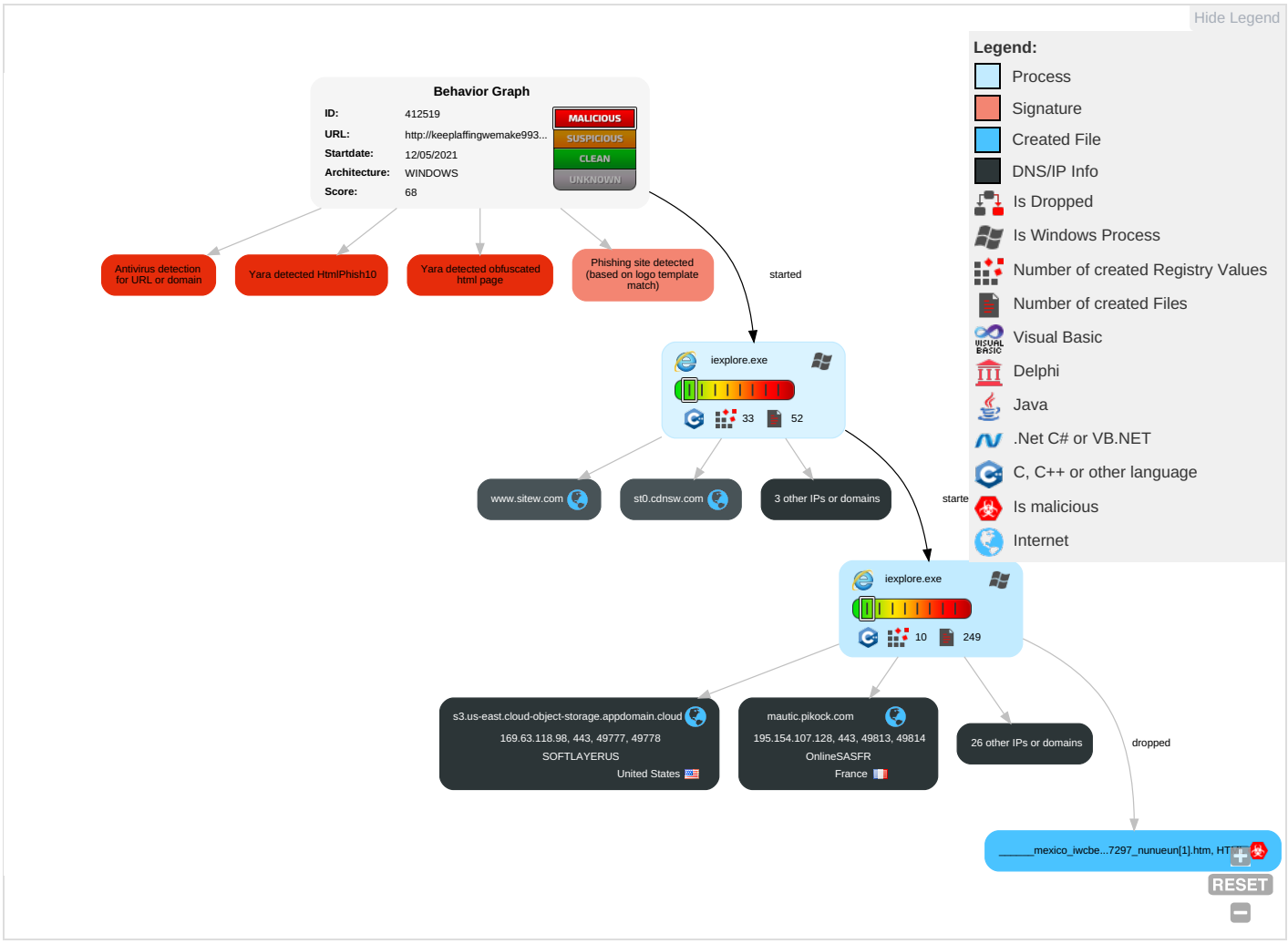
Yara detected obfuscated html page

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

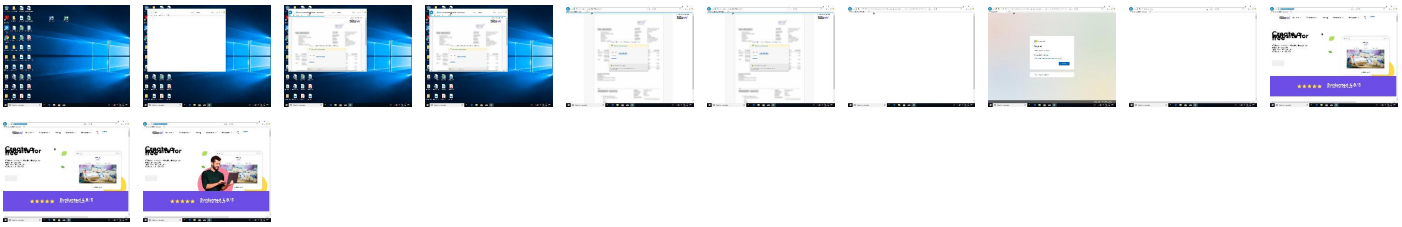
Behavior Graph

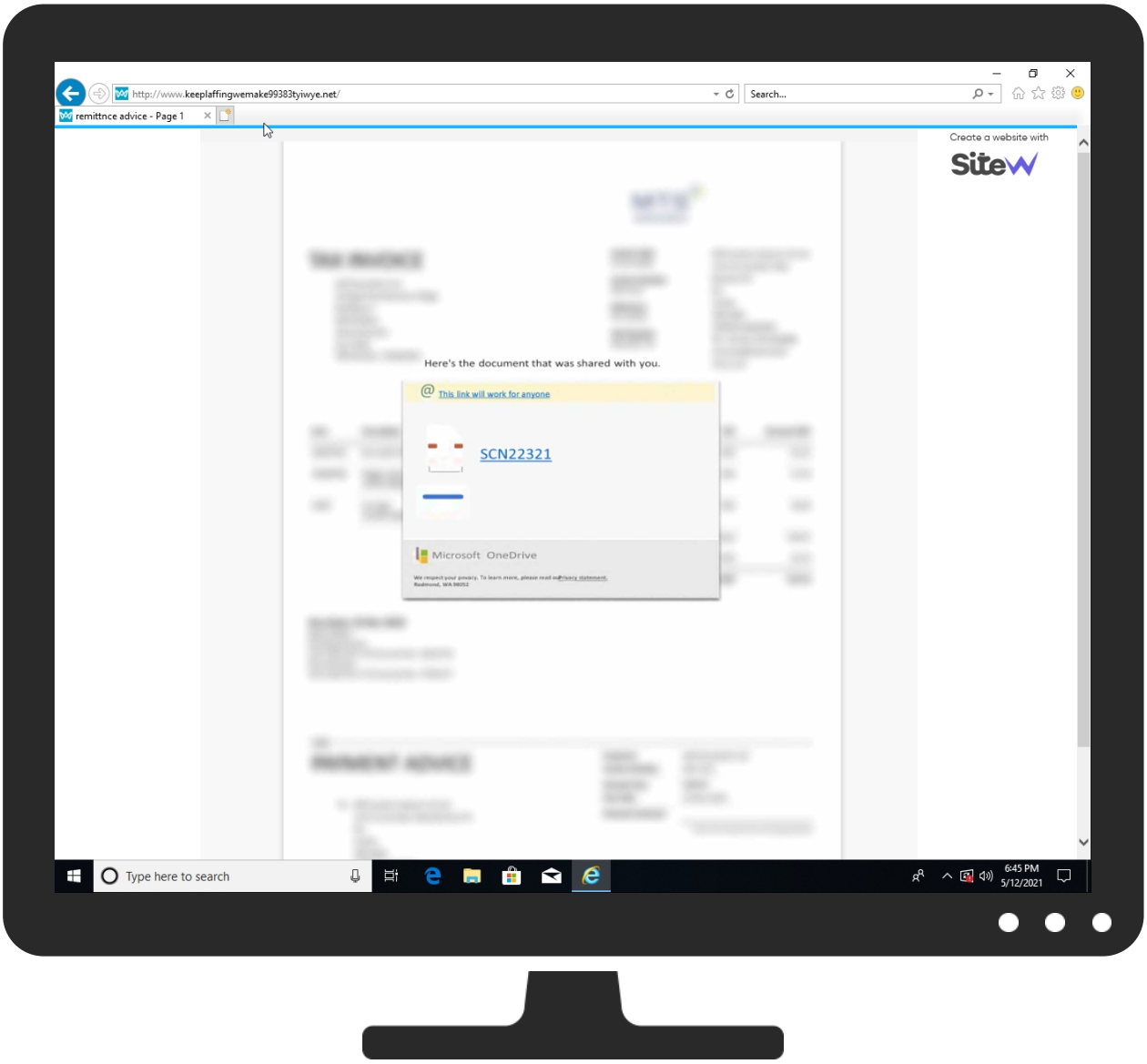


Screenshots

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%	Virustotal		Browse
http://keeplaffingwemake99383tyiwye.net/	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
cs1100.wpc.omegacdn.net	0%	Virustotal		Browse
ssl.sitew.org	0%	Virustotal		Browse

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 Engineering	
http://https://ssl.sitew.org/images/blog/templates/v2/52_mobile.jpg	0%	Avira URL Cloud	safe	
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://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://www.keeplaffingwemake99383tyiwye.net/TMEOW	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	

Source	Detection	Scanner	Label	Link
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	
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	

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	142.250.184.195	true	false		high
d1r3aid9v9xqmp.cloudfront.net	13.225.74.42	true	false		high
cs1100.wpc.omegacdn.net	152.199.23.37	true	false	• 0%, Virustotal, Browse	unknown
ssl.sitew.org	188.165.33.133	true	false	• 0%, Virustotal, Browse	unknown
stats.l.doubleclick.net	64.233.167.157	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
st0.bp.cdnsw.com	188.165.33.133	true	false		unknown
mfs0.cdnsw.com	46.105.199.115	true	false		unknown
www.en.sitew.com	178.32.55.155	true	false		high
googleads.g.doubleclick.net	142.250.186.34	true	false		high
cdnjs.cloudflare.com	104.16.18.94	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.sitew.com/json/site_owner/?callback=jQuery112406271402232648 69_1620837913434&site=www.keeplaffingwemake99383tyiwye.net&_=1620837913435	false		high
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 Engineering	unknown

Name	Malicious	Antivirus Detection	Reputation
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

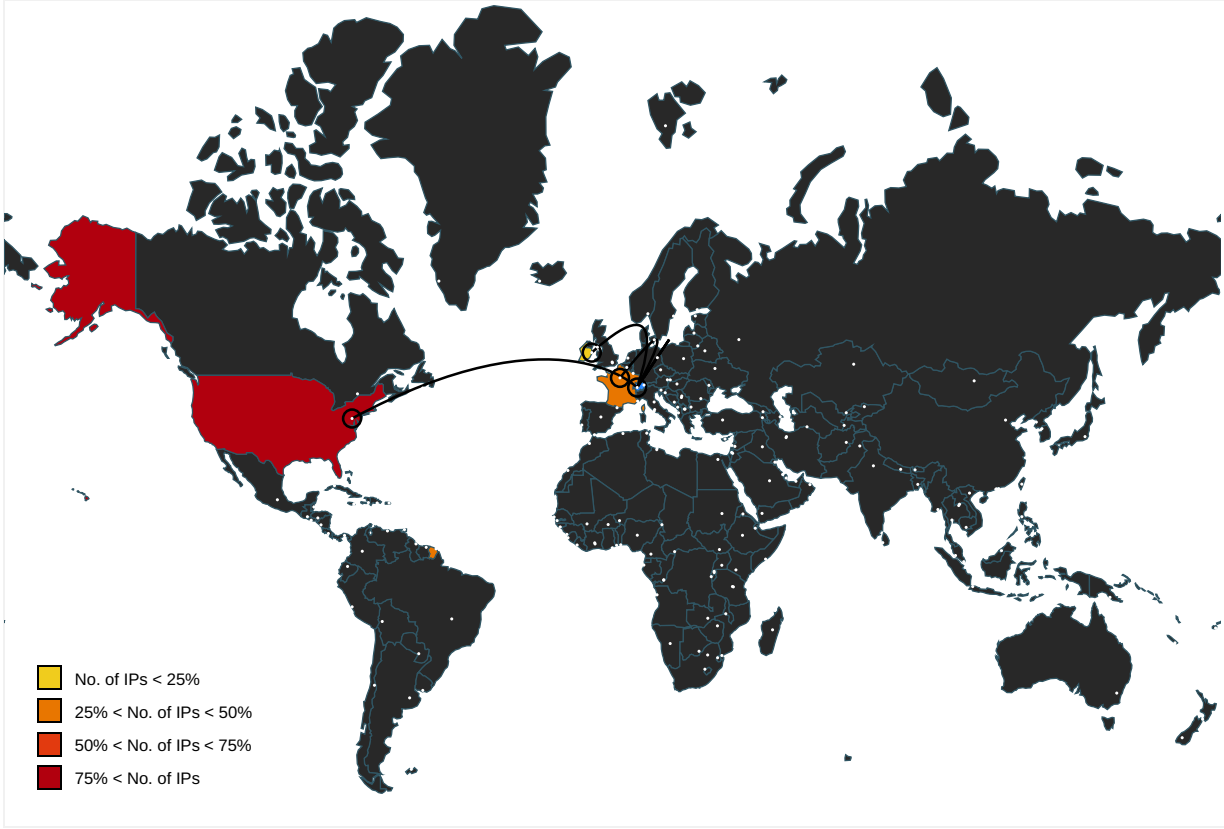
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://player.vimeo.com/api/player.js	TXMZ4AWB.htm.3.dr	false		high
http://https://ssl.sitew.org/images/blog/templates/v2/52_mobile.jpg	HC9WYB3E.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://ssl.sitew.org/images/blog/landing/2021/home-reassurance-1-rapidite.webp	HC9WYB3E.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://ssl.sitew.org/images/blog/landing/2021/clients/home-typo-clients-asso.webp	HC9WYB3E.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.sitew.com/log/save_session?split=iH1lO3nn22XnmA%7CGd3gbyVWnBgnQWGZkhl4dy40muLDCWPWhI	~DFE49EA245F4FFB57B.TMP.1.dr	false		high
http://https://ssl.sitew.org/images/blog/landing/2021/templates/picto_site_pro_home_sitew.svg	HC9WYB3E.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://ssl.sitew.org/images/blog/templates/v2/32_mobile.jpg	HC9WYB3E.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://ssl.sitew.org/images/blog/logos/2021_wide.svg	HC9WYB3E.htm.3.dr, TXMZ4AWB.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://f.vimeocdn.com/js/froogaloop2.min.js	mtc[1].js.3.dr	false		high
http://https://ssl.sitew.org/images/blog/landing/2021/product_store.png	HC9WYB3E.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://rb.bp.cdnsw.com	TXMZ4AWB.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://st0.cdnsw.com/logo/MtxgY0xq7ZaF%7CDUvJtZIe53rcKjBFj1eQJPNWVo5Jw754tHoCVffmfcn4wJuaxIE.png	HC9WYB3E.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://ssl.sitew.org/images/blog/landing/2021/clients/home-typo-clients-indiv.webp	HC9WYB3E.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://ssl.sitew.org/images/blog/welcome/icons_menu/2021/contact.png	HC9WYB3E.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.en.sitew.com/Starting-a-blog	HC9WYB3E.htm.3.dr	false		high
http://https://ssl.sitew.org/images/blog/templates/v2/33_desktop.jpg	HC9WYB3E.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.en.sitew.com/tCreate	~DFE49EA245F4FFB57B.TMP.1.dr	false		high
http://https://ssl.sitew.org/images/blog/templates/v2/32_desktop.jpg	HC9WYB3E.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://www.keeplaffingwemake99383tyiwye.net/265cgilogon.s3.us-east.cloud-obje	{69FDE9A5-B341-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://mfs0.cdnsw.com	TXMZ4AWB.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://ssl.sitew.org/images/blog/templates/v2/31_desktop.jpg	HC9WYB3E.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://twitter.com/intent/tweet?url=	en-landing-ec980e52dfd088a76959023999079f96[1].js.3.dr	false		high
http://https://ssl.sitew.org/images/blog/landing/2021/home-green-illu.webp	HC9WYB3E.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://stats.g.doubleclick.net/j/collect	analytics[1].js.3.dr	false		high
http://https://platform.twitter.com/embed/index.html?	en-landing-ec980e52dfd088a76959023999079f96[1].js.3.dr, TXMZ4AWB.htm.3.dr	false		high
http://scripts.sil.org/OFLWeightRomanItalic	QGY_z_wNahGAdqQ43RhVcIgYT2Xz5u32K0nXBi8Jow[1].ttf.3.dr	false		high
http://https://ssl.sitew.org/images/blog/landing/2021/home-accompagnement-efficace.webp	HC9WYB3E.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://ssl.sitew.org/images/blog/landing/2021/templates/picto_site_blog_home_sitew.svg	HC9WYB3E.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://ssl.sitew.org/images/blog/landing/2021/home-fonctionnalites-photo.png	HC9WYB3E.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://w.soundcloud.com/player/api.js	TXMZ4AWB.htm.3.dr	false		high
http://https://ssl.sitew.org/images/blog/landing/2021/product_ndd.png	HC9WYB3E.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://github.com/weiweihuanghuang/Work-Sans)Work	QGY_z_wNahGAdqQ43RhVcIgYT2Xz5u32K0nXBi8Jow[1].ttf.3.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://ssl.sitew.org/images/blog/templates/v2/33_mobile.jpg	HC9WYB3E.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://ssl.sitew.org/images/blog/templates/v2/53_mobile.jpg	HC9WYB3E.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://connect.soundcloud.com/sdk.js	TXMZ4AWB.htm.3.dr	false		high
http://https://schema.org	HC9WYB3E.htm.3.dr	false		high
http://https://unpkg.com/dropbox/dist/Dropbox-sdk.min.js	TXMZ4AWB.htm.3.dr	false		high
http://brandon.aaron.sh)	jquery.mousewheel.min[1].js.3.dr	false	• Avira URL Cloud: safe	low
http://https://ssl.sitew.org/images/blog/landing/2021/templates/picto_site_asso_home_sitew.svg	HC9WYB3E.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.sitew.com/log/save_session?split=iH1lO3nn22XnmA	~DFE49EA245F4FFB57B.TMP.1.dr, HC9WYB3E.htm.3.dr	false		high
http://https://ssl.sitew.org/images/blog/landing/2021/top/fr/leaf_2.png	HC9WYB3E.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://mediaelementjs.com/	mtc[1].js.3.dr	false		high
http://https://ssl.sitew.org/images/blog/landing/2021/templates/picto_site_portfolio_home_sitew.svg	HC9WYB3E.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://www.keeplaffingwemake99383tyiwye.net/2wemake99383tyiwye.net/Root	{69FDE9A5-B341-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://ssl.sitew.org/images/blog/templates/v2/38_desktop.jpg	HC9WYB3E.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://st0.cdnsw.com/assets/gilroy/gilroy-medium-31b466a996548760e5ed85b12e182bc9.woff2	HC9WYB3E.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://ra0.cdnsw.com/cc0/	TXMZ4AWB.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://ssl.sitew.org/images/blog/editor_icons/design_panel/gt_icon_	TXMZ4AWB.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://outlook0ffice365cgilogon.s3.us-east.cloud-object-storage.appdomain.cloud/Root	{69FDE9A5-B341-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://ssl.sitew.org/images/blog/landing/2021/animation_en.mp4	HC9WYB3E.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://ssl.sitew.org/images/blog/templates/v2/51_mobile.jpg	HC9WYB3E.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://ssl.sitew.org/images/blog/welcome/icons_menu/2021/templates.png	HC9WYB3E.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://ssl.sitew.org/images/blog/landing/2021/home-reassurance-2-sites.webp	HC9WYB3E.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://www.keeplaffingwemake99383tyiwye.net/favicon.ico~	imagestore.dat.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://ssl.sitew.org/images/blog/templates/v2/21_mobile.jpg	HC9WYB3E.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://ssl.sitew.org/images/blog/landing/2021/home-google-simple.webp	HC9WYB3E.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://ssl.sitew.org/images/blog/templates/v2/12_mobile.jpg	HC9WYB3E.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://ssl.sitew.org/images/blog/templates/v2/31_mobile.jpg	HC9WYB3E.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://st0.cdnsw.com/assets/precompile/cpts/common/icons-7d2d8846fab8b0d98519a12a90295eb6.css	en-landing-ec980e52dfd088a76959023999079f96[1].js.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.en.sitew.com/	TXMZ4AWB.htm.3.dr	false		high
http://https://ssl.sitew.org/images/blog/landing/2021/mascotte_pos_1_s2.webp	HC9WYB3E.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://ssl.sitew.org/images/blog/landing/2021/clients/home-typo-clients-pro.webp	HC9WYB3E.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://www.keeplaffingwemake99383tyiwye.net/TMEOW	~DFE49EA245F4FFB57B.TMP.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://st0.cdnsw.com/assets/gilroy/gilroy-regular-f1ecb849891a09cae3f3d560b7ed2e08.woff	HC9WYB3E.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://use.typekit.net	webfont[1].js.3.dr	false		high
http://https://lb.affilae.com	ae-v3.2[1].js.3.dr	false		high
http://https://ssl.sitew.org/images/blog/landing/2021/top/en/browser_1.webp	HC9WYB3E.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://twitter.com/intent/tweet?text=	TXMZ4AWB.htm.3.dr	false		high
http://https://ssl.sitew.org/images/blog/landing/2021/home-google-argent.webp	HC9WYB3E.htm.3.dr, en-landing-ec980e52dfd088a76959023999079f96[1].js.3.dr	false	• Avira URL Cloud: safe	unknown
http://www.keeplaffingwemake99383tyiwye.net/z	~DFE49EA245F4FFB57B.TMP.1.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://ssl.sitew.org/images/blog/templates/v2/4_mobile.jpg	HC9WYB3E.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://ssl.sitew.org/images/blog/templates/v2/27_mobile.jpg	HC9WYB3E.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://es.sitew.com/	HC9WYB3E.htm.3.dr	false		high
http://https://ssl.sitew.org/images/blog/landing/2021/home-reassurance-2-anniversaire.webp	HC9WYB3E.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://ssl.sitew.org/images/blog/landing/2021/product_blog.png	HC9WYB3E.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://schema.org	TXMZ4AWB.htm.3.dr	false		high
http://https://ssl.sitew.org/images/blog/templates/v2/53_desktop.jpg	HC9WYB3E.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://www.keeplaffingwemake99383tyiwye.net	TXMZ4AWB.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://ssl.sitew.org/images/blog/templates/v2/21_desktop.jpg	HC9WYB3E.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://ssl.sitew.org/images/blog/landing/2021/support_team.webp	HC9WYB3E.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://ssl.sitew.org/images/blog/templates/v2/54_mobile.jpg	HC9WYB3E.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://www.keeplaffingwemake99383tyiwye.net/2om/ilogon.s3.us-east.cloud-obje	{69FDE9A5-B341-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://ssl.sitew.org/images/blog/templates/v2/51_desktop.jpg	HC9WYB3E.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://connect.facebook.net/en_US/all.js	en-landing-ec980e52dfd088a76959023999079f96[1].js.3.dr	false		high
http://https://ssl.sitew.org/images/blog/landing/2021/product_background_front3.webp	HC9WYB3E.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.en.sitew.com/Starting-an-online-business	HC9WYB3E.htm.3.dr	false		high
http://https://ssl.sitew.org/images/blog/landing/2021/product_vitrine.png	HC9WYB3E.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.en.sitew.com/Create-showcase-page	HC9WYB3E.htm.3.dr	false		high
http://https://ssl.sitew.org/images/blog/landing/2021/templates/picto_site_perso_home_sitew.svg	HC9WYB3E.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://st0.cdnsw.com/assets/gilroy/gilroy-regular-2574ec89d9fd02ee8503459b281d2e80.woff2	HC9WYB3E.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://ssl.sitew.org/images/blog/landing/2021/browser_multiBloc.svg	HC9WYB3E.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://ssl.sitew.org/images/blog/templates/v2/49_mobile.jpg	HC9WYB3E.htm.3.dr	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.250.184.195	www.google.de	United States		15169	GOOGLEUS	false
142.250.186.34	googleads.g.doubleclick.net	United States		15169	GOOGLEUS	false
142.250.186.67	www.google.ch	United States		15169	GOOGLEUS	false
46.105.199.115	st0.cdnsw.com	France		16276	OVHFR	false
64.233.167.157	stats.l.doubleclick.net	United States		15169	GOOGLEUS	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
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
104.16.18.94	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	412519
Start date:	12.05.2021
Start time:	18:44:22
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 18s
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:	10
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@3/211@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 • Excluded IPs from analysis (whitelisted): 40.88.32.150, 131.253.33.200, 13.107.22.200, 92.122.145.220, 13.64.90.137, 88.221.62.148, 142.250.184.238, 142.250.186.131, 142.250.186.138, 142.250.184.234, 20.82.210.154, 69.16.175.42, 69.16.175.10, 152.199.19.161, 92.122.213.194, 92.122.213.247, 142.250.185.162, 13.107.13.80, 142.250.184.196 • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • 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, store-images.s-microsoft.com-c.edgekey.net, iris-de-prod-azsc-neu-b.northeurope.cloudapp.azure.com, a1449.dscg2.akamai.net, arc.msn.com, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, skypedataprdcoleus15.cloudapp.net, e12564.dspb.akamaiedge.net, go.microsoft.com, www-bing-com.dual-a-0001.a-msedge.net, arc.trafficmanager.net, www.google.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, api-bing-com.e-0001.e-msedge.net, www.google-analytics.com, www.bing.com, e-0001.dc-msedge.net, skypedataprdcolwus17.cloudapp.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, aadcdnoriginneu.ec.azureedge.net, lgincdnvzeuno.azureedge.net, dual-a-0001.dc-msedge.net, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, 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.

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\E5F0NRSV\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):	4.88758291424045
Encrypted:	false
SSDEEP:	6:JFK1rUFWqGk6aEls3vqu3aV8aEls3b18qu3aV8aElqb:JsrUdG37u3483Eu3483g
MD5:	8DD5636D53B2E7F947086FF61EA5C2FA
SHA1:	2D0E8A9B931F93A28ECEE6736AC8AB987CC2FB1D
SHA-256:	B103E1D6DC6A19CEE6C56807D7065E0C9D686310F510D0D80CAE0058EDA70956
SHA-512:	600C2074219F5C07F84AD9C8F4B555DB4027F48352515AECF8CB0DE1AF974AAFBCA27C9D716E8EAEED2FA0A06B827748562BA58CCC8CCC7F6E012496FE36B4 78
Malicious:	false
Reputation:	low
Preview:	<root></root><root><item name="mtc_id" value="1312936" ltime="1113449840" htime="30885710" /><item name="mtc_sid" value="aehw7ahtc805x56r0jydy2g" ltim e="1113449840" htime="30885710" /><item name="mautic_device_id" value="aehw7ahtc805x56r0jydy2g" ltime="1113449840" htime="30885710" /></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{69FDE9A3-B341-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8509693370606257
Encrypted:	false
SSDEEP:	192:rrZYZg28WdtciffBfzM8nBnNDOsfUBOjX:r943rnxyYddt
MD5:	C2F56E6D75D06BAE6EE4AF6046C9F059
SHA1:	B08A98ABFBDE16774C45F988E130C4F64CFD4111
SHA-256:	D5857D73C8A234A080D2B1BAFD214A46740E2C6876F2B7DC7547E4370CB760BC
SHA-512:	0B3A3D3B4C75BD092FA127A16BD7EA5FD67ABFDE23781A1BEBC293D566DE83B85E8958E10B6698B449F8DF4F08B175375F3FF2E70D5E26F0B48A0BD47E1988 0
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{69FDE9A3-B341-11EB-90EB-ECF4BBEA1588}.dat	
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{69FDE9A5-B341-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	71806
Entropy (8bit):	2.3520621551335914
Encrypted:	false
SSDEEP:	384:rRNTfTIkMDftL1frrClHChx3h5CrqIh2FEPJ3KFGYUdzuMut2FLU:5uMut26
MD5:	C3480390CF5CFB5FD7B129CB45645298
SHA1:	4FA42277CD4E5CA9B8CC8C389D970D5D8BFF0197
SHA-256:	16C575AA21C4D745D71DB117254EDA708231AE384CF76C04FCE371BEED36051C
SHA-512:	E29224C04A8B4B6AD02DFA89AB4BE52776DDD8A46C5350A81240D9CB2798FF0E8B82A0DCBAAE019B9CAD9EF4BB7ACC487F25ADF913C33BCB809CFF742DC24CF
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\{700F9368-B341-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5642237186388743
Encrypted:	false
SSDEEP:	48:IwcGcprxGwpaUG4pQsGrapbSZmGQpKfyG7HpRSTGIpG:rAZrQk6qBSZeAfdTGA
MD5:	186EDEECF6510FAC391E666809852F28
SHA1:	AA79F12C5129995A1CBC0B2EDC798CB0C09CCB35
SHA-256:	73D62AFDB70FE6546C1385602288469FD150DB6771B8D46B036F23BA53AD02E2
SHA-512:	1CED8D3D6B70ECA7817CE9711DABAFE3B8FB73D3AD0051C387CF5AFE5C5844CC2FF5F1E267060DC09636BFD43C1D2F26D47FF3BBAADFA4CA1429D67718A0765
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\gee00pr\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	27257
Entropy (8bit):	4.371763005968613
Encrypted:	false
SSDEEP:	96:ohNL1evBCcWo4+rWeVjlvwMwmg1L8dgpe1/KJA7153eVgzkff8X9QQQQQBhb9Mg:ohNxigcWo4/AFXaw2pek2LC
MD5:	2D36DA154770C30AE30948286B72225D
SHA1:	CDA14DF9331DBBA8C0A66AAB4A17B9307A6FA2D5
SHA-256:	8190724AF5BB1FA38A019A7967BFC9C2C280A015AE1E3CAB1BF1B3C9D859704A
SHA-512:	8B059A2760D4E83825429EC168E6BFB04703576241877508887D694036E023D42A295325E6698638130AD7BCBD2D90F5D638C9F9A409A94A00D05BB213AC4D52
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\QWXHQVIL\animation_en[1].dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\History\History.IE5\mms\QWXHQVIL\animation_en[1].dat	
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	2.946975957861409
Encrypted:	false
SSDEEP:	768:0Ftd7mo7zstJUsQ7w/0rLsa7ugpPkPgDspX09Cmwa:0FtxRL7wc/Fmgg1h
MD5:	F6DBA6DA8E4ED4BFEF68707E87B8D68B
SHA1:	AE0BC0662CA0744784F59BFD6991FD3AF38D5D11
SHA-256:	02060781CB9733025D00632077AE10E78D4E6D7EBCA5DC75E0CD323844F62F9A
SHA-512:	FA8DA0BC81620E6C57F48E0CC958D3D057EC48D3A260EA488E0434FFE2CF8B8485BE8996F97FA86A5BB9E0C83460331C13A147A54C6CC998C505D6F936B336F
Malicious:	false
Reputation:	low
Preview:	K(z..B.B.....I..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\History\History.IE5\mms\RQJKLIRW\animation_en[1].dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	1245184
Entropy (8bit):	6.329130529832116
Encrypted:	false
SSDEEP:	12288:gPlBUj9iPz17pOdKoRCOEgwvS49GrCuJ0bqp5bchNwZpA8S8e7I2e8tcnv1z9GnM:MUj86BRTEqrGeLnv1z9GVNz
MD5:	8C00F28262A9EF45628FAB74557B3F26
SHA1:	1123E6E9DC3B674D24AA9D563820FDCAAA0D65A5
SHA-256:	52ACD593EFB86D2098054DAF49F1146264B2BC441BD03FF3F8DAD0DE18043A5A
SHA-512:	0DDE596AD9AA5D5A168A387C932BBAAF04AEACD8E2000D87D7D89F32760F9D364DF55C52EE68BCD668EF2999CF462537D8EE53E189755A8154823B4BC559E4E
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\INetCache\IE\2WF3MMUU\1[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	40
Entropy (8bit):	4.0061983328100945
Encrypted:	false
SSDEEP:	3:dRHXseKcq:dRHvKJ
MD5:	0EB8D22E1566A37477FC81DD5D940899
SHA1:	7B3EF425024A19EEAF0E68A187ACAAD1675BCD15
SHA-256:	5D4DEAA7FDCF267ADBB1B3E98603E9AA54EF9BB5A8C6E95019191E06A436D1CD
SHA-512:	EBF00FB097E1901215E74B6D9BA54D765ECF1839AC9462CC78F2F11FDE88F1ADDE654EA20009AE5C57BF3F69DE1B675A59F38117A76601DF4F08EBB899ABFF08
Malicious:	false
Reputation:	low
IE Cache URL:	http://www.keeplaffingwemake99383tyiwye.net/assets/precompile/gt/textbox/1.css?clearcache=5
Preview:	.gttextbox_preset_1{visibility:visible}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\1[2].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	37
Entropy (8bit):	4.00212810987065
Encrypted:	false
SSDEEP:	3:edFeKcq:XKJ

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\1[2].css	
MD5:	3D265A850819F594D78A406F402674C6
SHA1:	F35B9152ADC4D49CEBD4929D898009CB6FEE7A24
SHA-256:	96881B39C2BFB1D5BAEF00DA4235D93A35388EBB7FDD3B6ECC8AFD74DA05CEA5
SHA-512:	824EC5715CA10BF61EDE64E0561A440F5E4A2CFC584BC012181EDCFAD1EA30C267559EC2109962FF8B1A42A043A0D55CB788F425242B44F765252A4CA324F40
Malicious:	false
Reputation:	low
IE Cache URL:	http://www.keeplaffingwemake99383tyiwye.net/assets/precompile/gt/link/1.css?clearcache=5
Preview:	.gtlink_preset_1{visibility:visible}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\24_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):	250341
Entropy (8bit):	7.947292518788355
Encrypted:	false
SSDEEP:	6144:2dK89bQvhd4TVNTaV5yrCdXd82+wZoGCbFvd:OK89Uvhd4x5a2GdK35GC/
MD5:	25851841B2F2DFB3D5185B28953F06C2
SHA1:	3410BF43412856F2DFAA959EED494F8300636A78
SHA-256:	1C49E7FAA7EABFD2A81E671172B5FEBD44DBD716A4DBF595E7FCB3EA9BDB2E40
SHA-512:	661DE379CDB27CF0D25063B1B15BE5521015B1EE7E56ACF74C3D0700348B2739F553D0EB629945E1FD0F7CDDD0508F46CD4486454F175EF6DED155455E7424D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.sitew.org/images/blog/templates/v2/24_desktop.jpg
Preview:	......JFIF.....H.H.....C....................................%...#... , #&')*)..-0-(0%()(...C...........(...((......<.g.."...e................... ....!..1.A."Qaq...2..#BU........3...$R...brt...467Sds...%5CVu....&'DTc..8Eev.H................................5......................!.1..AQ"a..2qR........3B#4..b............?..j(....(.(....(=.....+Z......(............r..?..(.(....(.(....(.(..........j]|.mJ....Z8|;.R.A.9.......h....:..t...Ni..P...^...H.g......m.........zK..nB.F.<S....L..dPx.....I}R......+...6...r......@.W.V.\..u...E.v.e.w.. ....*v...P......+..5.....G..L&.on....H)..H..\.[.r/..t..k.....!7.V...%}.&& .

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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\2WF3MMUU\2[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	40
Entropy (8bit):	4.0061983328100945
Encrypted:	false
SSDEEP:	3:dRHXvM2Xcq:dRHfM2XJ
MD5:	FD30188DCF835132B7352EAE88A0EB05
SHA1:	631B15F0CDF51FB625B7461D05E9B183DA6A11E5
SHA-256:	EA5BD6F1E5713116B691468FA850F5D7ACE6E4424277F84FA422FAC41C2B3196
SHA-512:	C43608FB5AB36CB0C4B0D2D3E4A2B16575681C536F17FA8C900518B4C91AF40FF8EBF69493ABC7D8627CDA1F2FF96C0AB369EDA2ADAE7B6D4D563FB95E035 05

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\2[1].css	
Malicious:	false
Reputation:	low
IE Cache URL:	http://www.keeplaffingwemake99383tyiwye.net/assets/precompile/gt/textbox/2.css?clearcache=5
Preview:	.gttextbox_preset_2{visibility:visible}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\2[2].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	37
Entropy (8bit):	4.00212810987065
Encrypted:	false
SSDEEP:	3:edGM2Xcq:nM2XJ
MD5:	9DB9FCE4F55DC08CBCC9EE0C3CB0E09A
SHA1:	254F97F4CFEC5BF7E7CEA92DC6FE9213447B8881
SHA-256:	295D48D26428E21ECF6F487DC42A544337BAE417D611EF3E082E1FC15A9BC03D
SHA-512:	D5099F8C0595D8D61985745C2FAABA8E2363B9464419970A47894BABC126872026F34374CC84E4CCD0A486B2230592DA4E32BE270839E55579F582612FE67FDA
Malicious:	false
Reputation:	low
IE Cache URL:	http://www.keeplaffingwemake99383tyiwye.net/assets/precompile/gt/link/2.css?clearcache=5
Preview:	.gtlink_preset_2{visibility:visible}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\31_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):	86081
Entropy (8bit):	7.970986566437667
Encrypted:	false
SSDEEP:	1536:WnDDIMFSE6XDS5fu2PleoyuShdAuQRHiqEZ0BlEP34Bwmae753EvzOK3MN65zGl7:CsMwFm5jleoYAuQRCqg7Le71+z9zAa4T
MD5:	72DFC913453C36B15C419A083FA9C2DF
SHA1:	8850D6CECCA794F70D9DF75405C73D37B043AE45
SHA-256:	256153C10ED7D86ADBC7827B63FC2C0BBEF67479C3F49B599E57738E53B53905
SHA-512:	3ED4521D702EDD2954BAC2B9C342127EDDFE68C4F9E58F0875A193DC13BD4F9B0348BA5E3CD5FD26161CCB84A4F22D9623E3922C898DEEF2DE7BD46655403 AA
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.sitew.org/images/blog/templates/v2/31_mobile.jpg
Preview:	

......JFIF.....H.H.....C....................................%...#... , #&')*)..-0-(0%()(...C...........(...((...........".._...................
....!..1.A.Qa."q.2.....#.....36BRTdrst...5DSb.....$&7Cce.......%4EUV.8.'..................................:.......................!1..2AQ.."Ra...3bq...c#Br...4C..............?..d.I..I$.I$..$.@$.I..I$
.I$..$.@$.I..I$.I$..$.@$.I..I$.I$..$.@$.I..I$.I$..$.@$.I..I$.I$..$.@$.I..I$.I$..$.@$.I..I$.I$..$.@$.I..I$.I$..$.@$.I..I$.I$..$.@$.I..I=6>.F..=.;Z.K...3.../R.....2......R............m..)Iz...
..V...%........m..)It.o...D.....1C.....<=...G."x9\..$.H..I .I$.I$..$.H..I .I$.I$..$.H..I .I$.I$..$.H..I .I$.I$..$.H..I .I$.I$..$.H..I .I$.I$..$.H..I .I$.I$..$.H..I .I$.I$..$.H..I .I$.I$..$.H..I .I$.I$
..$.H..esV.....Q.X.'4.>.AV4.G.....".....,/0.s..{.2.....5z....f......nk\|.KI.I(..N\..........-..S>.(S.GP.:.{....$................7....?..G..<..%...............g...}#.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\38_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, 795x796, frames 3
Category:	downloaded
Size (bytes):	91881
Entropy (8bit):	7.969043029752055
Encrypted:	false
SSDEEP:	1536:jxMzX14NBPMDRoFXjk83YX7HXCYICTxjRHvHZsV+KKmDL4ojACd:jxMzIBHN3YX7HSiNjRHv5Ravd
MD5:	1D3FC9B0D179BD82504516DA9CFE8756
SHA1:	2F899938196C4495D54A3F0B1040109374BF08DA
SHA-256:	54929B4DAE504F0FD5BF058F5CDCE1F9CDA7ADAEF78ACD6EEE493F650717C41E
SHA-512:	8724EFDC08895F3CCA4E931DB257DA3B0A60379993EEF187A835B219FFF6B5DFE871CC6226D0892B8A3317B9AB6A79FFBCE802575C07532780A73C8F064446C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.sitew.org/images/blog/templates/v2/38_desktop.jpg
Preview:	

......JFIF.....H.H.....C....................................%...#... , #&')*)..-0-(0%()(...C...........(...((..........."...^..................
.......!.1A."Qa..q...2....#BRU......$3t...6STVbdr.....%&45Cu.....7DFs..'cve................................9.......................!.1A..Q..."2RSq..a...#B....C3r.............?..q....*.....-....>.......
.5...+4wj9*.;%wh..d.....<.$......Su.t..._Rz*...".F.....\...M....q....KN..4.L-c..O'...$...>..\..;..y&".m...L)...9.............0G.,.J..Zij...J...02We\......).....L""......-pU.J.IZ..Np.....@d...$wz)'|"b
.49.|ncHo.-q. u .>.{...|I.c.P..I..6.....N....d..0.O%..M.)...#..F ..Ky.1.n.'w?....|K.U...#......{(....\t...p.78b...3_.ocZ.{..78.:..`rN.~..>%.*ix...Q26.J.....;Inr......w.Vav.(...n...a{.t.....:...ub..;..
.h.]{.h."g..5.F"..%. ;`.. .[...y...9.{_...c.".#...(..ul>L....".+.F..8.C.dTV. m}-.OW1KS/c$E..{7H:n.h.-..%2....pd..xq...ky..a...T....*..X..%.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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\2WF3MMUU\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
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\2WF3MMUU\50_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, 1218x1218, frames 3
Category:	downloaded
Size (bytes):	188314
Entropy (8bit):	7.976826760856431
Encrypted:	false
SSDEEP:	3072:bqqeVueduRQV/RvmCv22jutVgZjFVFuYGIMixdgmyneMs4fk8jI7/tZvpR30u1da:mTdduC5HStVgZpoI/dg/nevGJaxp4
MD5:	B83AF0FF2C3996DC36ADF970475BFE11
SHA1:	C516119C147EB84FA003C98D7CAFBA88DF085BE4
SHA-256:	14379598449BE97A8E55673489C1A96B64AA0CB744C5F1E41403A97A1C444B6B
SHA-512:	8FE64B271BC1279AE98D342F4FDC67049CB5B8F9C6D083E718DF6C62BCDF0F89129F735CA01CDE24C81B78C6151C087AED62CD829C78B2EC1B847D89606B8F E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.sitew.org/images/blog/templates/v2/50_desktop.jpg
Preview:	......JFIF.....`.`.....C....................................%...#... , #&')*)..-0-(0%()(...C..........(...((..........".......................................a.........................!1. .AQ."a.2q.#.....BRV....$3T...SUbr.......%45Cst....&6DEcd....7e'F..(..............................C.......................!1..AQa."...2q.....Rbc...#3BCS.4..5r..$.............?.....a.U......q....u.. c..'...A3....}~.l|L.x.h.Q..DG3.,2..m....;/.~..L4..NK...z.i^....{.5..y..d..'.N.....d-..Lp..........!py...]._.r........V....>.zli.......}+...|.K{...C.....U.F.dk"c..l...^..Ya.,;,.Z*..9...q.fiyq.r.7s........XvK.."j *.)`...x.3re|d2L......e.......)a.,;*.......)a.,;*.......)a.,;*.......)a.,;*.......)a.,;*.......)a.,;*.......)a.,;*.......)a.,;*.......)a.,;*.......)a.,;*.......)a.,;*.......)a.,;*.......)a.,;*.......)a.,;*.......)a.,;*.......)a.,;*.......)a.,;*.......)a.,;*.......)a.,;*.......

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\50_mobile[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\50_mobile[1].jpg</th></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>104276</td></tr>
<tr><td>Entropy (8bit):</td><td>7.9691120599889755</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>1536:/67p/XXoCRcR8UZDgTdhN08lNOmMs/1ttQekOnQIr/n50Mk0whOwZ1a4m9DjDgkU:A/XXelDgF0gN90snQoIh/aF90kPs</td></tr>
<tr><td>MD5:</td><td>D23390986E9AC9BEE94F66A1AD5ED12A</td></tr>
<tr><td>SHA1:</td><td>572089368ADB8A37E80C006926D96A0000C17721</td></tr>
<tr><td>SHA-256:</td><td>C5FDD5269F0B2AD58A1E1886F34DA7671A985EBAD3A1DD41F16D1A1DDD958EF6</td></tr>
<tr><td>SHA-512:</td><td>A655434DB934A89CC749A83C956E8D091CBA83331A89B519A3886364E2A873B4BC3A1D7B22672CAA39F39166531B8CB3954B45DD3887749A9FBE8B77E7605306</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/v2/50_mobile.jpg</td></tr>
<tr><td>Preview:</td><td>......JFIF.....H.H.....C....................................%...#... , #&')*)..-0-(0%()(...C...........(...((..........."...c.................
......!..1A..Q"aq.2.....#Bb......Rr.....$35EUst..%467CDSTd....&Vc.....'u..8.F.................................>.......................!..1.AQ..."aq....23R..#4B...b%Cr.$...............?..d!...B.B....
.!...B.B.... .!...B.B.... .!...B.B.... .!...B.B.... .!...B.B.... .!...B.B.... .!...B.B.... .!...B.B.... .!...B.B.... .!...N...F.6..y.kZ,.P.B.,o...h#..~4|.I2....O......X..[..R............#........V....t.o.....cE
.8b..4.dc..>......@.B......!.!.@.B......!.!.@.B......!.!.@.B......!.!.@.B......!.!.@.B......!.!.@.B......!.!.@.B......!.!.@.B......!.!.@.B......!.!.@.B....&\,.2...<.6F:.9..X.q..j8.q9..&VB..M..~......5
..v6~..`=..-.k..........o+..e....O.-\...L.3..C...,.....'.?.g.?..P.........W..C....G..y_.-...Z.al...........b?.g.?..P.....,....$.##...<0..,yy.u</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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>
<tr><td>MD5:</td><td>E2F94DF5BE388E04D034327F662E04FF</td></tr>
<tr><td>SHA1:</td><td>E682BF79D9FE879AFB4EEDB5F4B665F77FF1408E</td></tr>
<tr><td>SHA-256:</td><td>67A61345981F11B6DB6FCCD27331C4617B4AF5063386BB5017D50957080D8912</td></tr>
<tr><td>SHA-512:</td><td>B8DA360BAC16F066190354E1DB207B8606B272201EADCDBFB211CAA978A58C0CBA27D74EFF42CB3B5E6BB41E742DB921A3B9F87BAB3E054202A43427BBDA9
7C</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_mobile.jpg</td></tr>
<tr><td>Preview:</td><td>......JFIF.....H.H.....C....................................%...#... , #&')*)..-0-(0%()(...C...........(...((..........."...`...........................!
..1AQa."q.....27ft.....#56BRSbrs.....34u..CV.....$8TU..%Wc..&....d...............................9.........................!1.AQaq...."24....3..R..#BDSr.............?...
....;F.I#Y.\..wZ.UU@..J.`..h#...h....*..o....@Z....G..".J.......Q.....@Z....G...".l..C_.ME4Z.. ....#....p..L...k@..
.................Z*.*..<.6F;..j....[i.p.....6J.Y.U...L.q.~...ki....<."x.e[../sU..J...n..V.....ei.3...xF..t...5..........\?.X...7U..C.......Z.....!....?...........\?.X.;...Wm.z............\.e\.D.LpN.>$...=..k}5.
....."H.k..n.x..'...z</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\QGY9z_wNahGAdqQ43Rh_ebrnlwyYfEPxPoGU3ms5pIfe[1].woff</th></tr>
<tr><td>Process:</td><td>C:\Program Files (x86)\Internet Explorer\iexplore.exe</td></tr>
<tr><td>File Type:</td><td>Web Open Font Format, TrueType, length 29120, version 1.1</td></tr>
<tr><td>Category:</td><td>downloaded</td></tr>
<tr><td>Size (bytes):</td><td>29120</td></tr>
<tr><td>Entropy (8bit):</td><td>7.982307308237849</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>768:zhtI28eZGy7YAu7AMHryTzlVesXYW8a85nLhSA+Dz3:FtCgZYlE9zlVDXYW8a85nL0A+Dz</td></tr>
<tr><td>MD5:</td><td>F52486207F157177A78F375B2E19454B</td></tr>
<tr><td>SHA1:</td><td>4EAE88EB3840CFFDDE0CD22486ABFA6F053BF903</td></tr>
<tr><td>SHA-256:</td><td>1D12EEE488133CC4BB8634834217B207AF6483CF63FF6A0FEFDB75CC1951E04F</td></tr>
<tr><td>SHA-512:</td><td>7C78A21F8B3D25FFBCABA00E3E7A3805377BE4B6340360F08112282DCD40834E7AA7479367C8EF58C0B4697B2EB6F5F6CEF34CF12885107855AAB383BA5AC6E</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://fonts.gstatic.com/s/worksans/v9/QGY9z_wNahGAdqQ43Rh_ebrnlwyYfEPxPoGU3ms5pIfe.woff</td></tr>
<tr><td>Preview:</td><td>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.<..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.<br>.@......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.</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\QGY9z_wNahGAdqQ43Rh_ebrnlwyYfEPxPoGUOWw5pIfe[1].woff</th></tr>
<tr><td>Process:</td><td>C:\Program Files (x86)\Internet Explorer\iexplore.exe</td></tr>
<tr><td>File Type:</td><td>Web Open Font Format, TrueType, length 30076, version 1.1</td></tr>
<tr><td>Category:</td><td>downloaded</td></tr>
</table>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\QGY9z_wNahGAdqQ43Rh_ebrnlwyYfEPxPoGUOWw5pIfe[1].woff	
Size (bytes):	30076
Entropy (8bit):	7.982292718946404
Encrypted:	false
SSDEEP:	768:hzSthAeZrndmgAMGBy/QKgl6P2tMU38xin3:NpeOVwq6ri3
MD5:	C6730CEE0079AC03FB54A256C72AB29B
SHA1:	8751E8D39D2B78DF6F7D2BABC73DE54250543A00
SHA-256:	2C47E476F0CCCB041C06245691A143E905619DAC12575ABE399FDF0A165517CA
SHA-512:	B997C185FB44004A3D29F49C62AF5ADE79B55A43579F2618CB361546A839451419EAF9EA8EBCA53C9077F1DC614952305B71972EFCE1B41D1655E3FCD50D7A4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/worksans/v9/QGY9z_wNahGAdqQ43Rh_ebrnlwyYfEPxPoGUOWw5pIfe.woff
Preview:	wOFF.....u|.....GDEF.....0...>...;GPOS.....E...k.GSUB...H...'...nZ.;.OS/2.. p...R...`].'.STAT.. ....6...@....cmap.. .....o.cvt .."....t....+...fpgm..#8.....6 ..gasp..)..... .....glyf..*...C...{..+g.head..m....6...6.=..hhea..n....#...$....hmtx..n0.....v...loca..p....\...d.A..maxp..sD... ... ...qname..sd...5....>.[.post..t..... ...2prep..t.....8. 1px.=... .....N....NG."....S\...a*q....P...x.L..t.P.....x&;qR;X.m.m.m.....p!....],&|.....}.U..p. .5..... dj...LLz..Lk.5..62.g.".d...L..'..m.m..Vl#....?:.;....].S..d...e..e%...<=>3... j.e..u..).....e.f....!.!...s.....{z.F[j..!..R8...4Y....D'.+/...-.....r_y..S~*.W4...X...V...U.P^*/i._..q.gC.PO(..1"wT..1yc...M68no|.....j....G..4..F..n7../..fF...fa....IOn....^.,..>....b(.b. &b.VPc.....8..c..a...8..$.`&.....a.^S[....v|.'..oB.....xq.d ~.&<.p.H.?.v.....Uh.R.{...x*.....Vw....~I...K..R<...)M.C..._....>}.~..cs.3.s.....G....ZC^t,..~...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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:	EB88663E73EEB3CC9EE1DEBFD29EF5B6E5DF84435A65039DADF17AF8CE1038F01E036D1F675CAEB52D195732ECC33C182863537BB1A8BD20AE31E1064940B0 9A
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$loca..p....Y...d..*maxp..sD... ... ...qname..sd...A....Geg.post..t..... ...2prep..t.....8.1p x.=... .....N....NG."....S\...a*q....P...x.L..t.@.....dk7:z.m.m.m.m..t.o.{A.X...../[.....i.s{.....`f...!...8..dd..5..ro.C.....r.....6.Q7.O^1....i.l.i.....NS..>...%...3.I..Jk.....OJ.:.....Y/. ...<.F...y....;.<...,...C.....L...I.k.UV?&V1N.*6.....c. .FJ...i.....s...o.1.|...6="'*,J.....h..8^....6.....Uk.5.W+:,...s...U.jP.j....jm."S.....\.....!..~X..2f$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\2WF3MMUU\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\2WF3MMUU\TXMZ4AWB.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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\TXMZ4AWB.htm	
Entropy (8bit):	5.414183636486543
Encrypted:	false
SSDEEP:	24576:jdCThiwmf8lyrXWdigQYGobhcODdqy3ttOYoH:jdCThiwY8l/digQY3l5tOYoH
MD5:	5BF48A1C7F536E963A9C09A9DBBBE239
SHA1:	6C36648F46D5BA7D157BA4B6A93CF2F3AA8814C2
SHA-256:	1E90B736DFC26775FB87CF56A55D6B4A24E92968A999BE00EB2214DBEBF0891E
SHA-512:	D3D65585FAE70D81D5C08A0ECA61F925E207B055E9D4738CE52E51E5E73F50720BDE4154E679710CB3A369CFDDFB58F2329BDD5A2079E0977C45263A648C9D2
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" crossorigin="anonymous"/>. <link rel="dns-prefetch preconnect" href="https://rb.bp.cdnsw.com" crossorigin="anonymous"/>. <link rel="dns-prefetch preconnect" href="https://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 property="og:title" content="remittnce advice - Page 1">..<meta property="og:type" content="website">..<meta property="og:url" content="http://www.keeplaffingwemake99383tyiwye.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\2WF3MMUU\browser_1[1].webp	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	RIFF (little-endian) data, Web/P image
Category:	downloaded
Size (bytes):	15872
Entropy (8bit):	7.983508681345451
Encrypted:	false
SSDEEP:	192:puTG/dxJT8G78Gd4k42zn5/3ICtpJznRRqgPf0LKn7btuNrxK+WtbyJfgNcpCXq+:xP8bkMCNRRqwfR2NKntOCHXqjYe4D
MD5:	CEBC1918222299344F5A3073DA8BC3B9
SHA1:	4612783EE9056EB20BD04A63959D0AC718F64C03
SHA-256:	AF15E11360250C4E189338116CB8A1B621EBF1259C273F7786B1A031CEA6F41F
SHA-512:	745894B95DB0C538B60185D3BAB3B0866FDAFC3F2E4D3D5BF5D402CAFEEB4C43A11B71578BAD9CBA24232E55064406BD79437011E33457B67EDD68F31CC2073
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.sitew.org/images/blog/landing/2021/top/en/browser_1.webp
Preview:	RIFF.=..WEBPVP8X.....*.....ALPH.....m.8..c.].G..`.t.BB...)...L...'...u..;...)qR.ll.n.^ H.3tT..k.....hyfq'g.....l6..p.m$.):..;..)...F...e..B..FO..'....Qo.~vw?...]..;.5E(..i.....~5..."B..6.$Y..T...U..j~@HI._..)..K...+7...?Ha...P.IH...w.....W6C......e.....m..)....m.....UX.9H.*hcz...U.X...s..e.P$.SA.n.....}YQT.CE.w..aC.....Y..p...!..$]....}L .|L.....6..ek".zp_..a...a...Z.!"..._...C....jU.F.}..r.:.w(v.....m*..DpMU.....<.yBP.}.y.v.i.d...*.....}..j90:... s.}....9*(p.]z...."..E.(W....1.q.A...tG..ED."...V9.K.De\\..{.v.`JA...s\h@..y:...,...y^.)*.....KU.u..@.kORI.IA...:j.]"....sR`.....f.... c_.7.....x..!2.....F..5.`...`..k.Jv.....;<.3.....h.....-|..8.....#]Y[.t.....P..P.U..N.[..~.....5.$02.....H...vxY.Z...M..|B...ey~.Ejj9.t...<_L...-..k.l..}.7...j.":....<.Q.rMFE7.t..;...M%....<.oL....5.]....C../Y.....V...%Q.....t.i.../...sd.Y/.t.i)`&.....iw .c4.:.x..C.:./....z..l....pa....f..Q/^..\.....9...D

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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:	EFFE15E105FC5FA853E76917B533AAE6C75EBA9A256049FB5EAB88BBF319D63A4CE4AE3743A09D6A5F474B01649D6EDC5C8BCCC61B8CA9EA9E5C39E7AE724C16
Malicious:	false
Reputation:	low
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-.607A1.107,1.107,0,0,1,14.857,6.857Z"/></svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\ellipsis_grey_2b5d393db04a5e6e1f739cb266e65b4c[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\ellipsis_grey_2b5d393db04a5e6e1f739cb266e65b4c[1].svg	
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\2WF3MMUU\f[1].txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	37049
Entropy (8bit):	5.493515419348243
Encrypted:	false
SSDEEP:	384:QzSG52hCl0xoxfs92x2QqL9aWB5XteWAMizkKpjepTgMCw/DASBjt4cF1r5pfyKV:whtnsnaW7izkOKT1jZifJOwO
MD5:	80BB54CD686F03BD344E0FEC0B70A792
SHA1:	5E3413130F4AD6ABA7E9A2FEF2D1E7B07DECEF63
SHA-256:	BCFE8A6BA59B117A8C558075EE84FD9E95ABF2B5E2A263B7F44D2688D6EAAAC7
SHA-512:	947F1F5FFC8F90564B52063C473A7F8D7CCA2B111B523846CA727C7A21591B742853598DD2435C545D144122842050A0AFBD1117AFDF95F58BB9C97F7516B48B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.googleadservices.com/pagead/conversion_async.js
Preview:	

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\favicon_a_eupayfgghqiai7k9sol6lg2[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 6 icons, 128x128, 16 colors, 72x72, 16 colors
Category:	downloaded
Size (bytes):	17174
Entropy (8bit):	2.9129715116732746
Encrypted:	false
SSDEEP:	24:QSNTmTFxg4lyyyyyyyyyyyyyio7eeeeeeeeekzgsLsLsLsLsLsQZp:nfgyyyyyyyyyyyyynzQQQQQO
MD5:	12E3DAC858061D088023B2BD48E2FA96
SHA1:	E08CE1A144ECEAE0C3C2EA7A9D6FBC5658F24CE5
SHA-256:	90CDAF487716184E4034000935C605D1633926D348116D198F355A98B8C6CD21
SHA-512:	C5030C55A855E7A9E20E22F4C70BF1E0F3C558A9B7D501CFAB6992AC2656AE5E41B050CCAC541EFA55F9603E0D349B247EB4912EE169D44044271789C719CD0
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://aadcdn.msftauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico
Preview:	

.............h(..f...HH...........(..00......h....6.. ....=..............@..........(....A..(...................(....................................."P...""" ...3333333333333333333333333333333"" ...33333333333333333333333333333333"" ...33333333333333333333333333333333"" ...33333333333333333333333333333333"" ...33333333333333333333333333333333"" ...3333333333333333333333333333333"" ...33333333333333333333333333333333"" ...33333333333333333333333333333333"" ...33333333333333333333333333333333"" ...33333333333333333333333333333333"" ...33333333333333333333333333333333""

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\features[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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\features[1].png	
Size (bytes):	31122
Entropy (8bit):	7.980200205130251
Encrypted:	false
SSDEEP:	768:ro2K9UgcuQACSIfLOjEf2CnHEw08GdRkN7sjWrZ:E4pijzCHxZsU
MD5:	CD922382DFF68C851AA4F98E87B610C0
SHA1:	5432F4A60B45A949D64A5D10ABC1B5A988DD1D1F
SHA-256:	AC24E76C3FA94165A7324932BACB946995CE29B0715ABB3F31BA315349992123
SHA-512:	2C7AE731719553280849CA10A0D9856B11B24AD42779BE76F800AD8F35D0D657A0B001DF1511145AE439BACAB05BEC927D579D6B84CAE0AF641B5EFDAE6CDB03
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.sitew.org/images/blog/welcome/icons_menu/2021/features.png
Preview:	.PNG.....IHDR...,.....`..`..yYIDATx..K.,m...Vd.{...WWW.....0....c..b.....C....B. .!$. .'0.....X..BF.....`!d0.a.7.mw.....?.='c3.x....'.'.*...=..\|DF~...^{..q<...8...?...x....X..q<.....8.....x....X..q<.....8.....x....X..q<.....8.....x....X..q<.....8.....$.....w.....K..~....lY.8..9.q,_Z...Gr.W9.s..`xk...."9.... .....?.....[.....o..|.....'..~....u..$../1.D.;=Y.yh.QZo..._....g.....o.j\.r{....._..o.;.....p..2.....y.s....o=.....x.s....?.zU...?.?.....4..v...'.=..S.....%.X...D..P.....:...?.3.....o}..sm|&...?..K..?....?.....o..s...._....#'Y.H..x.z...)9@...Q.I..+...P=7y.....>?... .....q'..).X.....X..~.....~...W...."%.....(...=[.Ap...y..s..w.\....,>V.sj...w..!y..gw....A.....ik..KDv....^p8...8m^..v...B0...p..bB.j..z....././.....D}f.Y...~M.....}.qS...4ox._@t...X..~.....?@.....i7..l-v`.K....X....j.s..2.9..Z ..K..k...".=...3>.]..|...._?.#.8.H.s.....o8.q'

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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:mmMtI+A4CSIDqvnI+YTBrFPvVrJjhiRAiiEL:mXtI+A4GDUI+Y9rpVljhiIEL
MD5:	C495654869785BC3DF60216616814AD1
SHA1:	0140952C64E3F2B74EF64E050F2FE86EAB6624C8
SHA-256:	36E0A7E08BEE65774168528938072C536437669C1B7458AC77976EC788E4439C
SHA-512:	E40F27C1D30E5AB4B3DB47C3B2373381489D50147C9623D853E5B299364FD65998F46E8E73B1E566FD79E97AA7B20354CD3C8C79F15372C147FED9C913FFB10
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\2WF3MMUU\gilroy-regular-f1ecb849891a09cae3f3d560b7ed2e08[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 26440, version 1.0
Category:	downloaded
Size (bytes):	26440
Entropy (8bit):	7.978235771802257
Encrypted:	false
SSDEEP:	768:471jytWqy4Nk+ZsQuCUGezD9rzDBszgp7zTkn:61jP4NkpCUb9rzlUgpzTkn
MD5:	9E87C6E1F8D0D381ED270E7881093CAB
SHA1:	B1E446D98CB537B47041A1EFED516DE2BC125020
SHA-256:	D5809181114B71E873CD7201C2B3CFA27108867E97186564DC169F961BA127CB
SHA-512:	7F56D85C2C7A681B7143263D3830B35C4645B470AFBF0DEE29A166914BEEC66581FFF3708B4BFB10E1E38A69EB6D0B98737DCCC14225DE98C43602142BBB0C1B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://st0.bp.cdnsw.com/assets/gilroy/gilroy-regular-f1ecb849891a09cae3f3d560b7ed2e08.woff
Preview:	wOFF.....gH.....FFTM..... .GDEF.....(...*....GPOS.....m..@.....GSUB...H.....P..tOS/2.....U...`.`{fcmap...p.....b.~.cvt .....4...4.v..fpgm...8.....eS./.gasp.....glyf.....D....."..Vhead..^....6...6.d..hhea..._$... ...$....hmtx..._D.....K.loca..aD.....A.maxp..c.... ... .name..c(.....D*.}.post..d....."..prep..f.....%z.....o.....J.....x.c`d``..b% fb`f`dx.....y.....,`...P...x..[[.$.Y....V.3.3.3{.d.....^{6f.cd....u6.7!..)...eq.f...$dR." .$Q..<.A .J.8...R..^F.b\D.6....%.....w.:...I..U.u9u.?.....I.../=~.....<(>.J./..JHWz...G._;%.G.y...q..'.y....\.~..S._}D]...$..s.s/..K2..k/.(-^Q.....w,..9..%9.j..]_8.....0..w.y...|.....:.....v..V..p."..e.w.U~O....Kr..5..-..../K..(s[~C^....(Ui.SY..y.... ...!.8Rw...S.....~W^...A..-....g.P..L..).R.~.y....C...~,.p~.).WO..&.:.U).....@.Y...Ip'A>..\3wK.e.\B).e/../.P....F.....c..wY.....Q..~...#^.`..;.....oa..\m].'..>f.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\home-engagements-illu[1].webp	
Size (bytes):	8982
Entropy (8bit):	7.967036627244742
Encrypted:	false
SSDEEP:	192:h55552Y0CVILC+whtSD1qAZEy2lQqgyTd861YPjLCAtxu2aRAz0l:F0O+whUBWysQqgye06CZPC
MD5:	BA3A12266D4D0B33D7EB42BA7595F226
SHA1:	8CE370D016835E6A7E68BC55A675BF1C85382B27
SHA-256:	20EC47ACB54764DBC22DA306C1A99D1628BE9236DDEB7CE60194549073D3FEA2
SHA-512:	9E71EE3D771F7E04702E8371DA5298B94FC449D72D36713F54870CAD508F756834122789088288338322222FBEDCD4AE03A00E559D53036C69F2EB7CBF502F472
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...$'..Fal.:0'F...[Kw7.....ru:._b...#f..;.u....T|.....A..7z..X.c.^....Xc...#3.Z..z$.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...[.Iy .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\2WF3MMUU\home-google-argent[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):	101876
Entropy (8bit):	7.9840439806569785
Encrypted:	false
SSDEEP:	3072:mYXUoJeCEDYEs6mFVo1OkWUloKZaJUimIj:mAOCE/mFuVZaOIj
MD5:	11331A3DB14B9615CD007F28AA789DB0
SHA1:	BCD3B48871417649A503A9888EA5EE23ADB3E8EB
SHA-256:	A7B82D2D46E1B3D86D70DCE1EB6417A88BD1C9AA1B6077998FB0912F133513C0
SHA-512:	7076AA043C43666408A648D3AEC4A62945AB4CB691C22D1A8A00141482CDEECE405D3C1136CA7AC2B10E21DE399E2FAE03512CDCB2A06475BA57B4EA713464CC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.sitew.org/images/blog/landing/2021/home-google-argent.png
Preview:	.PNG.....IHDR.....IDATx..}w.dE.....o..;9..s...$'A`@DD.A..P..@}>.....>..0.....H....{.....].....7wn.:....{..k.J)..#.0..#.....F.a..F..0..#.0..#.z.a..F.a...=.0..#.0....F.a. .F.....#.0..#...a..F.a..F..0..#.0..C.E.....alJ..6....F.a..<4.p.4al. M_...3.0..#...alR.....9.Q..hu.P...>. ...n ...KH.....4foOJ..HA.1P.A.5 ..DU ...(%..J.k.=.G.{./X..>sm....#...a..Z.m-. .....v..Im...+.L?...O9..y...Iu...)....c'O./.;...:.....c..8.^j.8j.'...C.mT.+I)..... ....@q=..'..z.....&...(o ...D.e.}.....o.}..ux.Y.K..../..?A-k.".0...D...g.a...\i..gn.)..D..._.1~\q...._8o.....|i....1..#.....tp .P...@.....U..GP..D.F.7.fA.4...(..h....U`.$.o2.....1@{.h...&.....,.....b...O|.[?../.yx.../.....@>.0^.C.....x..7!.L....QR(.Z.../.....y..N:..s..r{.....wL..*`.. *....g.`A..!._....f_#?.*.C...-w$.:.W...@...`..^.T..=.G.....K.....o_...../..?sx..@.....#.z..0^U ...q.1<<.]w.f..g.r.....s..r.;.....A...../....R.....).....1..9(....>A.....8.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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\2WF3MMUU\home-google-serein[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):	42647
Entropy (8bit):	7.973461996523163

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\home-google-serein[1].png	
Encrypted:	false
SSDEEP:	768:x2zPNQtAMPgKJu7srLO0B3eiRsr3uDgJVi3TB4YVpVvB6uHcMKe:IPN0gKJPxeQsPJUB4cBuG
MD5:	8FA255602793FF24D43AF810DFB6352B
SHA1:	E43D4F9D41D5C0A0F72C37C78BB1AC9E1F31DCA0
SHA-256:	A16E70767279F7F1C1F99EEF85185B7ADFA6B10465D3A00AACBEB67769D01B7D
SHA-512:	19036F1104ADB469CD7602B5D3124AD23BCEB1FE4269AD34424617545360668E6D5D05C963A1F70903D9ECCDAB8AE1548795E6EC2B760A7F94ABC1108FB88B9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.sitew.org/images/blog/landing/2021/home-google-serein.png
Preview:	.PNG.....IHDR.....^IDATx..i.l.u.....oh5.....$Y.)Jv.....(p,.A,.T"+..9p.@..$@....EA..G~....O..Q.+.e..%...D.d. .S. .-.s....{...s...T..^w.ao....:u.T.....ZB.....w.u.******. .+******..+******..+******..+******..+******..+******..+******..+******..+******..+******..+******..+******..+******..+******..+******..+******....%...s.<..... mp....^.. ..^....x....Ob.,.....a;.g.. .....l.....F.....3..B .....?..?P ...@.....O.....x.q.l..!..`w..A ...d...q.0..d..qv}zI!.=...{.x.....O..f.?..d7.....2..H..x.....0...`.Ppv.....Lo.....p.#..g.. F0..._=.v.\zq..{F.....-.....|.K_....p7.....{.....|m.pU..g;@d...B`.-..@NO!2BN.._7B.....v.@...b..~.?._.&....~.....\.....q....^...@@...6.....Nq..o.....%...=.|}.gy.....?.Z...O?..6.-d. [...#.....\{....-...s...g...2.x..k...}..{.i...0..;.. N.W....>....A@R}%..F.#!"..$(.....#G..^.....@.....o...`....r.....0L...W.....k.c..@ 8;;...= G..c..#...{.....<.K.-8...0..B.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\home-google-simple[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):	63696
Entropy (8bit):	7.989394673195322
Encrypted:	false
SSDEEP:	1536:ELFRzvMENq8teCjGpA8Hh69H+HJOyUTCe3l7XcUO:UFRzvMmqcjjGpAS60wyUt3l7XcUO
MD5:	C844D819C0D9FC9870A9A40FA9C40798
SHA1:	C8018F06072C9D65F5AC1774DE5800D29F6642AE
SHA-256:	00CB5FC55F36AFAB35A283873A006F1A06B3D03366C5DA59D720602055D77459
SHA-512:	856FF957D295312C6D819DE7FC36BF6096FB60BFD8B5753AAF0B2415D660FB097A035F91738F74867B38F29E012F43EE42E5A52FF8891B8659B0E197543FF9C8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.sitew.org/images/blog/landing/2021/home-google-simple.png
Preview:	.PNG.....IHDR.....IDATx..[.$Kv..vdV.y...v..<8..$..IpH. %.. .....K0h..a...I...>D.. .,P.i....'...Z4...a.%.&.!53.._...*3c.#..2##v.sN...=.....X{..{....-[.l.e.d[.. [.l.e..-[.l.e..-[.l.e..-[.l.e..-[.l.e@.-[.l.e@.-[.l.e@.-[.l.e@.-[.l.2.g.-[.l.2.g.-[.l.2.g.-[.l.2.g.-[.l..e.-[.l..e.-[.l..e.-[.l..e.-[....e.-[....e.-[....e.-[....e.-[..l.e.-[..l.e.-[..l.e.-[..l.e.-z.l.e.-.z.l.e.-.z.l.e.-.z.l.e..=[.l.e..=[.l.e..=[.l.e.)..Q..l.e{=-....o}....g.-.k...@...]..-[.l.^.H<.....o..2.g.-.k..o.....{....?.....WNj.X.^HN...|:.Ae....g. ..8(h.....?.....g@.-[.....o.....O..w...#y.^..#..+?.....o....W../.....#.=?.z..l .e..9....]...+.....).....f?V,#...s.u,Bg.8...Z..w.....3..'.....~..L...h=.z.l..`~..=|..._..}.O.p. .../...|....qtjqd...]...._.?.~..~._d....z..l.e.t.9.._....?|...?..i."..3...(..gK|8.X...../..w~..~.o.....  ....=[.l.>.....o.....].`k_.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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
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.Xfff.Xffff.Xffff.Xfff.Xffff.Xffff.Xfff.Xffff.Xffff.Xfff.Xffff.Xffff.Xfff.Xffff.Xffff.Xfff.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..lA^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\2WF3MMUU\home-reassurance-1-rapidite[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):	17827
Entropy (8bit):	7.902116044447362
Encrypted:	false
SSDEEP:	384:vApcImELPdr7+/lQN8hcXiVNpULxF/x2nCKiGTlp5ySbZcR:vA60PGIxBQ/YnCHsYSb0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\home-reassurance-1-rapidite[1].png	
MD5:	33C9BE78092162F7071AC756DC1ED4DE
SHA1:	9CC988CA1BCEB7ADEFD71D8E800487887D6EB370
SHA-256:	893B2C451B8E8FC77B801799861564D003B10B9BAE43613D414E83863D8FC624
SHA-512:	F8A782127BF3642E6FBF8B6BE1B974530F5893335A8752F44806D773D2AE414A8B5280E0248ECAE986AF2DD4F3166B79001FD8310ABD2B834A7E5900F815A9E8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.sitew.org/images/blog/landing/2021/home-reassurance-1-rapidite.png
Preview:	.PNG.....IHDR...,.....`..`..EjIDATx...x.U..I.....,?XPA.4.....(...&.CzHB..F...P..M...;..dw.Iv....;O...3y.=.{...8PPPP.B.@AAA..... `QPP..((((.X.....,.....EAAA..... `QPPP..(((.X.....,.....EAAAA.... `QPPP..((((.X....,.....EAAAA..... `QPP..((((,,,}W.Vo.2..gm.....%sz...;/.A._..U.....G....#..vt..>].}e....s.*.....e.....v.....?.....f_..r..a.....T.X...9 `92`u.p <u...M.q.....:.r...aUZ.....$.zt.A+%.....|W.....%=.H}:|8..!..o....!..B....=..~-.j\..j..V...G.Bfb.d...d..mk.....5..+r+.....!.k:..e..k.~.....M..Q.V..c....6)R.V|...e....7ot....c... X.d.....,%.....E`i|g..{.h...7..ub..;.6.E..M..I...G..$3`I.m[.....m.mY.e...e..%<.e8.F..+.....+.w..k..{O.... jM.....2.z...*..}.N.9!....C.<C...bm.q..+].~...F`....).K0.5.%.....Y.D.<8.....V...&.. ,:T..\.%D..,>.... .vm.e..s...tY%.Fe.+`....1.4.Y.G.....^S.....^.`X...-..VN...zt....{.#:...e..tY/..a-.1,.V3!.G...k.h[.k h..M..B/....E...N.:...Y..m=d....5..M-.t

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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
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\2WF3MMUU\home-reassurance-2-sites[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):	18587
Entropy (8bit):	7.945704403895065
Encrypted:	false
SSDEEP:	384:mjODAQfvb0ZuHVl0RKm2BTZFNOsKZKb4jtmyItcno5a56hgmab6:mjODAKQZQj0Im2BtaGb4j4ygcn8n/Z
MD5:	289A303FAAED46155A885582F534B026
SHA1:	C79D3DB5817D00A9F1E806BB415308584E52A578
SHA-256:	FDC8D2CD5E3523C17C50A25237B00B87045E5BFF97CC08DFE8A1EC099240399F
SHA-512:	AAA5BD231801EB5BDEAB05EAC2A75CB8D45617B7292AB08C785B897C1B332D671CE6FA280C04389F0CD0597464DFF5F21F7736A55EE0F9BA4FA63A19887563 E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.sitew.org/images/blog/landing/2021/home-reassurance-2-sites.png
Preview:	.PNG.....IHDR...,.....`..`..HbIDATx..}{.m.U.o....8..{...}.6.....`.....[.D..GZ.*b..!.c.....5b...#..Q.Q.....R.}..Rn.m{....{..X.1..s....{.1./.9..{....7.c...c..psss..6.[..... .....vq....N....M....{.F...4....*.....,..I.eXT.8..f.....g..M.h...<.Y..M..F.?....W..5.eY...".."..a...g .1.....9W...O....n...]..._.'.zo:.^+.rJ.}"./...`....0.*..@tX....m.....).....=...O}rZ?.c0....w...(.|.....z.....0.p2).....i...z.1|.../<..?...N.G.<..QR.qV....z.....84...87.....f3|.W}.l....,...b}..\&5.. 5.....OA.?...".3...L....~..../.^<Z}.....U...}6..}...8...g.....\..).....4..g?;.u..%.O.....w>.....O~.....E.....z..y..=....p...5&+o`.....a..^.;J._8.NJ...g.~.z.a.3....TI..7?.....~...k..."j Cr.\}.....|V~'..an...M.....Cf><88....}oC|..y...W...J.o..|.[.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\leaf_2[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 57 x 45, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	388
Entropy (8bit):	6.831283122151977
Encrypted:	false
SSDEEP:	6:6v/lhP7hLKEEEEEEEEEEEEE6dPgRYj0XN0JKPLbdehTiJHC46kVXwyLrSsJS04Sc:6v/7sg7FE2Jmk9wXsg0Xc
MD5:	2B63261AA40DAB03A965F6F084251B47
SHA1:	96FF7517AA202D41795B39EBF990EAF631293F0A

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\leaf_2[1].png	
SHA-256:	32D09A900473670BDBCA8622B3FA88CDF0907AD9FE8DEB046D4B8F4BA4EDCC8E
SHA-512:	A91A4E14CD13FE9DB0FAD887F2F0FF917E33DE9517B2C2329334DBD3183AEA94221AE81B5865A40DEFBAD740D4BB4504E846D604006B38EDA0843F3CE7A162 D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.sitew.org/images/blog/landing/2021/top/fr/leaf_2.png
Preview:	.PNG.....IHDR...9...-.....#.3:...3PLTE.....]&.....tRNS.. 0@P`p.....T.....IDAT.....r. .....0.?m>U.n.....g....%..f.>Y.^..(9..x.S.Gu.+.9g...8).&pZ. .q^.o...P.p.(.8.FA.)Q.0xJ.....5*2.HI.P)...%.....Sc.6J.....S...(i..J2:O....T.;%..5..Q.1$J..AE..(1.+...H..T(...9.....%\eN...q.8.mx.9.E....J..GZ.3.1.o.j){.....ymkl.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\microsoft_logo_ee5c8d9fb6248c938fd0dc19370e90bd[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	3651
Entropy (8bit):	4.094801914706141
Encrypted:	false
SSDEEP:	96:wO4DZ+Stb/jY+eo4hAryAes9mBYYQgWLDm9:wToSBjlevudl9nO
MD5:	EE5C8D9FB6248C938FD0DC19370E90BD
SHA1:	D01A22720918B781338B5BBF9202B241A5F99EE4
SHA-256:	04D29248EE3A13A074518C93A18D6EFC491BF1F298F9B87FC989A6AE4B9FAD7A
SHA-512:	C77215B729D0E60C97F075998E88775CD0F813B4D094DC2FDD13E5711D16F4E5993D4521D0FBD5BF7150B0DBE253D88B1B1FF60901F053113C5D7C1919852D5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://aadcdn.msftauth.net/ests/2.1/content/images/microsoft_logo_ee5c8d9fb6248c938fd0dc19370e90bd.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="108" height="24" viewBox="0 0 108 24"><title>assets</title><path d="M44.836,4.6V18.4h-2.4V7.583H42.4L38 .119,18.4H36.531L32.142,7.583h-.029V18.4H29.9V4.6h3.436L37.3,14.83h.058L41.545,4.6Zm2,1.049a1.268,1.268,0,0,1,.419-.967,1.413,1.413,0,0,1,1-.39,1.392, 1.392,0,0,1,1.02.4,1.3,1.3,0,0,1,.4.958,1.248,1.248,0,0,1-.414.953,1.428,1.428,0,0,1-1.01.385A1.4,1.4,0,0,1,47.25,6.6a1.261,1.261,0,0,1-.409-.948M49.41,18.4H47. 081V8.507H49.41Zm7.064-1.694a3.213,3.213,0,0,0,1.145-.241,4.811,4.811,0,0,0,1.155-.635V18a4.665,4.665,0,0,1-1.266.481,6.886,6.886,0,0,1-1.554.164,4.707,4.707,0, 0,1-4.918-4.908,5.641,5.641,0,0,1,1.4-3.932,5.055,5.055,0,0,1,3.955-1.545,5.414,5.414,0,0,1,1.324.168,4.431,4.431,0,0,1,1.063.39v2.233a4.763,4.763,0,0,0-1.1-.61 1,3.184,3.184,0,0,0-1.15-.217,2.919,2.919,0,0,0-2.223.9,3.37,3.37,0,0,0-.847,2.416,3.216,3.216,0,0,0,.813,2.338,2.936,2.936,0,0,0,2.209.837M65.4,8.343a2.952,2.9 52,0,0,1,.5.039,2.1,2.1,0,0,1,.375.1v2.358a2.04,2.04,0,0,0-.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\mockup_mobile_Templates_HD[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 457 x 784, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	32256
Entropy (8bit):	7.930989290860849
Encrypted:	false
SSDEEP:	768:hPgEJkZYdl3GF/HIZ9sMyjek3qpz8VyY2+4BFlQDCZRGJ:hPFkZYnfZ9s1K8VyLBnQu0
MD5:	84436DF6C315EC37546C849DB0CAD67D
SHA1:	F5B4D047A43C5B8F83820640444C253F59812D04
SHA-256:	64DD6C9D1389A9949563D2BF541B92DFB6BBA135419E561EB49E507EA88A1D9E
SHA-512:	4F676860435F43675522CFBCAFB9BA26434A90DA7439A70C67F38040CB95E789FD6D893B00930EE2312E2538DE83E1CEE5D5119A7DC874FED64FFD84E88A75E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.sitew.org/images/blog/templates/mockup_mobile_Templates_HD.png
Preview:	.PNG.....IHDR.....L.....}.IDATx.....W}...UW..J3.,Y.-./..&...\.1.8.....<b...{..p.....,..c..!.lf...,...R...T.L.,.....,_..u...._...FCj...r9..l&#.j.~,.LJ...<)....}.D"a.6..I.|.|.e>.....1] .y.3n>^.T.5.....K.X.*...'..~.~.....cO8".....9)}$.'....u>L..[...H..~.....8.s.[p=o.^...;.y.=.X.....fGG.4..b. ..=..c.9..1.5.Q.o.c.....ce.V..9.....y|.1'<..qV.^?n~...c.....6_c?'..3.J. .k.....4..D!il3.x...>....fgO5....k..ej8..n 1...E7.J.x..w.....:..a.h.....7Lx..o..4...&....~yaaa.y.N.(..7.O....o7.E}.'<.o.2.WH.J28+...jO.U....?.....X...Q.?...=.....`.7w..).F.b.....l.Ff.... (...Z.n.f B.Z.j.R).0.....}[.....nL...6..M.P.y..7$.IH....N-.J.j6...Y.3c1wJ..^H...O&Sa0F..T.Q(.M. ...lNFR.@..q.....r..<0,.....S..V....,.KR*.w.J...R.BA.....]..b.2.%...op6. ..2Q...[...4.6..e.&... ..dM8.l.5..*..J+5x....Q..!....9.CE.`..HG.Z.....[.....c6...5..:V.....;-..f.../.....]k....8y...p..>..X.Z=.X,..P...|`{6;jC

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\person_1_mobile[1].webp	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	RIFF (little-endian) data, Web/P image
Category:	downloaded
Size (bytes):	22714
Entropy (8bit):	7.988571080728299
Encrypted:	false
SSDEEP:	384:3DuKewjxao1LT17bSLc2Yat7JcQwfIdXFVf5wACN/FqJzy02:3DUUJ1F7/axrk+XFVxT
MD5:	E5FA90BA8A26A586379B0BCFB40450C7
SHA1:	4F3E65DCA239D780E504C755FE077B8E94272E34
SHA-256:	A2E11BE3310CAFC8EDBA6BC99C0D92AD05232CB333AB30A0AAE67512D227F43B
SHA-512:	E0EE62A29537C8CF22A2E5D5D5676DAC35846987F3D32DE80331EFD4AB4C0833A526C3AED6295A7B41599211643F5120F6B4355ED0F3CA5B3F32555A2DBA5DF
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\person_1_mobile[1].webp	
Reputation:	low
IE Cache URL:	http://https://ssl.sitew.org/images/blog/landing/2021/top/en/person_1_mobile.webp
Preview:	RIFF.X..WEBPVP8X.....W.....ALPHr.....m.0..o.:G..$A:..*DA.....]N.....!C.b."6.C . ...*..E_.Cq..-'.Pl...H...e).BKq.H.].WA.R.ti.P*E.X...,"!.V...(...#.f&.\.u....Y.m[...t .J/...,..`D...P. ....)n^.>#b....?....?....?.7..;....l>....x:r....:Y.h..l..k..&.C~.Vnx..i.6,n...z..n..)..:Z.'lLXv.e.{....t.....R..).,{.(dW..F.o.!.....n&!.$yd.J.yo.G..2../..0.).$.,+...S..{..".."..I".....9`OB..$..xU.O.4.. .O.....^E.H.!.v..d.B..<..U5...T..C..6..U....|^E.H..B....3.!D.dE.....@.`.J.|^E.$B...-.r.....#+....z.....w..F..D.....3G.....e.bg.... .H.. \|mr..St.9r..9..w...?....:...,.B...[.f....%.'..f..r..-.o ....KW%OM..*.D3.`.40&!D.h....Lva!.{>.?....]...<..U..x$B.....3.!.\)m.e..\...."....B.?.@...=..~.Ne.B$..qi.....r.C.\.c...u.W..!.Z.l.....d...\~..C...:..._Ud.V..<.....Y..d...\.|..T.F..]....r... e.J_Z6..I....L&.].....L.e...H.e.e.\..B.*.Z=.Lc.H.m..p....vo....bYn..._.....[u....?.OM..@.:$Y@...#i.....x.....^.....d..0H....Mv.C.....2tQ.S:s.....q....S5...D.....g`NB.b.S

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\person_2[1].webp	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	RIFF (little-endian) data, Web/P image
Category:	downloaded
Size (bytes):	17536
Entropy (8bit):	7.987487612429157
Encrypted:	false
SSDEEP:	384:I4v90YddWlqmnWPDf3G2CaKSrry7OGJ0OddtpphtTS/:IopWljnWbAIIuJ5dS
MD5:	6216C21B4A5E891B1EC588AF2FB5F586
SHA1:	CAC73DA531E43281BAF389F62CF228D7A9F27C43
SHA-256:	2C5615D90BD6C139D727B338B37F0DFBF5D42C58D9E84327E7FE0ABD06990215
SHA-512:	0444E5ACA40E77E2231ACC2EBC2790E21D39318155B98EC8CA0247804840BBDB11887787BB6AF1468AF4400237B767DBD789EFE7C57678EC30FFA0EEC9CD7B C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.sitew.org/images/blog/landing/2021/top/fr/person_2.webp
Preview:	RIFFxD..WEBPVP8X.....!..D..ALPH.....m.F..c'is.#b..u+..<.`..k.....).....0h..0.0BHH.....@...b.%y-.....{q.z..6..ZH^.6w[6..o..`.3.-..+.I ..E._...s.....y..a.....FH....'.}.b.+.J@.. ...$ ..H..H..H..H..=.....)".@.....|.(u..:7.....#Q.a...#rMN. ..!s.b...I.k1.BYTl...v..rs.y'Ay...P.1....%.u.....6.s.\?.*....O.l...vF.D.....KTeN.R.X(.....1...T.j@U.J.....M..<.... [..Xa...<.n.\.....csin...zC.z.....%. ...q^P(.H.Z.....M.Vk..V..dCQH.9G.k.&,....k.....!.l.].t.O.[w..h..W+.b....h.5>Z*...".|....F.....C.f.....YX.....M....v..x.....r.....g...,.l...S)...R..Vj. .....K.,NP.6...!....l.&wS.N..t.:..'h.JG...!w][G.0.V.,...J....mLvh.....,.f..j...d_.....nT.J.M...^.U.C.$c.2.....sd?.....6.j.Hs...`_!...e%|?.?.....;/.V.....B._..m..E....b.&6.....K....k..y.[D.].@'. .Ea.b..I...n.....D_.. .ikz<.1...? r....a.wU\.,.M.7...\....r_..+.\+.....Bd..q.. .7.O.9.{.}.8.BC.x..nH..O..h..l..?N...mp&.....z.My!.@N(.]...{@N..3p...8.Y

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\picker_account_add_56e73414003cdb676008ff7857343074[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	222
Entropy (8bit):	5.004415423297573
Encrypted:	false
SSDEEP:	3:tIsqDmJS4RKb5zMc7XpCN+bJMacvRxyJAgR/QvfqhcDQKG2TcVER+HLZqWTboZUq:tI9mc4slztdbC/yXADQKDTcVEqLwDZsc
MD5:	56E73414003CDB676008FF7857343074
SHA1:	9ED7A58CD0E81E9689AC8C6D548A47D0185E0FDC
SHA-256:	749F85621D92A5B31B2A377A8C385A36D48A83327DAD9A8A8DA93CD831B8C9A2
SHA-512:	FAD0071AC2DFA23989BFBC7D3850415F3C340A74A54D3D8D797AFCCD6A301513BBC769DF4E5148605BE1E23A8750973EB80726F3CC959A2A457B0EC09AE14F 7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://aadcdn.msftauth.net/ests/2.1/content/images/picker_account_add_56e73414003cdb676008ff7857343074.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="48" height="48" viewBox="0 0 48 48"><title>assets</title><circle cx="24" cy="24" r="24" fill="#e6e6e6"/><path d=" M25,23H36v2H25V36H23V25H12V23H23V12h2Z" fill="#404040"/></svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\product_background_front3[1].webp	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	RIFF (little-endian) data, Web/P image
Category:	downloaded
Size (bytes):	22936
Entropy (8bit):	**7.990228564663952**
Encrypted:	**true**
SSDEEP:	384:kQUmNuhmurTgTxnYYylGXslM5L9IcrnRmzQzZ8z5MmKsDzLZFsepPnbwTMfpz8RN:TUeuhmurUpYkqC6crnRCnJzLZFHpPn1c
MD5:	F51B52BAFB6065A944EF3906C65CD979
SHA1:	E76A3682A50F161C45393F957111C5ADDE5E3986
SHA-256:	C36E1AE944C71476019AA650A423A3C86A88F6EAAB5B854DCD0DA2B4C26F7D3A
SHA-512:	3AD58B1F657A76F0D63A342B499B0EC169274ABFCAC71B3982791B883D6BBC2C336FDC211A7E4094B9CC1E0C01D06921A6C3C50F91B2C5BB3A8A0BBB41F5AA 2D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.sitew.org/images/blog/landing/2021/product_background_front3.webp

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\product_background_front3[1].webp	
Preview:	RIFF.Y..WEBPVP8X.....#.....ALPH./.....m.I..:.....&....`.Y $S.....k.!-.....uM.d.z(.+3.PS.#. .....~pL.:..kbi..*Q..~Y.8..6...=...@DL@...../.Va..q.h..N..e....^.@..c.%$m..V...7.i .....m.. .....Z...'.+..\...p..*...U..vw[qOr.<t.V...R+...O..."&@.$.u..F.@. ~Q..G.....w.4.....j..%...R.2...m7.:.v.m.#...s.:g..}....'G.3.....e.-..Q...#.....T{.u.o...._.m....h..Rk.....1..."<^u.\]X.J.. .O.j.Y.m.R.....]Au`;.[....'.o..q.{..... .....i.....8....m.%..U7..m.xnU.Fb.]....@...?4...TPE.#P.9..i<Q.... AbK9..4.....j.9...##.2...U.,{_Nj.k.....h.....$K...K..do{.}5.a.2|`.Z.....&....7....`.V. .}6Tny?...n.6.....r>v.K.vnK..&v..J9u.U..{.`..&....M...h.]......G...[y.V.G.`.....MTwUZ....L..+..<.....e.G..P..H.]fW._/...2.....Q.._...}veu.2({`...Z. .Y-..*....H.....t.....2R.Wk.f3..q.Z... nD.u.....Eu.'.....-B..o.k.....hH.....20d.U..#...ho){.u.Q.K.....6.(...c.....?.Sk..E...._....M_.<wrs#.m`=....U.mi..i)O.W.H>nw.;.l5.U#n6&u..q..[5.h....Z....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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\2WF3MMUU\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?..ll.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..~.I4...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\2WF3MMUU\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
IE Cache URL:	http://https://ssl.sitew.org/images/blog/landing/2021/product_ndd.png

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\product_ndd[1].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\2WF3MMUU\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..l.%..[.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\2WF3MMUU\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\2WF3MMUU\reassurance-photo-fanny[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 300 x 300, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	149911
Entropy (8bit):	**7.990636345677174**
Encrypted:	**true**
SSDEEP:	3072:jbOcLldlcN6iRJlfzmmFZbbIqvr00cUBLBbVa/gdcx2KpmsZo3c:jiyla6WmaZbsqDhbVa/gda2OTZV
MD5:	7DA329BCDA595C6A3B95CB9DF04A8E3A
SHA1:	F309A79CDFD669ED852460BF672250DD4B963EE9
SHA-256:	28BBB1E307B3D08FA1D84CE0440A469DA3CC0697ECB60AFFB36DA26D98461132
SHA-512:	929B21276447B973F378F250184F94CEC9CCEEB6CECB3D796AB45F48EC064DB58A6FB308F141CF684A921525F7B5859F096FD21E015BE2796BBC82D6A649DF6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.sitew.org/images/blog/landing/2021/reassurance-photo-fanny.png

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\reassurance-photo-fanny[1].png

Preview:

.PNG........IHDR...,...,.....y}.u..I^IDATx...y..YZ.~...o....!...!...B.DD[.).Q.j...V.mmEh..k.A.a...auDGw....NM...@!A.......)..*3..{..k.....o.'..j.T..x..}.9........>.AT.G..>........A....xV...U
.i.AU.xV..UE.T@5....L.o jD.D@T.....~.@...^D....z.._.?..w....!..........).oGx.xZ..A.L.AHU.TiT.B...T.R.....F.IE.E..Z..(.qR.:......AUs..T.0..........?.G.....S.8.....>+"...>.50.F".....@.S..#..
5+,...PP.T.4b..".s.S.3.:dz...Qc.6...?S.C....X......E?.|.K..W...].T..}|.|.....g5....T.xFES.B..Su...?..."...`RW....RUL...h.L...bH..0b.....`..3.:......S...c,.?&?...Y.Er.EA#...4n. "...?..:.G..../
.....?....oG..Q=..X4.1.]."1..bRqP..\jt...7tW...Q^5..B$..!uEH*nC.eg......c..N.....8 `.w..o.O...M.z...T^P./.._...=*X.>~.............vUy3..V"f....4u.SgB..;.1L.....@.W..y\....s........$.B..1&.%
.._..Ff.c1......R..\.....K...|...6....~XD^P..Dx.o.........`=........O..#..CU...M......(1FTg.y.B.).Ae..!.0.&.Hh<.2.........x.jz.h..RI.<..!...gE/F.8....g..~..&o&..L..4..<.q|.S.._.... ..x...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\reinssurance_trustpilot[1].svg

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	3397
Entropy (8bit):	4.5339742831567635
Encrypted:	false
SSDEEP:	48:UpodXEJkocQJdcCo6EjJDpvV5oQ0tcNf/XRXEJuPqV3JKUiRIczsR6kJkNgWkcM/:oJalJF9H5+JuPmHJ43JF20tU
MD5:	4BA685D97B0A53CBF57E312A7D74582A
SHA1:	00687828DE604DE7535B68A70EBE1CCAEFC90EEE
SHA-256:	F52942C74CC0F6CC356A8297049E8B599338955717E8E313B8CF017C29605D94
SHA-512:	94564C9B3836ADB601F2D4238572A75BDBF48A9D1296A40CA7134546815407FFA6DF965E952E16305DEDFE6A54A53D9D7D1FF1E78824E72D822AB48A540855C2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.sitew.org/images/blog/landing/2021/reinssurance_trustpilot.svg

Preview:

<svg id="Calque_1" data-name="Calque 1" xmlns="http://www.w3.org/2000/svg" viewBox="0 0 423.1 69.32"><defs><style>.cls-1{fill:#ffefaa;}.cls-2{fill:#ffdc40;}</style>
</defs><g id="Groupe_1306" data-name="Groupe 1306"><g id="Groupe_1238" data-name="Groupe 1238"><path id="Trac._2155" data-name="Trac. 2155" class="cls-1"
d="M1137.76,506.87l9.43,19.12a2.32,2.32,0,0,0,1.74,1.26l21.09,3.07a2.3,2.3,0,0,1,1.28,3.94L1156,549.14a2.31,2.31,0,0,0-.66,2l3.6,21a2.31,2.31,0,0,1-1.89,2.66,2.27
,2.27,0,0,1-1.47-.23l-18.86-9.92a2.28,2.28,0,0,0-2.15,0l-18.86,9.92a2.31,2.31,0,0,1-3.13-1,2.27,2.27,0,0,1-.23-1.47l3.6-21a2.31,2.31,0,0,0-.66-2l-15.26-14.88a2.3,2.3,0,0,
1,0-3.26,2.34,2.34,0,0,1,1.32-.68l21.1-3.07a2.29,2.29,0,0,0,1.73-1.26l9.44-19.12a2.31,2.31,0,0,1,4.15,0Z" transform="translate(-748.9 -505.57)"/><path id="Trac._2156"
data-name="Trac. 2156" class="cls-2" d="M787.31,506.87,796.74,526a2.29,2.29,0,0,0,1.73,1.26l21.1,3.07a2.31,2.31,0,0,1,1.94,2.63,2.27,2.27,0,0,1-.67,1.31l-15.26,14.
88a2.31,2.31,0,0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\sitew-39b59ec7a84ef00cbe4b85e40ce2f290[1].eot

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), sitew family
Category:	downloaded
Size (bytes):	74588
Entropy (8bit):	6.220287609235973
Encrypted:	false
SSDEEP:	1536:E+KJeB6MiEneTlsAIG4TdCF+Ezx/zvvgOCXedhiKyQC6Xia+ByZTTajFKizfD+dF:E+KoB6hEeTlsAIG4TdCF+i/zgOCXmwKP
MD5:	978E298001D1003BDD422BFE502C2ADF
SHA1:	DFCDB15DBFE12BAABF7B808BDFB712759193C16F
SHA-256:	B37440BEAA4DAB995E986ED3BD78AD6160438F24384BD8C309E9080B35E1929E
SHA-512:	CB5E84DF9CD389373973854F64E2BA95CC896CE188B39D0DA43198740189F3F7D79E97E5137371EF650085DB715F1A6225950162A949CCAF2E3F035AC2AADA32
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://st0.bp.cdnsw.com/assets/sitew/sitew-39b59ec7a84ef00cbe4b85e40ce2f290.eot

Preview:

\#..."..........................LP.......................w..3..................s.i.t.e.w.....R.e.g.u.l.a.r.....V.e.r.s.i.o.n. .1...0.....s.i.t.e.w...............0OS/2W.........`cmap.G..........gasp............glyf[
=.........head .>....p...6hhea.N.........$hmtx!m.8.......,loca..^x........maxp... ..!.... name....!0...npost......".... ....L.f...G.L.f....................B...... ....@......... ... .
........4..............4..............4........................ .$.5.?.B.G.I.Z.e.i...h.`............z..........q \ . . .!.!.!.!.!.!.!.!.!."P"a"c"y".".".".#'#+#R#p#.#.#.#.#.#.#.$.%y%.%.%.%.%.&.&.&
.&.&.&0&7&j&l&o&.&.&.&.&.&.&.'.'.'.'.'.'.'+'B'R'.'.').B)J)b)d)n)t).*.+.+.+"-@m.......S.U.`.l........2.F.M.S.b.g.......*...0.2.4.:.<.`.h......!.7.S.~.........9.<........-.9..........7.......8.:.Q.S.Y.
[.b.i.n..........8...M.|.=.@.....!.R.\.j....X...K.g.j.~...0.>.d.v......... .#.5.?.B.F.I.S.e.i...h.`............z..........q \ . .

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\templates[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):	19901
Entropy (8bit):	7.9571696248967845
Encrypted:	false
SSDEEP:	384:fWIO7JOpnQl/DAeV0HqsDovFS/fQjp62NgLJW+kmEWgRgGk89H3hD:fWZ7JN/sCoqsDffQjp6OgLU7LWg2Ul3V
MD5:	E3BD289C2F07FB9106C8347ADBFE1692
SHA1:	C1FD48AD2474A0E6A22CCD8D3C1165624B3B084F
SHA-256:	8AB9B0D91C93410A4088FAD4E64EC452129F662DF8D0F0959E505106B3189DA6
SHA-512:	03C1CB7F24B2EEE7769340D33B4B8C7A006BB0D0B7ECCFA70B5879901B39726B14CE94DFE8A5FAFFC65AFDC74190F891D063D066961E89755BC508D3F393169 B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.sitew.org/images/blog/welcome/icons_menu/2021/templates.png

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\templates[1].png

Preview:

.PNG........IHDR...,.........`..`..M.IDATx..k.e.q...>.....<L...)R.EI.#..B.VhAN,.CG.....'..I.........KA..I`....t,.rD.!i#...2)R...3........t...{....V.......t.=U@...{.>......V......v/...............................
....P.""..n.....7.-o.^.mK...#LD#.M...h... ..&.....#.....
.L`..t...0G...!>...M'..A.c.......M...r..B...a.y.S.7..0s.`AD.[......KS.>..@8f.M...z..'N.}...<_^..V........'p>kwv.1..a...~.O......~.gn./.\.i".Y|p.........|k..._]x..[...gqQ...8...5O-.....`s........N'....
....^.S...GD...^.01.k1..=...../_^1...D.....{X]=...zW.oy`.[L.h..`...S.....1..C.j8|\..{..}<...D.?.........8....N_y.......%.2.@'.>a.3.f..O.>..sg.,.^.1..2c~.hz..?..g...../...].....F.._.....s..._....: p..Z
..&'.?.....&7.....0..g........9V...........,..r.....>.^3.7.:.....[.S.3...y.~...P5...........h.d..];...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\12_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):	109307
Entropy (8bit):	7.836048438526025
Encrypted:	false
SSDEEP:	3072:2OCDsfGCDQpz/qwXWSYDsuYA4x3n3BPZz6uI:2lIApzywXWNYA4x3n3B16uI
MD5:	1B0FB65D2720D05C58CE2FEC9A7847B5
SHA1:	AC1EB94D019EB5FA77F4EBA15DEACCC37CCD844A
SHA-256:	0BAA667276318AC2BE15D34E4468F1278F083E7648FD253F5D6456BFD54C3BCB
SHA-512:	D011A0422EED4D9E6246C43631538A77132692A8C6A3CD935E93356B6B4F7435B3AE14E9B87402E669376912CEF8A3C814762EC60FB169E939B0484E5FF02BEC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.sitew.org/images/blog/templates/v2/12_desktop.jpg

Preview:

......JFIF.....H.H.....C....................................%...#... , #&')*)..-0-(0%()(...C...........(...((........g.."..\...................
......!.1.AQ.a.."Uq.....2S....#BV...$346Rr....%57Tbst....CE..8c&DFu...v..............................:........................!1..AQa..RSq.."......#23r..4B.b$............?..R................N.]kwj.
.U:in.Q.(.r......|.....?......>..l...8....G..c..u...wj.........t_.YO...Z..Ju&...
'.#..A..W.}W.:...iW.........e,6..~.G.;.*.....A.k......S..j..Hj.[.....q.8.....&.S`}.i.j.'.>.X....c...0|...N.f]i.u7KS.J...X&...QK.....q......u.k.GN..?,.VJ.T.Sb...O...I...5#Z.*..g.%.2.:*q..R[....l.S ..5M
[Y.o.hS.......\..wV.I.0.g.F9...^V8..w.j.:U...P...F...*...|J|...R}...~}2..[P.m....Y].N......{..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\12_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):	63058
Entropy (8bit):	7.907405652867074
Encrypted:	false
SSDEEP:	768:FhgdSkwXKEiKo9Penp/GK/UqYmHaJjp8zaHqiIKqgVzMb1Fpyv7pDjEAPOxB:vISDaEI9C/YvFxKeqaW1av7pPjOxB
MD5:	10DD696B11AEE60650B4FF216083376A
SHA1:	4FD4264D63D97515463D5F86521C611CD08209A0
SHA-256:	2FB658B5F435002004BE162088A60F1D820A57681E8F3788594571E7CD01CC8A
SHA-512:	833EAC4C1041026D8CB7583DD6DFDF7E0A092A2ABA6AC0573A11EC5A93AB6C403C5B7BC6D7B8468FF772BF0A36D30F22F6329CC2706C37A194B0D3B08BBBAFE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.sitew.org/images/blog/templates/v2/12_mobile.jpg

Preview:

......JFIF.....H.H.....C....................................%...#... , #&')*)..-0-(0%()(...C...........(...((.........."...c...................
.....!..1.AQa.q.."2......3BTVr.......#45Rbst.....6Ce....$%&7SUc...'d...DEFH..8..............................7........................!1..AQS.....R..."aq.2.#..Bb.............?..`...............................
....'R.i..9.X.).&.<^{.@=J.~<.B...mM.g........I..q..V.....=[.............qY...p..@.........6j..".Fp..'..u..Y..9...
....&...gyB..\..T.XK.Qi.n.K.m...F...j\..9.$.$..r..`{.....*.3m:.bs...?......'.9s..G...........MT)...o%[...c...[.._..H...?.@.o.r..^...|.....r..^...|...6~.}#.P..U..
...C.T....{N........aif....F.,e.<gd........k..gut...R...U.U .8J..p.V$..<.............................

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\1[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:	6:OdkTTyQgdD/qdv7dnp92kqdzLhqdvf92kqdvFZJZgdML/qdvYJO:okLqDMvhngzLavevFfcMLMvYw
MD5:	9DF4FDDB8CE1CF4C3AAF5F530947B843
SHA1:	2F29AF29F6D4840201B7DCE34B489D5AA056AC05
SHA-256:	E58BFD62D5F8F293F1E6F90EF89E45B8D49623B0FB3F534F29B1094E0C2A91B1
SHA-512:	762C6F16D331F613767FC98714E1A0CB5B3536109DB16E7FE3E24DB776B7B5B5FF1F1B57B97584E429C71EBE6B4A261EE94599604C368A2E872F9330B24BBA23
Malicious:	false
Reputation:	low
IE Cache URL:	http://www.keeplaffingwemake99383tyiwye.net/assets/precompile/gt/button/1.css?clearcache=5

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\1[1].css	
Preview:	.gtbutton_preset_1{position:relative}.gtbutton_preset_1 .button_block,.gtbutton_preset_1>.site_button{background:#002}.gtbutton_preset_1 .button_block .button_content,.gtbutton_preset_1 .button_block.site_button,.gtbutton_preset_1>.site_button .button_content,.gtbutton_preset_1>.site_button.site_button{color:#000}.gtbutton_preset_1 .button_block i,.gtbutton_preset_1>.site_button i{color:#001}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\21_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):	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\9026IKNJ\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_content,.gtbutton_preset_2 .button_block.site_button,.gtbutton_preset_2>.site_button .button_content,.gtbutton_preset_2>.site_button.site_button{color:#000}.gtbutton_preset_2 .button_block i,.gtbutton_preset_2>.site_button i{color:#001}.

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\33_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>101276</td></tr>
<tr><td>Entropy (8bit):</td><td>7.971399150234189</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>3072:VIHX72eqwFNF2fy2gkHSCH40n/ZSjkUbHTNH0DM:VXUFN062guSZkEz90DM</td></tr>
<tr><td>MD5:</td><td>F9D78D0E78CAB11991AE53D744425B2E</td></tr>
<tr><td>SHA1:</td><td>2B4DFDFF93CB648E08AC66B36E64C9A73804C104</td></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. ....D..TQCAIF.c..2..Z....aa.}.>];...#..\-....i.......9.w..8k`..." "".".""."."".".""."."".".""."."".""</td></tr>
</table>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\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\9026IKNJ\4_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):	66942
Entropy (8bit):	7.710765822310323
Encrypted:	false
SSDEEP:	1536:/WWWWWWWWWWPmwOGsNIYH5WNdMLa8kJbWv4UbjPxIX5mD5RRZ:ZOJNN2OazJav4S7ipmD5RRZ
MD5:	A77B87FA3DED43AFB71864496106689F
SHA1:	88862C55F7D6A5AA60AEEBA52218CA8099E84520
SHA-256:	362A18969FD937A0AD76ED400F175CF4E535BBCBC46AFA3DF3890FC784DF91BA
SHA-512:	B0496830484120A8053B20A99DD3FE8029F1201A22337EB57A9413463A558F5071D06062B202DF2954F9F405F65525DE6DCD62944DA5A2F75A082338EA62E7FC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.sitew.org/images/blog/templates/v2/4_mobile.jpg
Preview:	

......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...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\51_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, 1240x1240, frames 3
Category:	downloaded
Size (bytes):	115831
Entropy (8bit):	7.903628420591862
Encrypted:	false
SSDEEP:	3072:7ych5tQ+5eiD4JZ8cccccccccc8kAsSU4SNfP23FSv:77h595e+4US7a3wsv
MD5:	C7B67DCF3C56D605303C080AE617F51D
SHA1:	F1B5BD5C5CF4DD3D1B84E28621C686B55FC53D13
SHA-256:	AFE5BBAC219AF58A087EEB613B4DE13ECB14F5D7CD4E1C90A04F32BA84B1D894
SHA-512:	16D7C70C8007C9601593555164F98CDCDFE5632C8C5016EEE4A256DCD42AF208795D43FE50B2521CF7796FA65571E92C74AA70114D811F0CDC305BDE160301A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.sitew.org/images/blog/templates/v2/51_desktop.jpg
Preview:	

......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.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\52_desktop[1].jpg

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..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\9026IKNJ\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:	E0F971EAFCB6D5634B5DD392DAF816B25272F428757B79DD11FFAADDFF9A9B8A6854D27AA705A27D080225423492075EFC3523CDBAE160B01B4A1CE300F910(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\9026IKNJ\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......Icvt .......*...*."..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.$.^R@oq.. B.. C......,..f...g.a.I!....R..hJ..v.6P..`W.l^.?.+...d. 4[..^_.^..RDa...;...W.u$(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\9026IKNJ\6xK3dSBYKcSV-LCoeQqfX1RYOo3qOK7j[1].woff

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\6xK3dSBYKcSV-LCoeQqfX1RYOo3qOK7j[1].woff	
File Type:	Web Open Font Format, TrueType, length 20180, version 1.1
Category:	downloaded
Size (bytes):	20180
Entropy (8bit):	7.97320012816743
Encrypted:	false
SSDEEP:	384:S3ECNC9EU5uXBx/d17jzOBmhUXQOTF3IHrYZEFeWXU5ebGLtCjUdtjVOTg:S3EC2rMXBdjzOBRx3IHrYOFeWLotCYL7
MD5:	5CC3AAE674EA3B199313B3B83BD795BC
SHA1:	993DB0EC4347B0CC53128CFDCBB767606D8A3576
SHA-256:	38399EFE707A8FFC12359A0086E7340315B42194A10FD2E1D1288BE12DA9E39C
SHA-512:	2346622E53705ABB58BDC45818D497CB17E9F9869B546CAF298D1E4D4A2D7E15B5A3C3EE8E6779D64C4C4BB0F98A58216A394BCA81F6660AE137FC6326B4895
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/sourcesanspro/v14/6xK3dSBYKcSV-LCoeQqfX1RYOo3qOK7j.woff
Preview:	wOFF.....N.....GDEF.....6...F....GPOS.....f.x.{GSUB.....{... J.c.OS/2...8...V...`[.t.cmap.....3cvt .....*...*."...fpgm.....s.Y.7gasp.....glyf... ...4...f.....head..E....6...6....hhea..F.... ...$....hmtx..F .....P.=).loca..H4..."...*.s.Tmaxp..JX... ... .3.zname..Jx...A....[.s.post..K.....SF.prep..N....S...V.c..x....@....{..::#0. ZGK..`....R...^qT..qW<^..../....x....a.....f.]C..fe.5fs...m.a<]Cv}...7..NG..7l.#.}&..J.....^c.S.....>..yv.<{.C...N...p@...>....$..!.....:...BH...p.C.}).O/..M...t...TB....E....t.....s..L.H _..G3.l.....l?..y.`.....=.....Q.6.e....v.n.]T.....}w..iz..czc;.....C....Z6...m.2G|....b.8....x|I'T..Lb%.xI'Q.H.p.%..."UbH.$.%..I&SR.&.4.$...RP2($a..4JJ.e$...M9...DSA..(.T.< *S.xjI:Mh..vD.^.. !t..)t.'i./..`....&.1.%..L".)L.a.8.....#...@|..."..Y....J..$.....f%k.a.d.N<...r..6.#...}.gf~S.9.....A.A..affff~.....Y.TZ..j....E..N...pO.l..Ze).....`.V..[.c.W.10./.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\6xKwdSBYKcSV-LCoeQqfX1RYOo3qPZZMkids18l[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
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.....lcvt .....*...*....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\9026IKNJ\6xKwdSBYKcSV-LCoeQqfX1RYOo3qPZZclSds18l[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 19248, version 1.1
Category:	downloaded
Size (bytes):	19248
Entropy (8bit):	7.970518757485756
Encrypted:	false
SSDEEP:	384:wCdVwGEC63uXBrHasvZeCtXiGpaKAmy9wSKOG2sQnRNbr2:wsVwBh+XBrjenGI5m/1BWna
MD5:	15776EEC451FF4C88330CC66EDD9E1E4
SHA1:	3428D0CE8BA520CAB0ED8748FDFDB18D244C094C
SHA-256:	9EB48DFACBA6024EACB293382DD7CAC4B3916C2EBFEF494FEA3F8FA9D1D169BE
SHA-512:	195B2E0E3FB3CDE8E4721DBE73109CACAE4262437BBE80BD92D9C12E8F8F32DC7982E42A2BB063A54F63C27A79FDB4285009D77D7AE00E68365D2219ED8FCCD1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/sourcesanspro/v14/6xKwdSBYKcSV-LCoeQqfX1RYOo3qPZZclSds18I.woff
Preview:	wOFF.....K0.....GDEF.....0...:\..GPOS.....;...b..GSUB.....#.#.OS/2.....Z...`\.v.cmap...`...k.....lcvt .....*...*...9fpgm.....s.Y.7gasp.....glyf..... .4...d..?..head..A....6...6.!..hhea..B0...#...$.U..hmtx..BT...R...D.o.Dloca..D.....$[.ukmaxp..F.... ... .+.Uname..F....G....^.u.post..H(.....prep..J....R...V4...x.....0..... .....v@.C.=..xz.>....ZY...x.W...W.}.1...d.....0P..9..3..<7.....`_...:...d}._}Y+.....r..3.?....D..o{.a.D!D.]wt...].?..q..g\.?..T.`.j...=~tEo....w....L....Vh..q..(Aw....}.d...c..9.[H\.\t8...G... ..d2.....B.z.'.\t6.0.p..6...\..p....F'".....q.,.....>D_.C.~..=....?>...P..B....r..B%...(.:.B.BgT.....E(@W...bt.J.C.B9z...[....Ur7a'..Ta/....*.(T...+....0....%8Bh.#.2.....IBg...$/.e(..B9..|.....B' .[...$.....g.".T...B.~.*..x...c..sEs .E.0.0.a;.k.....^?c.Gp...Z.....YZT.*L.l...Z..sY....l...3&.....\.....e.S..%u6qm.;".}D.Be@...$c.....3Y..s.#.....j.L....,d.:.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\6xKydSBYKcSV-LCoeQqfX1RYOo3ig4vwlxdo[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 19896, version 1.1

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\6xKydSBYKcSV-LCoeQqfX1RYOo3ig4vwlxdo[1].woff	
Category:	downloaded
Size (bytes):	19896
Entropy (8bit):	7.973207257576149
Encrypted:	false
SSDEEP:	384:vi9GdFUguXBNV01KI0EhV+xnP+gu9ZLpanYwJz1aRRxaFsq+6LVnQVOTa:vi94iVXBYQnmUYwJz87kLhxnQVOTa
MD5:	B03F2EC28F8E60E61974DD8C57610E5B
SHA1:	DFF9B2C95F626F894185C98CFBB976BB98B50F33
SHA-256:	D8DD0DE638293EB62DBA15A6E410FB0AF9A5B36C35DF226237B1B609D573C63E
SHA-512:	A585B769AA7CD7311FB4075DB5EEBE09E65A46CEA773639482DE0EAAD248C0BCDC571BEF16BCC9EE1196596014871FF39541AF66C1A53FA8B026A82C0F0090D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/sourcesanspro/v14/6xKydSBYKcSV-LCoeQqfX1RYOo3ig4vwlxdo.woff
Preview:	wOFF.....M.....GDEF.....6...F....GPOS.....f.o..GSUB.....{... J.c.OS/2...,...V...`\?v.cmap.....3cvt .....*...*...9fpgm.....s.Y.7gasp.....glyf... ...3...e.q.B4head..D....6...6....hhea..D.... ...$....hmtx..E.....P.k!Nloca..G(.....*.].(maxp..lH... ... .3.rname..lh...8....X.p.post..J.....SF.prep..Md...R...V2...x....@....{..::#0. ZGK..`....R...^qT..qW<^...../....x.....]...w.jm{..m....m...m.F1.n....|.....8....w..Uj.6oWkX.....?..0.{...{3....4.K..pP....(.{.%..!./(.x....}C.d.`.....29x.@...+.!.....Q...T..*+]g.^p.9. ...x.agI.W[jg.m.K.....-.c.E.D.....6..r...!.7>.....X+.ok..+7k.o.yj.%..<.uw.*....v.N...>...L`.....x...&..I.....4B$.p. F..4.$.D.#I.I.HR$.TI$MbI.2.,rH%WR...t.P.T>.T>.L>.,>..>.(..... \.....I.....)B8E%.b....H.4.I...I..u4.!Y4.114..)..=.....t..>z..^.x.#^.....3Pr.$~.3.I.H:.....FmS%.R....#.S..cvE...6^[...v....Z..`A..]R.hg.\S../w.([.s.n..y.{.....osc....At.....x.%Q

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\6xKydSBYKcSV-LCoeQqfX1RYOo3ik4zwlxdo[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 20204, version 1.1
Category:	downloaded
Size (bytes):	20204
Entropy (8bit):	7.9749078907666116
Encrypted:	false
SSDEEP:	384:qxWQ/O1lUMuXBGWZrkF3UZfWXeKcJL0SjvO86XbyNFA6xRGaElAVOT9:qxTF5XBGWZrkVuGeKVSydXbyNFHxyqVE
MD5:	A5002963B0570A073E28156403C78670
SHA1:	8DF8BC2936228257335163236651178D5BC400F
SHA-256:	4C24262A87FDF021D377BF7E4D6C08CE81A1862E774FACCA70713391A4CD3BC7
SHA-512:	4D5AA58E055081B5146594FD77B8940B3FD872907F60F74E0CEAD3420FF041FA4E0A415CC8E5304CEDF68F1259FCBD06026CEF48125AA9D9D91C4290DDDA67F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/sourcesanspro/v14/6xKydSBYKcSV-LCoeQqfX1RYOo3ik4zwlxdo.woff
Preview:	wOFF.....N.....GDEF.....6...F....GPOS.....<..GSUB...T...{... J.c.OS/2.....T...`Z.s.cmap...$.....3cvt ...<...*...*....fpgm...h.....s.Y.7gasp...d..... .glyf...I..5...h..$..head..E....6...6....hhea..F$... ...$....hmtx..FD.....P.3..loca..HT...#...*....maxp..Jx... ... .3.~name..J....:....U.p.post..K.....SF.prep..N....R...V2..6x....@.... {..::#0.ZGK..`....R...^qT..qW<^...../....x....dY...B..]].v.x~.m.^...o.m.m.z...z.>{"6#..i.B{N....7o.nJ@7/.0.O}.s_..[...{Y....=<..o:..<.*...f.]N....y...@...wz.....aK.x.....h.....2../..-.... ..fj.y.G..OX>e.x.....VK..E.{}.t,....m.....W...._..cX..2Kn....N .c..5.....)..6.}.....j0#...06I.;.W^.?.g.P....y~./.5e.3.|...../.6~m:.x$e.qa..i..c.....f.P7.Ybv...a.....''V.K.0..4.2d.c.1...0;Ye.... b.....+x.9.....d..`s!.1.<.\...Q..c..8s.g.<...E..b.....ky.5.....;x.....#9.^}.q]..f..e...i.Kf./.U.bV..Y.k|.+.i..m....L...5...^.....TC.,:....|...i.nD..m'....9.....4.!..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\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
Preview:	wOFF.....x ....GDEF.....*...8...xGPOS.....E.`...GSUB.....@.xOS/2...X...P...`[.'.STAT.....9...D...cmap.....z..Scvt ..!....Z....)V..fpgm..''..... 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.....I./...#..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\9026IKNJ\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\QGY_z_wNahGAdqQ43RhVcIgYT2Xz5u32K67QBi8JoA[1].woff	
Entropy (8bit):	7.98370330936173
Encrypted:	false
SSDEEP:	768:0tSYsZLAMbfkwgWqSua94cC8Nt6xtusf3:F2qkwtvua94Kt6Lb
MD5:	93B5260A7C4C11D8D4B0DB28C406783C
SHA1:	B4745A622DD2F3E0E77D30A90CF5C878A359F3DC
SHA-256:	7A8E60EE675A444A2E0E40619083A090E6623BFCDCA719726376662B67672940
SHA-512:	23B715D0C1D85AB61335B5946AAAD594B3043B550BB33963F07B34320046F106B79488EEBB0870B54B93F6B6C99F9ED3795A6713E9D6A9170972C7E817BD7206
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/worksans/v9/QGY_z_wNahGAdqQ43RhVcIgYT2Xz5u32K67QBi8JoA.woff
Preview:	wOFF.....{.....$.....GDEF.....*...8...xGPOS.....E..B[.GSUB.....\|.OS/2.. \...P...`].&.STAT.. ....9...D....cmap.. .....z..Scvt .."....c....,..fpgm..#..... 6..gasp..).....glyf..)...J'...${..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\9026IKNJ\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:	9213A98E1FA04556EB4BEE5FCD6EF4C797FD2F53DB0DC2778C1592A8C16B4EE2090B00C892B15AD5DD6731C7F4FF03246DDB9C9447F228FC06DE123FF370D0A
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\9026IKNJ\about[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):	24063
Entropy (8bit):	7.977954246035982
Encrypted:	false
SSDEEP:	384:cH1KXCYUG2kcvNraYB2EhvshVjQkCx08bttoBljRNTlKf8vNaoOKJ4+4Pz8nd:ia0GVgNnocsjjBCx9ttUljPo0HOQRq8d
MD5:	6FFC7C087ACC28686925A22303714E85
SHA1:	EDC9AC9B72E1E6539010DA3A8F7D14A23783070C
SHA-256:	D32504DFFC38CAF402B49591DBEDB88F370215B1C85244D04787BF290F4BDC67
SHA-512:	BEDEB350B510358553CB017B0B4AD3A9C1F0A9DA7F4594AAD07EBAB8A8EDEA5E787DA1F203A668E664BA80C9B2F02A9886ED9D0DDB63E83C02B1B155D8EC0E2F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.sitew.org/images/blog/welcome/icons_menu/2021/about.png
Preview:	.PNG.....IHDR...,.....`..`..].IDATx..w|TU.....;5.'$!!.7)...b..u].ZW}....]WW]..../.^.DPzI.@z2..s.?..a&.. .....L2...{.....<.a...7n...~..q....7n.X.q.....7.,n.q.....7n.q`q.....7n.8..q. ....7n.8..q....7n.X.q....7.,n.q.....7.,n.q`q...7...!.L$.....Pj<.:.. .`.... J... ?m...c...%.]...d..a....._.....#&d....B....H.5&*2DJ.lv.$.t.F.)).....n.-po.$..j....nX.d..*.....p..e..WX..D;..<c ..I../.3q.C...../.....,MM.N.Q0.. ....`.`.8t....,Cm..h.....UuM.~[R.....4g..|. .....8....g:q.....?..A..d..t...t.....(B..D..1..[..x.5.aw.iw"#.HI....5.[.m._.c.....\.vc._.n.X.@.`.Q.'.u...8.... .....V.... .....HAf....xe.|....y./....E...V.....}.G.9...F.>.$A....>.....1W.)D...<;2.....i..g.....6m...W...V..R05.....i._v.....>y.....A@.B .3.A..d..#?. D!.^..+o~p.#....._^n.X=.TY9...>.K.p0 d.X.....Qd...(c..Fi...T`..o^}..;.X.da}.g...+.`.p...O7.z..w.P...g.B.^.....(..u.oq..s...|...^...V.....j.I.....w..:..x...:.S4....9QV

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\ae-v3.2[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	5453

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\ae-v3.2[1].js	
Entropy (8bit):	5.217821098823755
Encrypted:	false
SSDEEP:	96:t+qc8HzQF7G//Sbv0L4wrdSmfPCnz2zfKmvC9/o1U3gJ3rxgrNof730YIMtrIUBS:tbc+QFZwNr/XCQrC9/4UQJ3rxgrNoztO
MD5:	FE072BD8C830BE964FB72862B998990D
SHA1:	3474546D0505199073ABB6B53A25B5C954FE7E09
SHA-256:	897F9167F12C64D8BC0ACBA61E31E09DE4E0A3EB448FFC775046C79EB6BF679B
SHA-512:	87F4292F91A06F687995B2C59260940DEAA17F2BBA533B18DD4ED1A56EB84CE63533082DEDFB03AEB28FD5C68CC19162FCED09127FAF5FD171CE6BED030A6E30
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.affilae.com/ae-v3.2.js
Preview:	var AeTracker={readyStateCheckInterval:null,cookieRegeneration:"",isAdvertiserFirst:0,initTime:0,init:function(a){a="object"===typeof a&&null!==a?a:{};this.version="3.2";this.pid=a.pid||0;this.host=a.host||"https://lb.affilae.com";this.advertiserFirst=a.advertiserFirst||21600;this.allowSiteUnder=a.allowSiteUnder||!1;this.allowIframing=a.allowIframing||!1;this.forceReferrer=a.forceReferrer||!1;this.ip=a.ip||null;this.tracker=a.tracker||null;this.customVar=a.customVar||"";this.ptID=null;this.debug=.a.debug||!1;this.timerLimit=a.timerLimit||10;this.cookieNameForIP=a.cookieNameForIP||"AeIP";this.cookieNameForAdvertiserFirst=a.cookieNameForAdvertiserFirst||"AeFirst";this.referrer=a.referrer||"";this.debugId=a.debugId||"aeDebug";!1===this.allowIframing&&top.location!=location&&(top.location.href=document.location.href);if(this.forceReferrer&&"undefined"==typeof document.referrer)return this.log("no referrer, now exiting"),!1;this.readyStateCheckInterval=setInterval(AeTracker.checkReadyState,

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\analytics[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	49153
Entropy (8bit):	5.520906949461031
Encrypted:	false
SSDEEP:	768:/yR3fYFBLbfs5sP5XqY3TyPnHpl1WY3SoavFVv6PU+CgYUD0lgEw0stZM:/y9gZfl5h3UHpaY3SoRCw0sk
MD5:	6DF1787C4BE82D1BB24F8BFFA10C7738
SHA1:	3634E839429E462E49C5F42B75FBFB4BA318AF6D
SHA-256:	2CB09C7B3E19BFC41743CA3624EF81C3258D56525647FEAC76AA757E0292627A
SHA-512:	CB3CE2BCEB61F390298C21E470423CCEB6DD93E648A7DD0467195B11FEF30BF7A086DFF47C4494E2533498D1448C1A22AAB1414C14FD73278F1C92E0F7BC3F54
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.google-analytics.com/analytics.js
Preview:	(function(){/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var n=this||self,p=function(a,b){a=a.split(".");var c=n;a[0]in c||"undefined"==typeof c.execScript||c.execScript("var "+a[0]);for(var d;a.length&&(d=a.shift());)a.length||void 0===b?c=c[d]&&c[d]!==Object.prototype[d]?c[d]:c[d]={}:c[d]=b};var q={},r=function(){q.TAGGING=q.TAGGING||[];q.TAGGING[1]=!0};var t=function(a,b){for(var c in b)b.hasOwnProperty(c)&&(a[c]=b[c])},v=function(a){for(var b in a)if(a.hasOwnProperty(b))return!0;return!1};var x=/^(?:(?:https?|mailto|ftp):|[^:/?#]*(?:[/?#]|$))/i;var y=window,z=document,A=function(a,b){z.addEventListener?z.addEventListener(a,b,!1):z.attachEvent&&z.attachEvent("on"+a,b)};var B=/:[0-9]+$/,C=function(a,b,c){a=a.split("&");for(var d=0;d<a.length;d++){var e=a[d].split("=");if(decodeURIComponent(e[0]).replace(/\+/g," ")===b)return b=e.slice(1).join("="),c?b:decodeURIComponent(b).replace(/\+/g," ")}},F=function(a,b){b&&(b=String(b).toLowerCase());if("p

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\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
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"/>.. <feGaussianBlur 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="SourceGraphic"/>.. </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\9026IKNJ\de-ba3b57e12f3d6ff8ca5bd5b7e8900e04[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\de-ba3b57e12f3d6ff8ca5bd5b7e8900e04[1].svg	
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:	A3F4C0A591165A3046C9503346502CD77E4662B3C2B4DC95EC7BDB4BA5BFEC7FE56A7CF08BF0DF2BF217D752933361BEBFA82FD1B886608F72BFF1C0CDC1BF9B
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\9026IKNJ\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\9026IKNJ\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
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\9026IKNJ\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\fr-51dfbf8dee8670e6c6170f392d571b45[1].svg	
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\9026IKNJ\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\9026IKNJ\gilroy-bold-13ecf8e363c8931c26fd0293ace721ff[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 27760, version 1.0
Category:	downloaded
Size (bytes):	27760
Entropy (8bit):	7.979942095753643
Encrypted:	false
SSDEEP:	768:yRWaS/lSVhE9sLkhecgH6wOCrmPPgepI6O0klnN:mStSVh57cgAC1em6OJ
MD5:	E3B749EAA702B554A31B26C4840B8E6C
SHA1:	A51F9A834CD644101A4A495C2F9D784FF5135F01
SHA-256:	FF272849A30E0573C0FC6940042803155BF83F088AF56098667AC24896A7D157
SHA-512:	1E1F53DC206EC67388C1A09FFEE4C42FD7772978BC8DA88E8A8F68906F8464D721748EC4D543C838A98DCC424FD15DE43CEAEDD98A85B4D46475C51C0608D72
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://st0.bp.cdnsw.com/assets/gilroy/gilroy-bold-13ecf8e363c8931c26fd0293ace721ff.woff
Preview:	wOFF.....lp.....@.....FFTM..... .GDEF.....(...*....GPOS.....w..@.....GSUB...P.....P..tOS/2... ...V...`..~.cmap...x.....b.~.cvt .....2...2.s..fpgm...@.....eS./.gasp.....glyf.....G.....gT..head..c....6...6....hhea..d$.....$....hmtx..dD...(.....\>.loca..fl.....maxp..h,... ... ....name..hL.....D*.|)post..i.....".prep..k.....q!.....o.....V.....x.c`d``..b% fb`f`dx.....y.....`...P...x..[{.\.Y.....x.....$N.y8M6N..I.l].c L.....CZ%(..:..(..Z.....#.....+.%0L%..R.&\"#[.ZE.FhUU..B....9.....j.....>..y...O^.oJ....d._x^.~...?/wH.o%....A>...s...)....;d...p|...p|..q<..C8..W..;.....O}.W. ..{.....//.op..a.Nn.sG...Rv^....S[.....Y.....-.{...;..+..>.>[.C...\+.....u.$.o...;.o@w.....l.}.i....EG.P.HxA...e4l.....<{..E.....X`..H...uy../"...).G.%[..3.....J..r....x..f<?.7O.p}...e...D.....r.l..(+...e.|.....(.AoFe#..I6c$...F.-.@.f.A.J...._X.....TX.....S.|6.6..../.U...).y

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\gilroy-extrabold-75ff75de39edface89e23ac94b5cc0e4[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 27076, version 1.0
Category:	downloaded
Size (bytes):	27076
Entropy (8bit):	7.978448297201698
Encrypted:	false
SSDEEP:	384:Sv9VPL7hi3EPCqx93tZEKhm4kwFQoynpcR/YsnM/SrPOqQ8teZ/qPTc/:SlVPBiYjx9dZA4kwX/RQGMKrGy5Q

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\gilroy-extrabold-75ff75de39edface89e23ac94b5cc0e4[1].woff	
MD5:	0CBAE4A01F8839D1AFEE9D0E5817A1E9
SHA1:	24D7AE869530E9F8E23E131359403238BFE0E710
SHA-256:	591C2B43AC8E4C2B4CFF76DEC76F6A53B822C751FE1374C07E1365FD1A0AE0B7
SHA-512:	6439BC438CD3F94EB809D3E5402196D5671532B62E51D2C0BF66975DC069F76CD791ADB2910F98A2D2E13432D7EB9423FFB163071DC75095E2B3A86343246F8B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://st0.bp.cdnsw.com/assets/gilroy/gilroy-extrabold-75ff75de39edface89e23ac94b5cc0e4.woff
Preview:	wOFF.....i.....t.....FFTM.....GDEF.....(...*....GPOS.....AB.,:IGSUB.....P..tOS/2...|...O...`w.qcmap.....b.~.cvt ...`.....lfpgm.....eS./ .gasp...D.....glyf...L..F....L..R]head..al...6...6.bl.hhea..a.....$....hmtx..a.....6.loca..c.....maxp..ex.. ... .name..e.....5...post..g8.....''..prep..i.....}.....o.. .....x.c`d``..b% fb`f`dx.....y.....,`...P...x.[k.$.U>U.....}./.3....8.]....`..d.6`...6.lB.8.A.....A.D.c..%..A..-.....J<..(.F...P._h~E.|...V.....}.....HS./K..G/^...?..r..._..|R.x*.....#...}.....+8?..8_z."......+....{/|.s?.9.y..>+..1..y.s.e...r.....o.....:.x..m...{.....~...y.|.{.y.....Wptp."..<...../.W.....3...Y....d...{...%..G.pv.<o.3...{.);....9..@z..6.....p.Y...0....a...6.<..\u..M..p ..oMg%.6.[..Oo..w.|.<Mi1.c\.Q..&...iMY6.9.>.....L.....y.4.M..m..{'F...5M.3.n.-..\....]..c....L..Z.y.Kp.....^..#.gi.%c*..S...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\gilroy-medium-efd2197a6d1a674e9d4a876cbac69785[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 27360, version 1.0
Category:	downloaded
Size (bytes):	27360
Entropy (8bit):	7.979434737794823
Encrypted:	false
SSDEEP:	384:WNPnpFr3mEz4GvWHL2l1tnQgDACCLf+5kdc3PdeypzqedanbMw2xuNcuahXJogPJ:Wp3mjOyLQbnQSAiwgdppmedaG2yJLh
MD5:	FA2F4814E0C547840943F5199E7B2171
SHA1:	8188FC4B56A1150F648480D7BD586E75F3E4A053
SHA-256:	C68E2B6586B2B3AFE48964E079E38219FEDF39E9FA939E2BB8A4DC932E7B4455
SHA-512:	8B9B4B19718FE7DB824111F5E3DA41FC8453C820CBE46AD6BE0B99EB1D5EF05A73011ECA6A5E6090EB36A910C014CAEBF37E0E4F8E007948565FCC3218604B9 0
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://st0.bp.cdnsw.com/assets/gilroy/gilroy-medium-efd2197a6d1a674e9d4a876cbac69785.woff
Preview:	wOFF.....j.....FFTM.....jGDEF.....(...*....GPOS.....n..@.....GSUB...H.....P..tOS/2.....V...`..|tcmap...p.....b.~.cvt .....*...*.k..fpgm...0.....eS ./.gasp.....glyf.....F~...x..{.head..bl...6...6.5.^hhea..b... ...$....hmtx..b....*.....G.loca..d.....3iU.maxp..f.... ... ....name..f.....h0...post..hl.....''..prep..jL..... .o.....H.....x.c`d``..b% fb`f`dx.....y.....,`...P...x..[{.\.Y.....I...4.8..;&..u.... L#.0.#t.!.R.$...T.T...m.?.....dJd.).S. c.....j..j.(.Pe.....w.<vv.E.`>..<s...=.8''..+.UI..<v\..../../<..g..I.. .89..<....8....O>.]..:....<..#...q.Gp<..>?>.0.....~.>'..9..ge.O...78.Q..,w.#.._9)8..~z..f.'n...}..z.....w.....0.gd...._..d.|E.&w._.....y.,....KrN.9..:...>\...&.(oCxU6...\.e(|..X`..H..6..y. ...,r,''.U[..0.....Ca.gY.c4,''wE.B_6..a.yN...KH=(;@.....o.gm...c[_AY...(+...6.#o.t.....F..8 ...w.wul.w...zyB.O..BX..0.'.....*..Bx1,..N...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\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....SI.x.x.....N.....`..+/...5.P....+.....l.....Vx...Eo.Z...Pt..86..dK./.._....(..N.?Gd..4A.. ?O;....{...s..!..E3Z./3.^>.' ...=XD.I.,c

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\home-accompagnement-rapide[1].webp	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	RIFF (little-endian) data, Web/P image
Category:	downloaded
Size (bytes):	1340
Entropy (8bit):	7.810735336611906
Encrypted:	false
SSDEEP:	24:EmyLpI5PRi4EOWBEBKZ2zi759UKM6FLozMW6iJDRd1k5J+JGl531k98oyVFwh411:CE5i+k175SKZFMMWVRd/8w8oyLwhAeNK
MD5:	86F034596253743674055AD95C453EA3

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\home-accompagnement-rapide[1].webp	
SHA1:	E25D4969F8C15838E59590B7C3284BA074059B83
SHA-256:	04037037274B3812F83068932E93D32E47E4C258081FE84D0898E3CE84E14329
SHA-512:	68701D3822A89667C8328044E5CF3D6A00C7F4895B145E05AA8AF83B7BD7C9B4B9F64D435EF36266242B3B8EE5AB826065C90C3FB51FAB451DFA54BFB350C69(
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.sitew.org/images/blog/landing/2021/home-accompagnement-rapide.webp
Preview:	RIFF4...WEBPVP8X.....J..F..ALPH.....C..=.....m.m...T.m.....PG.....].@~`....w.....I..A.Y.'.....i..~.a.....Y.(...H..Q.!..9!..W.!.....Ev.^$..,.I...2..b.E..w.....4a/79...< I."..cN:..2...$t.C.R...`.g.|..(>..._...S3.....s./..V.'.../.....~.w.....'.H....,.h.N...5Q.O....6X.....Z..YIE.z.i....dS.....m@..%.....H.1.QR.K..!..= '.. W}.3!.C.. O".K)Q.E.G..9.....s.. o^.||..{.I.+...KU.Rv.....U..".C.=.{#m!..z../+@>q.'Nd.8^.....p\.VP8 L...p....*K.G.>.8.G%#.!/X.....b...Y....~.4.s. oKz...Vv.....E..A...7.....X,.6...K.....jr.....`CG...../.P....BD.q.B/.. ..J....b..@e.apN....m...K.....6l ....!.^.M..4\..!...-.R.0.TNP..rj.B2..~.,.....BDYa.5_.u7..hW.....wk.:\j.u....T.k....Q.I.....tB...K>.....L(....3A....[...+M.l....5.]mh..9o.U.c...@...&.. .....Y...Ux9....ITZ.....d."S.3F.C....~.D&...[....."s.../...Y}...%.....:J....=...X._.t...v..#..r._..S.~4U.*B.c.f.vq..\.U...K..D..u._..-}.8AJ.E..SBM.;.O-.. .YY.f(.F.3.b..-..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\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..I{.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\9026IKNJ\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.$.i..SL..ib.J.k..b.....v.."v.l.....;{..K_../O.v.",...T....B.P(T....P(...B..P(...B..P(....x@...e.wrg.?..D.C...@...C...lj./ I..qi..@2..6....8..G..2.:.....*.....@G... .B..7_....<tJp...6P....<.t.:.....a...N.....23....[fy{{.....@G.#..+.`..g-.['..~.$.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\9026IKNJ\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\home-reassurance-1-accompagnement[1].webp	
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....I..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.*.....I.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\9026IKNJ\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:	384:4ZRXYYWLpF3qmTXuE6GoRIAvLGKLyeD3n1n2B1cIx/64wpOQNKt0lNu:mB+Fl2ZLNFn2zxxy4wDK6lNu
MD5:	F307FC798D3CEFE4B87CD158897A8A5E
SHA1:	DA0B04C538E247232E3054371A9CB6BD94091922
SHA-256:	A7F9D53D28B6ED350925E9C01CEF4355F68C1EC7D8F220353AA8A2F46810AEE8
SHA-512:	1C79281D28EBFAC29305F2FEBA062402C85C22BC0C14FC23E3177E656D7C831604FBFA79DFF3FDF2F5213A887C5545F6505E0A0116D67BA8D7581FBD9B2AC11
Malicious:	false
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\9026IKNJ\home-reassurance-2-gratuit[1].webp	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	RIFF (little-endian) data, Web/P image
Category:	downloaded
Size (bytes):	1038
Entropy (8bit):	7.772513869225862
Encrypted:	false
SSDEEP:	24:8+eI41bGMaDFc0/kUiTsT4RgCrZaqFHAOigv72rp/z7e:8rBGvOUiTsy5rZaqBFMpr7e
MD5:	F5A86C61C4708916B6C87A1E1593A312
SHA1:	B007E2D129FE95F924CF1DE7FF216C4C89074973
SHA-256:	5B0A65309783D6195744A54D5D0B397A5C2DCC414A430B64F7066EDC34348D43
SHA-512:	FF29F3D0A2F6F30C9ADB9A56B885175B37A976D0A73CE29EFD7551A9E4E3116D310B36DD0E7B034B7A890DB1A0F0AC1AAEEFF89A3653B99ADA8F1CFB37BCB 821
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.sitew.org/images/blog/landing/2021/home-reassurance-2-gratuit.webp
Preview:	RIFF....WEBPVP8X.....T..O..ALPH\.....I.i[..m.m.m.m.m.....F.....E.m.x....4.....!p.WO....Fyi<.....~.....E...e.....PYV.%%....gb..AF6..g.7DQ56.....Q.....gc....p/..xE.. .'.Y3E...G~"J.....gP....l.g...Y..f....d.3....0.C{....D.P..K..(...3.L....JAp`..nJ.^..Bv}.....tH..Jb?q;...2b..K. > ..!.em{..1\O..v64..7.F^.....?.L..F....I.TI...T.c.>.....h.4...b..FA.x.. ?"...Z.A=..(.....>.D..R.i..H...h.R.2.yS/..&"..{.nAa..D..=.....1s.8P.pr=..A.Ie./)..(..ex$#.....H..e..9.\..b.b..L.[$....9.)._.....&....:HB+Xy.8w.....w1.P..Qdw.E....Y5[-...)&?..*b.]R...d;.. *....a.=zc.#....9..`/.no(.`....Rn\.eA....nY.U..[VP8 .....*U.P.>y2.G$.!.6xlp...d....[~~~..s.aN.o>.c.....w.N.J.....Nr.\..b!..... .....'.i...._Z.....q.X..x.fK-....D.<.v.HY.B..c.....Z5?...,.6.$0[.g.[.l|+f7/....._...b4.x.....q6\.....S....g..a.}e.....4+.v..qn.....JXT.bRY..."..eP.....G....1+V.....yRkR....J...C..{..}L.?.a.tY...]...(<...>.s.y.b..y..Z.....pM.t..c2.G.\...UV..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\home-typo-clients-indiv[1].webp	
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$@....h..._R.62....W...{.h.....VP8 "(.....*L...>.>.K%#'*#.)i@..gn.u..t.E7?....u.M.._._. ..vu..Y...?^.}.....w....%...C..ZW.....o.....XB>k..e..p.j.n.....w..2.>m.....a\|n.....O4_c{.....ha...=.....r.0..V.....Z.{w+C.n.ha...=.....r.0..V.....Z.{w+C.n.ha...=.....r.0..V.....Z.{w+C.n.ha...=.....r.0..V.....Z.{w+C.n.ha...=.....r.0..V.....Z.{w+:T...o.0..#.:.]...lw.w...@..R..N..D.h.. F.vDUU...e...\|%.._.=\P.x.3...9p-..Zn...`."....!Q.,.<.e.'...i.f.....Ke..`^...Xzg.4.4....!.. .~`..i..O.<..;...;^..i ..>...<.2.`#...Gc...H...n..z....B..Zw.....[..n-.o.].`.,..`q...g.&.0..d.!p.3?g....,.o.....cp..$`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...}.@..l;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\9026IKNJ\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:	F8CE7F5CFCDB425BE59943DA2C77ECFE6B566A43B1E86C373FF648B4D36B0E78C2758CB0A4C97A20F7CD87067E87B4AD967EB55863011B0B2943658E39096A8 1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.sitew.org/images/blog/landing/2021/clients/home-typo-clients-pro.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.....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.....BUDDD.*"".P...Q.....BUDDD.*"".P...Q.....BUDDD.*"".P.....BUDDD.*"".P.....BUDDD.*"".P.....BUDDD.*"".U.....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\9026IKNJ\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:	6C8831D367EA2C2CA0C7B9EF34DAB37C5AB2819553DBFA504F8CDDB658F25692097C42D09C5071DF57FB0803A757F5287AF8FD8765CCD35B2D1DF81ED117EE 5
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....'.@

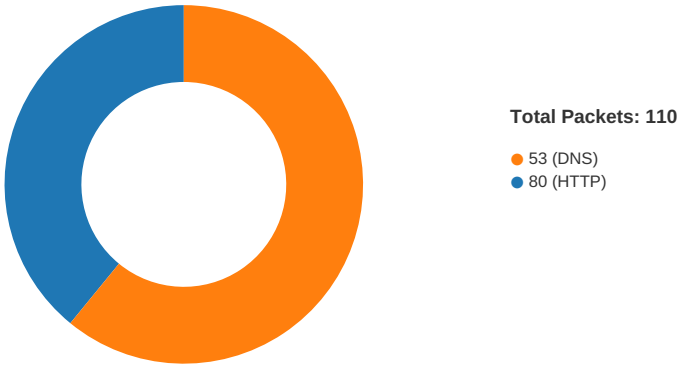
Static File Info

No static file info

Network Behavior

Network Port Distribution

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 18:45:12.490607977 CEST	49739	80	192.168.2.4	178.32.55.155
May 12, 2021 18:45:12.491836071 CEST	49740	80	192.168.2.4	178.32.55.155
May 12, 2021 18:45:12.540494919 CEST	80	49739	178.32.55.155	192.168.2.4
May 12, 2021 18:45:12.540694952 CEST	49739	80	192.168.2.4	178.32.55.155
May 12, 2021 18:45:12.541642904 CEST	80	49740	178.32.55.155	192.168.2.4
May 12, 2021 18:45:12.541661024 CEST	49739	80	192.168.2.4	178.32.55.155
May 12, 2021 18:45:12.541723013 CEST	49740	80	192.168.2.4	178.32.55.155
May 12, 2021 18:45:12.591514111 CEST	80	49739	178.32.55.155	192.168.2.4
May 12, 2021 18:45:12.607728958 CEST	80	49739	178.32.55.155	192.168.2.4
May 12, 2021 18:45:12.607851028 CEST	49739	80	192.168.2.4	178.32.55.155
May 12, 2021 18:45:12.677547932 CEST	49742	80	192.168.2.4	178.32.55.155
May 12, 2021 18:45:12.678664923 CEST	49743	80	192.168.2.4	178.32.55.155
May 12, 2021 18:45:12.728923082 CEST	80	49742	178.32.55.155	192.168.2.4
May 12, 2021 18:45:12.729044914 CEST	49742	80	192.168.2.4	178.32.55.155
May 12, 2021 18:45:12.730077982 CEST	80	49743	178.32.55.155	192.168.2.4
May 12, 2021 18:45:12.730166912 CEST	49743	80	192.168.2.4	178.32.55.155
May 12, 2021 18:45:12.730882883 CEST	49742	80	192.168.2.4	178.32.55.155
May 12, 2021 18:45:12.780735016 CEST	80	49742	178.32.55.155	192.168.2.4
May 12, 2021 18:45:12.952455044 CEST	80	49742	178.32.55.155	192.168.2.4
May 12, 2021 18:45:12.952511072 CEST	80	49742	178.32.55.155	192.168.2.4
May 12, 2021 18:45:12.952533960 CEST	80	49742	178.32.55.155	192.168.2.4
May 12, 2021 18:45:12.952555895 CEST	80	49742	178.32.55.155	192.168.2.4
May 12, 2021 18:45:12.952580929 CEST	80	49742	178.32.55.155	192.168.2.4
May 12, 2021 18:45:12.952603102 CEST	80	49742	178.32.55.155	192.168.2.4
May 12, 2021 18:45:12.952604055 CEST	49742	80	192.168.2.4	178.32.55.155
May 12, 2021 18:45:12.952622890 CEST	80	49742	178.32.55.155	192.168.2.4
May 12, 2021 18:45:12.952625990 CEST	49742	80	192.168.2.4	178.32.55.155
May 12, 2021 18:45:12.952645063 CEST	80	49742	178.32.55.155	192.168.2.4
May 12, 2021 18:45:12.952651024 CEST	49742	80	192.168.2.4	178.32.55.155
May 12, 2021 18:45:12.952667952 CEST	80	49742	178.32.55.155	192.168.2.4
May 12, 2021 18:45:12.952676058 CEST	49742	80	192.168.2.4	178.32.55.155
May 12, 2021 18:45:12.952688932 CEST	80	49742	178.32.55.155	192.168.2.4
May 12, 2021 18:45:12.952711105 CEST	49742	80	192.168.2.4	178.32.55.155
May 12, 2021 18:45:12.952739000 CEST	49742	80	192.168.2.4	178.32.55.155
May 12, 2021 18:45:13.002543926 CEST	80	49742	178.32.55.155	192.168.2.4
May 12, 2021 18:45:13.002578974 CEST	80	49742	178.32.55.155	192.168.2.4
May 12, 2021 18:45:13.002599955 CEST	80	49742	178.32.55.155	192.168.2.4
May 12, 2021 18:45:13.002624989 CEST	80	49742	178.32.55.155	192.168.2.4
May 12, 2021 18:45:13.002625942 CEST	49742	80	192.168.2.4	178.32.55.155
May 12, 2021 18:45:13.002648115 CEST	80	49742	178.32.55.155	192.168.2.4
May 12, 2021 18:45:13.002665043 CEST	49742	80	192.168.2.4	178.32.55.155
May 12, 2021 18:45:13.002670050 CEST	80	49742	178.32.55.155	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 18:45:13.002692938 CEST	80	49742	178.32.55.155	192.168.2.4
May 12, 2021 18:45:13.002703905 CEST	49742	80	192.168.2.4	178.32.55.155
May 12, 2021 18:45:13.002712965 CEST	80	49742	178.32.55.155	192.168.2.4
May 12, 2021 18:45:13.002722025 CEST	49742	80	192.168.2.4	178.32.55.155
May 12, 2021 18:45:13.002734900 CEST	80	49742	178.32.55.155	192.168.2.4
May 12, 2021 18:45:13.002756119 CEST	80	49742	178.32.55.155	192.168.2.4
May 12, 2021 18:45:13.002763987 CEST	49742	80	192.168.2.4	178.32.55.155
May 12, 2021 18:45:13.002778053 CEST	80	49742	178.32.55.155	192.168.2.4
May 12, 2021 18:45:13.002796888 CEST	49742	80	192.168.2.4	178.32.55.155
May 12, 2021 18:45:13.002803087 CEST	80	49742	178.32.55.155	192.168.2.4
May 12, 2021 18:45:13.002825022 CEST	80	49742	178.32.55.155	192.168.2.4
May 12, 2021 18:45:13.002826929 CEST	49742	80	192.168.2.4	178.32.55.155
May 12, 2021 18:45:13.002851963 CEST	49742	80	192.168.2.4	178.32.55.155
May 12, 2021 18:45:13.002871990 CEST	49742	80	192.168.2.4	178.32.55.155
May 12, 2021 18:45:13.002873898 CEST	80	49742	178.32.55.155	192.168.2.4
May 12, 2021 18:45:13.002897978 CEST	80	49742	178.32.55.155	192.168.2.4
May 12, 2021 18:45:13.002918959 CEST	80	49742	178.32.55.155	192.168.2.4
May 12, 2021 18:45:13.002928972 CEST	49742	80	192.168.2.4	178.32.55.155
May 12, 2021 18:45:13.002939939 CEST	80	49742	178.32.55.155	192.168.2.4
May 12, 2021 18:45:13.002942085 CEST	49742	80	192.168.2.4	178.32.55.155
May 12, 2021 18:45:13.002960920 CEST	80	49742	178.32.55.155	192.168.2.4
May 12, 2021 18:45:13.002996922 CEST	49742	80	192.168.2.4	178.32.55.155
May 12, 2021 18:45:13.003006935 CEST	80	49742	178.32.55.155	192.168.2.4
May 12, 2021 18:45:13.003038883 CEST	80	49742	178.32.55.155	192.168.2.4
May 12, 2021 18:45:13.003041983 CEST	49742	80	192.168.2.4	178.32.55.155
May 12, 2021 18:45:13.003058910 CEST	49742	80	192.168.2.4	178.32.55.155
May 12, 2021 18:45:13.003228903 CEST	49742	80	192.168.2.4	178.32.55.155
May 12, 2021 18:45:13.052651882 CEST	80	49742	178.32.55.155	192.168.2.4
May 12, 2021 18:45:13.052681923 CEST	80	49742	178.32.55.155	192.168.2.4
May 12, 2021 18:45:13.052767992 CEST	49742	80	192.168.2.4	178.32.55.155
May 12, 2021 18:45:13.052911043 CEST	80	49742	178.32.55.155	192.168.2.4
May 12, 2021 18:45:13.052931070 CEST	80	49742	178.32.55.155	192.168.2.4
May 12, 2021 18:45:13.052948952 CEST	80	49742	178.32.55.155	192.168.2.4
May 12, 2021 18:45:13.052966118 CEST	80	49742	178.32.55.155	192.168.2.4
May 12, 2021 18:45:13.052969933 CEST	49742	80	192.168.2.4	178.32.55.155
May 12, 2021 18:45:13.052990913 CEST	80	49742	178.32.55.155	192.168.2.4
May 12, 2021 18:45:13.053008080 CEST	80	49742	178.32.55.155	192.168.2.4
May 12, 2021 18:45:13.053015947 CEST	49742	80	192.168.2.4	178.32.55.155
May 12, 2021 18:45:13.053049088 CEST	49742	80	192.168.2.4	178.32.55.155
May 12, 2021 18:45:13.053106070 CEST	80	49742	178.32.55.155	192.168.2.4
May 12, 2021 18:45:13.053122997 CEST	80	49742	178.32.55.155	192.168.2.4
May 12, 2021 18:45:13.053152084 CEST	49742	80	192.168.2.4	178.32.55.155
May 12, 2021 18:45:13.053159952 CEST	80	49742	178.32.55.155	192.168.2.4
May 12, 2021 18:45:13.053178072 CEST	80	49742	178.32.55.155	192.168.2.4
May 12, 2021 18:45:13.053189993 CEST	49742	80	192.168.2.4	178.32.55.155
May 12, 2021 18:45:13.053209066 CEST	49742	80	192.168.2.4	178.32.55.155
May 12, 2021 18:45:13.053410053 CEST	80	49742	178.32.55.155	192.168.2.4
May 12, 2021 18:45:13.053431988 CEST	80	49742	178.32.55.155	192.168.2.4
May 12, 2021 18:45:13.053448915 CEST	80	49742	178.32.55.155	192.168.2.4
May 12, 2021 18:45:13.053467989 CEST	80	49742	178.32.55.155	192.168.2.4
May 12, 2021 18:45:13.053482056 CEST	49742	80	192.168.2.4	178.32.55.155
May 12, 2021 18:45:13.053488970 CEST	80	49742	178.32.55.155	192.168.2.4
May 12, 2021 18:45:13.053508997 CEST	80	49742	178.32.55.155	192.168.2.4
May 12, 2021 18:45:13.053524017 CEST	80	49742	178.32.55.155	192.168.2.4
May 12, 2021 18:45:13.053528070 CEST	49742	80	192.168.2.4	178.32.55.155
May 12, 2021 18:45:13.053540945 CEST	80	49742	178.32.55.155	192.168.2.4
May 12, 2021 18:45:13.053565979 CEST	49742	80	192.168.2.4	178.32.55.155
May 12, 2021 18:45:13.053587914 CEST	49742	80	192.168.2.4	178.32.55.155

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 18:45:04.143657923 CEST	53097	53	192.168.2.4	8.8.8.8
May 12, 2021 18:45:04.195123911 CEST	53	53097	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 18:45:04.594583035 CEST	49257	53	192.168.2.4	8.8.8.8
May 12, 2021 18:45:04.655791044 CEST	53	49257	8.8.8.8	192.168.2.4
May 12, 2021 18:45:04.931058884 CEST	62389	53	192.168.2.4	8.8.8.8
May 12, 2021 18:45:04.991311073 CEST	53	62389	8.8.8.8	192.168.2.4
May 12, 2021 18:45:05.111183882 CEST	49910	53	192.168.2.4	8.8.8.8
May 12, 2021 18:45:05.162682056 CEST	53	49910	8.8.8.8	192.168.2.4
May 12, 2021 18:45:05.968893051 CEST	55854	53	192.168.2.4	8.8.8.8
May 12, 2021 18:45:06.020761013 CEST	53	55854	8.8.8.8	192.168.2.4
May 12, 2021 18:45:07.072063923 CEST	64549	53	192.168.2.4	8.8.8.8
May 12, 2021 18:45:07.125754118 CEST	53	64549	8.8.8.8	192.168.2.4
May 12, 2021 18:45:08.318932056 CEST	63153	53	192.168.2.4	8.8.8.8
May 12, 2021 18:45:08.376013041 CEST	53	63153	8.8.8.8	192.168.2.4
May 12, 2021 18:45:09.592300892 CEST	52991	53	192.168.2.4	8.8.8.8
May 12, 2021 18:45:09.641061068 CEST	53	52991	8.8.8.8	192.168.2.4
May 12, 2021 18:45:10.674086094 CEST	53700	53	192.168.2.4	8.8.8.8
May 12, 2021 18:45:10.724780083 CEST	53	53700	8.8.8.8	192.168.2.4
May 12, 2021 18:45:11.154151917 CEST	51726	53	192.168.2.4	8.8.8.8
May 12, 2021 18:45:11.215010881 CEST	53	51726	8.8.8.8	192.168.2.4
May 12, 2021 18:45:12.412405968 CEST	56794	53	192.168.2.4	8.8.8.8
May 12, 2021 18:45:12.480396986 CEST	53	56794	8.8.8.8	192.168.2.4
May 12, 2021 18:45:12.508997917 CEST	56534	53	192.168.2.4	8.8.8.8
May 12, 2021 18:45:12.560677052 CEST	53	56534	8.8.8.8	192.168.2.4
May 12, 2021 18:45:12.615998030 CEST	56627	53	192.168.2.4	8.8.8.8
May 12, 2021 18:45:12.674937963 CEST	53	56627	8.8.8.8	192.168.2.4
May 12, 2021 18:45:13.036096096 CEST	56621	53	192.168.2.4	8.8.8.8
May 12, 2021 18:45:13.036355972 CEST	63116	53	192.168.2.4	8.8.8.8
May 12, 2021 18:45:13.036674976 CEST	64078	53	192.168.2.4	8.8.8.8
May 12, 2021 18:45:13.040904999 CEST	64801	53	192.168.2.4	8.8.8.8
May 12, 2021 18:45:13.042150021 CEST	61721	53	192.168.2.4	8.8.8.8
May 12, 2021 18:45:13.091401100 CEST	53	61721	8.8.8.8	192.168.2.4
May 12, 2021 18:45:13.093748093 CEST	53	56621	8.8.8.8	192.168.2.4
May 12, 2021 18:45:13.094223022 CEST	53	64078	8.8.8.8	192.168.2.4
May 12, 2021 18:45:13.096446991 CEST	53	63116	8.8.8.8	192.168.2.4
May 12, 2021 18:45:13.097925901 CEST	53	64801	8.8.8.8	192.168.2.4
May 12, 2021 18:45:13.345669031 CEST	51255	53	192.168.2.4	8.8.8.8
May 12, 2021 18:45:13.394583941 CEST	53	51255	8.8.8.8	192.168.2.4
May 12, 2021 18:45:13.471106052 CEST	61522	53	192.168.2.4	8.8.8.8
May 12, 2021 18:45:13.532747984 CEST	53	61522	8.8.8.8	192.168.2.4
May 12, 2021 18:45:13.852191925 CEST	52337	53	192.168.2.4	8.8.8.8
May 12, 2021 18:45:13.905502081 CEST	53	52337	8.8.8.8	192.168.2.4
May 12, 2021 18:45:13.940840960 CEST	55046	53	192.168.2.4	8.8.8.8
May 12, 2021 18:45:13.989732981 CEST	53	55046	8.8.8.8	192.168.2.4
May 12, 2021 18:45:14.012084007 CEST	49612	53	192.168.2.4	8.8.8.8
May 12, 2021 18:45:14.060746908 CEST	53	49612	8.8.8.8	192.168.2.4
May 12, 2021 18:45:14.582928896 CEST	49285	53	192.168.2.4	8.8.8.8
May 12, 2021 18:45:14.640321970 CEST	53	49285	8.8.8.8	192.168.2.4
May 12, 2021 18:45:14.746865988 CEST	50601	53	192.168.2.4	8.8.8.8
May 12, 2021 18:45:14.815583944 CEST	53	50601	8.8.8.8	192.168.2.4
May 12, 2021 18:45:15.649017096 CEST	56448	53	192.168.2.4	8.8.8.8
May 12, 2021 18:45:15.649482965 CEST	60875	53	192.168.2.4	8.8.8.8
May 12, 2021 18:45:15.705593109 CEST	53	56448	8.8.8.8	192.168.2.4
May 12, 2021 18:45:15.708092928 CEST	53	60875	8.8.8.8	192.168.2.4
May 12, 2021 18:45:16.656430960 CEST	59172	53	192.168.2.4	8.8.8.8
May 12, 2021 18:45:16.705426931 CEST	53	59172	8.8.8.8	192.168.2.4
May 12, 2021 18:45:18.338716984 CEST	62420	53	192.168.2.4	8.8.8.8
May 12, 2021 18:45:18.389636993 CEST	53	62420	8.8.8.8	192.168.2.4
May 12, 2021 18:45:19.752492905 CEST	60579	53	192.168.2.4	8.8.8.8
May 12, 2021 18:45:19.804153919 CEST	53	60579	8.8.8.8	192.168.2.4
May 12, 2021 18:45:21.930288076 CEST	50183	53	192.168.2.4	8.8.8.8
May 12, 2021 18:45:21.983935118 CEST	53	50183	8.8.8.8	192.168.2.4
May 12, 2021 18:45:32.754880905 CEST	61531	53	192.168.2.4	8.8.8.8
May 12, 2021 18:45:32.804837942 CEST	53	61531	8.8.8.8	192.168.2.4
May 12, 2021 18:45:33.521666050 CEST	49228	53	192.168.2.4	8.8.8.8
May 12, 2021 18:45:33.570552111 CEST	53	49228	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 18:45:33.708555937 CEST	59794	53	192.168.2.4	8.8.8.8
May 12, 2021 18:45:33.779378891 CEST	53	59794	8.8.8.8	192.168.2.4
May 12, 2021 18:45:34.339555979 CEST	55916	53	192.168.2.4	8.8.8.8
May 12, 2021 18:45:34.402390957 CEST	53	55916	8.8.8.8	192.168.2.4
May 12, 2021 18:45:34.590003967 CEST	52752	53	192.168.2.4	8.8.8.8
May 12, 2021 18:45:34.655394077 CEST	53	52752	8.8.8.8	192.168.2.4
May 12, 2021 18:45:35.906249046 CEST	60542	53	192.168.2.4	8.8.8.8
May 12, 2021 18:45:35.969677925 CEST	53	60542	8.8.8.8	192.168.2.4
May 12, 2021 18:45:37.458231926 CEST	60689	53	192.168.2.4	8.8.8.8
May 12, 2021 18:45:37.515710115 CEST	64206	53	192.168.2.4	8.8.8.8
May 12, 2021 18:45:37.517193079 CEST	53	60689	8.8.8.8	192.168.2.4
May 12, 2021 18:45:37.557738066 CEST	50904	53	192.168.2.4	8.8.8.8
May 12, 2021 18:45:37.577136040 CEST	53	64206	8.8.8.8	192.168.2.4
May 12, 2021 18:45:37.608329058 CEST	53	50904	8.8.8.8	192.168.2.4
May 12, 2021 18:45:39.065439939 CEST	57525	53	192.168.2.4	8.8.8.8
May 12, 2021 18:45:39.125936031 CEST	53	57525	8.8.8.8	192.168.2.4
May 12, 2021 18:45:39.391979933 CEST	53814	53	192.168.2.4	8.8.8.8
May 12, 2021 18:45:39.449477911 CEST	53	53814	8.8.8.8	192.168.2.4
May 12, 2021 18:45:40.145915031 CEST	53418	53	192.168.2.4	8.8.8.8
May 12, 2021 18:45:40.217472076 CEST	53	53418	8.8.8.8	192.168.2.4
May 12, 2021 18:45:41.022197962 CEST	62833	53	192.168.2.4	8.8.8.8
May 12, 2021 18:45:41.074266911 CEST	53	62833	8.8.8.8	192.168.2.4
May 12, 2021 18:45:41.195326090 CEST	59260	53	192.168.2.4	8.8.8.8
May 12, 2021 18:45:41.253808022 CEST	53	59260	8.8.8.8	192.168.2.4
May 12, 2021 18:45:41.316251993 CEST	49944	53	192.168.2.4	8.8.8.8
May 12, 2021 18:45:41.375904083 CEST	53	49944	8.8.8.8	192.168.2.4
May 12, 2021 18:45:41.989856958 CEST	63300	53	192.168.2.4	8.8.8.8
May 12, 2021 18:45:42.038486004 CEST	53	63300	8.8.8.8	192.168.2.4
May 12, 2021 18:45:42.212614059 CEST	59260	53	192.168.2.4	8.8.8.8
May 12, 2021 18:45:42.261260986 CEST	53	59260	8.8.8.8	192.168.2.4
May 12, 2021 18:45:42.534429073 CEST	61449	53	192.168.2.4	8.8.8.8
May 12, 2021 18:45:42.542581081 CEST	51275	53	192.168.2.4	8.8.8.8
May 12, 2021 18:45:42.542753935 CEST	63492	53	192.168.2.4	8.8.8.8
May 12, 2021 18:45:42.543193102 CEST	58945	53	192.168.2.4	8.8.8.8
May 12, 2021 18:45:42.591628075 CEST	53	61449	8.8.8.8	192.168.2.4
May 12, 2021 18:45:42.599904060 CEST	53	63492	8.8.8.8	192.168.2.4
May 12, 2021 18:45:42.605268955 CEST	53	51275	8.8.8.8	192.168.2.4
May 12, 2021 18:45:42.611484051 CEST	53	58945	8.8.8.8	192.168.2.4
May 12, 2021 18:45:43.027842999 CEST	63300	53	192.168.2.4	8.8.8.8
May 12, 2021 18:45:43.084625006 CEST	53	63300	8.8.8.8	192.168.2.4
May 12, 2021 18:45:43.154252052 CEST	60779	53	192.168.2.4	8.8.8.8
May 12, 2021 18:45:43.211280107 CEST	53	60779	8.8.8.8	192.168.2.4
May 12, 2021 18:45:43.264341116 CEST	59260	53	192.168.2.4	8.8.8.8
May 12, 2021 18:45:43.314466953 CEST	53	59260	8.8.8.8	192.168.2.4
May 12, 2021 18:45:43.399182081 CEST	64014	53	192.168.2.4	8.8.8.8
May 12, 2021 18:45:43.402462006 CEST	57091	53	192.168.2.4	8.8.8.8
May 12, 2021 18:45:43.459593058 CEST	53	57091	8.8.8.8	192.168.2.4
May 12, 2021 18:45:43.459621906 CEST	53	64014	8.8.8.8	192.168.2.4
May 12, 2021 18:45:45.008001089 CEST	63300	53	192.168.2.4	8.8.8.8
May 12, 2021 18:45:45.056904078 CEST	53	63300	8.8.8.8	192.168.2.4
May 12, 2021 18:45:45.306507111 CEST	59260	53	192.168.2.4	8.8.8.8
May 12, 2021 18:45:45.365292072 CEST	53	59260	8.8.8.8	192.168.2.4
May 12, 2021 18:45:45.989926100 CEST	55904	53	192.168.2.4	8.8.8.8
May 12, 2021 18:45:46.011686087 CEST	52109	53	192.168.2.4	8.8.8.8
May 12, 2021 18:45:46.038635015 CEST	53	55904	8.8.8.8	192.168.2.4
May 12, 2021 18:45:46.071759939 CEST	53	52109	8.8.8.8	192.168.2.4
May 12, 2021 18:45:46.916896105 CEST	54450	53	192.168.2.4	8.8.8.8
May 12, 2021 18:45:46.965689898 CEST	53	54450	8.8.8.8	192.168.2.4
May 12, 2021 18:45:46.980344057 CEST	49374	53	192.168.2.4	8.8.8.8
May 12, 2021 18:45:47.029202938 CEST	53	49374	8.8.8.8	192.168.2.4
May 12, 2021 18:45:47.031152964 CEST	63300	53	192.168.2.4	8.8.8.8
May 12, 2021 18:45:47.081449032 CEST	53	63300	8.8.8.8	192.168.2.4
May 12, 2021 18:45:47.577642918 CEST	50436	53	192.168.2.4	8.8.8.8
May 12, 2021 18:45:47.643162012 CEST	53	50436	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 18:45:49.310355902 CEST	59260	53	192.168.2.4	8.8.8.8
May 12, 2021 18:45:49.371447086 CEST	53	59260	8.8.8.8	192.168.2.4
May 12, 2021 18:45:51.028789043 CEST	63300	53	192.168.2.4	8.8.8.8
May 12, 2021 18:45:51.079569101 CEST	53	63300	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 12, 2021 18:45:12.412405968 CEST	192.168.2.4	8.8.8.8	0x28a5	Standard query (0)	keeplaffingwemake99383tyiwye.net	A (IP address)	IN (0x0001)
May 12, 2021 18:45:12.615998030 CEST	192.168.2.4	8.8.8.8	0x51a7	Standard query (0)	www.keeplaffingwemake99383tyiwye.net	A (IP address)	IN (0x0001)
May 12, 2021 18:45:13.036096096 CEST	192.168.2.4	8.8.8.8	0xc0bb	Standard query (0)	rb.bp.cdnsw.com	A (IP address)	IN (0x0001)
May 12, 2021 18:45:13.036355972 CEST	192.168.2.4	8.8.8.8	0x98b8	Standard query (0)	st0.bp.cdnsw.com	A (IP address)	IN (0x0001)
May 12, 2021 18:45:13.036674976 CEST	192.168.2.4	8.8.8.8	0x60c1	Standard query (0)	st0.cdnsw.com	A (IP address)	IN (0x0001)
May 12, 2021 18:45:13.040904999 CEST	192.168.2.4	8.8.8.8	0xccc4	Standard query (0)	mfs0.cdnsw.com	A (IP address)	IN (0x0001)
May 12, 2021 18:45:13.042150021 CEST	192.168.2.4	8.8.8.8	0x9262	Standard query (0)	www.sitew.com	A (IP address)	IN (0x0001)
May 12, 2021 18:45:13.345669031 CEST	192.168.2.4	8.8.8.8	0x7ba	Standard query (0)	mfs0.cdnsw.com	A (IP address)	IN (0x0001)
May 12, 2021 18:45:13.471106052 CEST	192.168.2.4	8.8.8.8	0xd9a0	Standard query (0)	ssl.sitew.org	A (IP address)	IN (0x0001)
May 12, 2021 18:45:14.012084007 CEST	192.168.2.4	8.8.8.8	0xa03d	Standard query (0)	st0.bp.cdnsw.com	A (IP address)	IN (0x0001)
May 12, 2021 18:45:14.746865988 CEST	192.168.2.4	8.8.8.8	0xd3fc	Standard query (0)	www.sitew.com	A (IP address)	IN (0x0001)
May 12, 2021 18:45:34.590003967 CEST	192.168.2.4	8.8.8.8	0x99fc	Standard query (0)	outlook0fficе365cgilogon.s3.us-east.cloud-object-storage.appdomain.cloud	A (IP address)	IN (0x0001)
May 12, 2021 18:45:35.906249046 CEST	192.168.2.4	8.8.8.8	0x3f85	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
May 12, 2021 18:45:37.458231926 CEST	192.168.2.4	8.8.8.8	0x39d0	Standard query (0)	aadcdn.msftauth.net	A (IP address)	IN (0x0001)
May 12, 2021 18:45:37.515710115 CEST	192.168.2.4	8.8.8.8	0xd097	Standard query (0)	logincdn.msauth.net	A (IP address)	IN (0x0001)
May 12, 2021 18:45:37.557738066 CEST	192.168.2.4	8.8.8.8	0x6e01	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)
May 12, 2021 18:45:39.391979933 CEST	192.168.2.4	8.8.8.8	0xe276	Standard query (0)	www.en.sitew.com	A (IP address)	IN (0x0001)
May 12, 2021 18:45:40.145915031 CEST	192.168.2.4	8.8.8.8	0x3ded	Standard query (0)	st0.cdnsw.com	A (IP address)	IN (0x0001)
May 12, 2021 18:45:42.534429073 CEST	192.168.2.4	8.8.8.8	0xac44	Standard query (0)	www.facebook.com	A (IP address)	IN (0x0001)
May 12, 2021 18:45:42.542581081 CEST	192.168.2.4	8.8.8.8	0x9f74	Standard query (0)	static.affilae.com	A (IP address)	IN (0x0001)
May 12, 2021 18:45:42.543193102 CEST	192.168.2.4	8.8.8.8	0x45d2	Standard query (0)	mautic.pikock.com	A (IP address)	IN (0x0001)
May 12, 2021 18:45:43.154252052 CEST	192.168.2.4	8.8.8.8	0xd6da	Standard query (0)	googleads.g.doubleclick.net	A (IP address)	IN (0x0001)
May 12, 2021 18:45:46.011686087 CEST	192.168.2.4	8.8.8.8	0x99fb	Standard query (0)	www.google.ch	A (IP address)	IN (0x0001)
May 12, 2021 18:45:46.916896105 CEST	192.168.2.4	8.8.8.8	0xe225	Standard query (0)	stats.g.doubleclick.net	A (IP address)	IN (0x0001)
May 12, 2021 18:45:46.980344057 CEST	192.168.2.4	8.8.8.8	0x6305	Standard query (0)	f.vimeocdn.com	A (IP address)	IN (0x0001)
May 12, 2021 18:45:47.577642918 CEST	192.168.2.4	8.8.8.8	0xab6c	Standard query (0)	www.google.de	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 18:45:12.480396986 CEST	8.8.8.8	192.168.2.4	0x28a5	No error (0)	keeplaffingwemake99383tyiwye.net		178.32.55.155	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 18:45:12.674937963 CEST	8.8.8.8	192.168.2.4	0x51a7	No error (0)	www.keepla ffingwemak e99383tyiw ye.net		178.32.55.155	A (IP address)	IN (0x0001)
May 12, 2021 18:45:13.091401100 CEST	8.8.8.8	192.168.2.4	0x9262	No error (0)	www.sitew.com		87.98.141.83	A (IP address)	IN (0x0001)
May 12, 2021 18:45:13.093748093 CEST	8.8.8.8	192.168.2.4	0xc0bb	No error (0)	rb.bp.cdns w.com		188.165.156.234	A (IP address)	IN (0x0001)
May 12, 2021 18:45:13.094223022 CEST	8.8.8.8	192.168.2.4	0x60c1	No error (0)	st0.cdnsw.com		46.105.199.115	A (IP address)	IN (0x0001)
May 12, 2021 18:45:13.096446991 CEST	8.8.8.8	192.168.2.4	0x98b8	No error (0)	st0.bp.cdn sw.com		188.165.33.133	A (IP address)	IN (0x0001)
May 12, 2021 18:45:13.097925901 CEST	8.8.8.8	192.168.2.4	0xccc4	No error (0)	mfs0.cdnsw.com		46.105.199.115	A (IP address)	IN (0x0001)
May 12, 2021 18:45:13.394583941 CEST	8.8.8.8	192.168.2.4	0x7ba	No error (0)	mfs0.cdnsw.com		46.105.199.115	A (IP address)	IN (0x0001)
May 12, 2021 18:45:13.532747984 CEST	8.8.8.8	192.168.2.4	0xd9a0	No error (0)	ssl.sitew.org		188.165.33.133	A (IP address)	IN (0x0001)
May 12, 2021 18:45:14.060746908 CEST	8.8.8.8	192.168.2.4	0xa03d	No error (0)	st0.bp.cdn sw.com		188.165.33.133	A (IP address)	IN (0x0001)
May 12, 2021 18:45:14.815583944 CEST	8.8.8.8	192.168.2.4	0xd3fc	No error (0)	www.sitew.com		87.98.141.83	A (IP address)	IN (0x0001)
May 12, 2021 18:45:34.655394077 CEST	8.8.8.8	192.168.2.4	0x99fc	No error (0)	outlook0ff ice365cgil ogon.s3.us-east.cloud-object-s torage.app domain.cloud	s3.us-east.cloud-object-storage.appdomain.cloud		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 18:45:34.655394077 CEST	8.8.8.8	192.168.2.4	0x99fc	No error (0)	s3.us-east .cloud-object-storag e.appdomai n.cloud		169.63.118.98	A (IP address)	IN (0x0001)
May 12, 2021 18:45:35.969677925 CEST	8.8.8.8	192.168.2.4	0x3f85	No error (0)	cdnjs.clou dflare.com		104.16.18.94	A (IP address)	IN (0x0001)
May 12, 2021 18:45:35.969677925 CEST	8.8.8.8	192.168.2.4	0x3f85	No error (0)	cdnjs.clou dflare.com		104.16.19.94	A (IP address)	IN (0x0001)
May 12, 2021 18:45:37.517193079 CEST	8.8.8.8	192.168.2.4	0x39d0	No error (0)	aadcdn.msf tauth.net	aadcdnoriginneu.azureedge.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 18:45:37.517193079 CEST	8.8.8.8	192.168.2.4	0x39d0	No error (0)	cs1100.wpc .omegacdn.net		152.199.23.37	A (IP address)	IN (0x0001)
May 12, 2021 18:45:37.577136040 CEST	8.8.8.8	192.168.2.4	0xd097	No error (0)	logincdn.m sauth.net	lgincdn.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 18:45:37.577136040 CEST	8.8.8.8	192.168.2.4	0xd097	No error (0)	cs1227.wpc .alphacdn.net		192.229.221.185	A (IP address)	IN (0x0001)
May 12, 2021 18:45:37.608329058 CEST	8.8.8.8	192.168.2.4	0x6e01	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 18:45:39.449477911 CEST	8.8.8.8	192.168.2.4	0xe276	No error (0)	www.en.sit ew.com		178.32.55.155	A (IP address)	IN (0x0001)
May 12, 2021 18:45:40.217472076 CEST	8.8.8.8	192.168.2.4	0x3ded	No error (0)	st0.cdnsw.com		46.105.199.115	A (IP address)	IN (0x0001)
May 12, 2021 18:45:42.591628075 CEST	8.8.8.8	192.168.2.4	0xac44	No error (0)	www.facebo ok.com	star-mini.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 18:45:42.591628075 CEST	8.8.8.8	192.168.2.4	0xac44	No error (0)	star-mini. c10r.faceb ook.com		185.60.216.35	A (IP address)	IN (0x0001)
May 12, 2021 18:45:42.605268955 CEST	8.8.8.8	192.168.2.4	0x9f74	No error (0)	static.affilae.com	d1r3aid9v9xqmp.cloudfront.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 18:45:42.605268955 CEST	8.8.8.8	192.168.2.4	0x9f74	No error (0)	d1r3aid9v9 xqmp.cloud front.net		13.225.74.42	A (IP address)	IN (0x0001)
May 12, 2021 18:45:42.605268955 CEST	8.8.8.8	192.168.2.4	0x9f74	No error (0)	d1r3aid9v9 xqmp.cloud front.net		13.225.74.80	A (IP address)	IN (0x0001)
May 12, 2021 18:45:42.605268955 CEST	8.8.8.8	192.168.2.4	0x9f74	No error (0)	d1r3aid9v9 xqmp.cloud front.net		13.225.74.72	A (IP address)	IN (0x0001)
May 12, 2021 18:45:42.605268955 CEST	8.8.8.8	192.168.2.4	0x9f74	No error (0)	d1r3aid9v9 xqmp.cloud front.net		13.225.74.46	A (IP address)	IN (0x0001)
May 12, 2021 18:45:42.611484051 CEST	8.8.8.8	192.168.2.4	0x45d2	No error (0)	mautic.pik ock.com		195.154.107.128	A (IP address)	IN (0x0001)
May 12, 2021 18:45:43.211280107 CEST	8.8.8.8	192.168.2.4	0xd6da	No error (0)	googleads. g.doubleclick.net		142.250.186.34	A (IP address)	IN (0x0001)
May 12, 2021 18:45:46.071759939 CEST	8.8.8.8	192.168.2.4	0x99fb	No error (0)	www.google.ch		142.250.186.67	A (IP address)	IN (0x0001)
May 12, 2021 18:45:46.965689898 CEST	8.8.8.8	192.168.2.4	0xe225	No error (0)	stats.g.do ubleclick.net	stats.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 18:45:46.965689898 CEST	8.8.8.8	192.168.2.4	0xe225	No error (0)	stats.l.do ubleclick.net		64.233.167.157	A (IP address)	IN (0x0001)
May 12, 2021 18:45:46.965689898 CEST	8.8.8.8	192.168.2.4	0xe225	No error (0)	stats.l.do ubleclick.net		64.233.167.154	A (IP address)	IN (0x0001)
May 12, 2021 18:45:46.965689898 CEST	8.8.8.8	192.168.2.4	0xe225	No error (0)	stats.l.do ubleclick.net		64.233.167.156	A (IP address)	IN (0x0001)
May 12, 2021 18:45:46.965689898 CEST	8.8.8.8	192.168.2.4	0xe225	No error (0)	stats.l.do ubleclick.net		64.233.167.155	A (IP address)	IN (0x0001)
May 12, 2021 18:45:47.029202938 CEST	8.8.8.8	192.168.2.4	0x6305	No error (0)	f.vimeocdn.com	vimeo-video.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 18:45:47.029202938 CEST	8.8.8.8	192.168.2.4	0x6305	No error (0)	vimeo-vide o.map.fastly.net		151.101.114.109	A (IP address)	IN (0x0001)
May 12, 2021 18:45:47.643162012 CEST	8.8.8.8	192.168.2.4	0xab6c	No error (0)	www.google.de		142.250.184.195	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	192.168.2.4	49739	178.32.55.155	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 18:45:12.541661024 CEST	1327	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 18:45:12.607728958 CEST	1328	IN	HTTP/1.1 301 Moved Permanently Server: SiteW Webserver 1.2.0 Date: Wed, 12 May 2021 16:45:12 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=elJ4QTd1VDhmU1NFdVRCZGYwcWE0T0dhRkdBK0JRT0txK1Urb2pXN2JucTFYdmdkMm xPMzNvalhlY0VrV3Z4TTN4dy81elo3YUMzQkZTNFRRQW9ock1nRGVBNDVLTisvd3NqZ0Q4ZGRsRWFWWV EyeEVwSndMZ290M0F0Q0FXRWszQlpTT3MvckZxK0JiTzAya0h2SENBPT0tLWVPK3VMa0lmcFdkTzY4aW J3ODRpeGc9PQ%3D%3D--7435498d70f0f96d1aa07959b66c615ef01dfe9d; path=/; HttpOnly X-Request-Id: fc295d32-3126-43de-8b9e-310dd3365454 X-Runtime: 0.015590 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	192.168.2.4	49742	178.32.55.155	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 18:45:12.730882883 CEST	1329	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 18:45:12.952455044 CEST	1338	IN	HTTP/1.1 200 OK Server: SiteW Webserver 1.2.0 Date: Wed, 12 May 2021 16:45:12 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=bEtrdHZRRU1zMXB2aW5hUjZtMFdkL3FDU0NxdnRpL2M5T0FFcDVSNmdNYmNLOXFmeW c3UEs2dHBER2tXWTNyYnN1bFVyRkM5SUVEV0FuVGVJYUVuWXBWcmttalVIektPQkFBL3gxTG9jUEk3UHk4cjdFL2xY ektnOWhwWkM2ZEJOTytMaXZzRFUyRlJseWdDenk0dy9VcWJiVVNQMWs4WDZFN0RoNmszZjd3MENYZzlR OHF3TVJhV21JTy9sSWpNd3ExYzczbE5lb1hROS9WejlQaXNKUW1CVVhxNFlqTW1XV09LcGlTeU5WNkh4 dXNWbzJOOC9Ea3JGVVQ1M29zZGpHZ2RnbGZYSENRVlJRaWNpLzkwY25GUFB1VUptUzhyZEVKNjc2eTE4 eWM9LS1KeXVKTmhwOXV4UTBtVG93Vm02LzNRPT0%3D--2a136187d49a2b59a086f9a8b85a9474a1146ceb; path=/; HttpOnly X-Request-Id: 9d423bbe-a570-433a-97a9-738aed446503 X-Runtime: 0.026162 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[@

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 18:45:14.502370119 CEST	2190	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=bEtrdHZRRU1zMXB2aW5hUjZtMFdkL3FDU0NxdnRpL2M5T0FFcDVSNmdNYmNLOXFmeWc3UE s2dHBER2tXWTNyYnN1bFVyRkM5SUVEV0FuVGVJYUVuWXBWcmttalVlektPQkFBL3gxTG9jUEk3UHk4cjdFL2xYektn OWhwWkM2ZEJOTytMaXZzRFUyRlJseWdDenk0dy9VcWJiVVNQMWs4WDZFN0RoNmszZjd3MENYZzlROHF3 TVJhV21JTy9sSWpNd3ExYzczbE5lb1hROS9WejlQaXNKUW1CVVhxNFlqTW1XV09LcGlTeU5WNkh4dXNW bzJOOC9Ea3JGVVQ1M29zZGpHZ2RnbGZYSENRVlJRaWNpLzkwY25GUFB1VUptUzhyZEVKNjc2eTE4eWM9 LS1KeXVKTmhwOXV4UTBtVG93Vm02LzNRPT0%3D--2a136187d49a2b59a086f9a8b85a9474a1146ceb
May 12, 2021 18:45:14.553241968 CEST	2242	IN	HTTP/1.1 200 OK Server: SiteW Webserver 1.2.0 Date: Wed, 12 May 2021 16:45:14 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 18:45:14.798780918 CEST	2260	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=bEtrdHZRRU1zMXB2aW5hUjZtMFdkL3FDU0NxdnRpL2M5T0FFcDVSNmdNYmNLOXFmeWc3UE s2dHBER2tXWTNyYnN1bFVyRkM5SUVEV0FuVGVJYUVuWXBWcmttalVlektPQkFBL3gxTG9jUEk3UHk4cjdFL2xYektn OWhwWkM2ZEJOTytMaXZzRFUyRlJseWdDenk0dy9VcWJiVVNQMWs4WDZFN0RoNmszZjd3MENYZzlROHF3 TVJhV21JTy9sSWpNd3ExYzczbE5lb1hROS9WejlQaXNKUW1CVVhxNFlqTW1XV09LcGlTeU5WNkh4dXNW bzJOOC9Ea3JGVVQ1M29zZGpHZ2RnbGZYSENRVlJRaWNpLzkwY25GUFB1VUptUzhyZEVKNjc2eTE4eWM9 LS1KeXVKTmhwOXV4UTBtVG93Vm02LzNRPT0%3D--2a136187d49a2b59a086f9a8b85a9474a1146ceb
May 12, 2021 18:45:14.848936081 CEST	2274	IN	HTTP/1.1 200 OK Server: SiteW Webserver 1.2.0 Date: Wed, 12 May 2021 16:45:14 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 18:45:15.605283976 CEST	2280	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=bEtrdHZRRU1zMXB2aW5hUjZtMFdkL3FDU0NxdnRpL2M5T0FFcDVSNmdNYmNLOXFmeWc3UE s2dHBER2tXWTNyYnN1bFVyRkM5SUVEV0FuVGVJYUVuWXBWcmttalVlektPQkFBL3gxTG9jUEk3UHk4cjdFL2xYektn OWhwWkM2ZEJOTytMaXZzRFUyRlJseWdDenk0dy9VcWJiVVNQMWs4WDZFN0RoNmszZjd3MENYZzlROHF3 TVJhV21JTy9sSWpNd3ExYzczbE5lb1hROS9WejlQaXNKUW1CVVhxNFlqTW1XV09LcGlTeU5WNkh4dXNW bzJOOC9Ea3JGVVQ1M29zZGpHZ2RnbGZYSENRVlJRaWNpLzkwY25GUFB1VUptUzhyZEVKNjc2eTE4eWM9 LS1KeXVKTmhwOXV4UTBtVG93Vm02LzNRPT0%3D--2a136187d49a2b59a086f9a8b85a9474a1146ceb

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 18:45:15.677942991 CEST	2281	IN	HTTP/1.1 200 OK Server: SiteW Webserver 1.2.0 Date: Wed, 12 May 2021 16:45:15 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=TlpWWDhhaUZrSmFKNVI4eUlFbjUyVm81V09YWXBWSDNYcW95R204SjA0Vk5Rdm1xNU EyeldPZkZ1RnNzazZwRW00cFhrSDVLRjJDSnZNc1hzckJlZi9KVFdrbjM2SXpxMkErVFFUODVzL1JMNjJFMTY1Mlls dmZFVlNnUUVnV2lmV25WeTVUZ1ZhdW9lYjhhdUpxdnlGZnJzUUJDclE3STRQU1E1V29ZNVdZeFNBSDhH cm1zT3QwT3B4MXBRWGlmUHhkUzU1bitXcmdnWi92QTJFWHBZSlNmeTdrTlY4ZllXMmdUdVk3Q2NYY3ps cERKVFB3V0dldDZjakl3aXhmQys1OWxLSEdWWERwTG5nNW9vQVIrSmFOSUJBVG1HQnJSWVFyeUdCZ1Z3 VXc9LS1pQlBGa2xvaDFIdnNwOG9CdTM0L0pnPT0%3D--61a1ca3f7cb4b088b8b2073bf2b7f44434028bbb; path=/; HttpOnly ETag: "587e3d21-1cee" Expires: Thu, 20 May 2021 16:45:15 GMT Cache-Control: public Vary: Accept-Encoding Accept-Ranges: bytes

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49744	46.105.199.115	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 18:45:13.668020964 CEST	1664	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
May 12, 2021 18:45:13.721849918 CEST	1666	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:C250_2E69C773:0050_609C0619_59E62:150C8 X-IPLB-Instance: 17352 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 c2 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'5ihFZI^/BGofxg

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49743	178.32.55.155	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 18:45:14.502985954 CEST	2191	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=bEtrdHZRRU1zMXB2aW5hUjZtMFdkL3FDU0NxdnRpL2M5T0FFcDVSNmdNYmNLOXFmeWc3UE s2dHBER2tXWTNyYnN1bFVyRkM5SUVEV0FuVGVJYUVuWXBWcmttalVlektPQkFBL3gxTG9jUEk3UHk4cjdFL2xYektn OWhwWkM2ZEJOTytMaXZzRFUyRlJseWdDenk0dy9VcWJiVVNQMWs4WDZFN0RoNmszZjd3MENYZzlROHF3 TVJhV21JTy9sSWpNd3ExYzczbE5lb1hROS9WejlQaXNKUW1CVVhxNFlqTW1XV09LcGlTeU5WNkh4dXNW bzJOOC9Ea3JGVVQ1M29zZGpHZ2RnbGZYSENRVlJRaWNpLzkwY25GUFB1VUptUzhyZEVKNjc2eTE4eWM9 LS1KeXVKTmhwOXV4UTBtVG93Vm02LzNRPT0%3D--2a136187d49a2b59a086f9a8b85a9474a1146ceb
May 12, 2021 18:45:14.553663015 CEST	2243	IN	HTTP/1.1 200 OK Server: SiteW Webserver 1.2.0 Date: Wed, 12 May 2021 16:45:14 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 18:45:14.805286884 CEST	2261	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+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=bEtrdHZRRU1zMXB2aW5hUjZtMFdkL3FDU0NxdnRpL2M5T0FFcDVSNmdNYmNLOXFmeWc3UE s2dHBER2tXWTNyYnN1bFVyRkM5SUVEV0FuVGVJYUVuWXBWcmttalVlektPQkFBL3gxTG9jUEk3UHk4cjdFL2xYektn OWhwWkM2ZEJOTytMaXZzRFUyRlJseWdDenk0dy9VcWJiVVNQMWs4WDZFN0RoNmszZjd3MENYZzlROHF3 TVJhV21JTy9sSWpNd3ExYzczbE5lb1hROS9WejlQaXNKUW1CVVhxNFlqTW1XV09LcGlTeU5WNkh4dXNW bzJOOC9Ea3JGVVQ1M29zZGpHZ2RnbGZYSENRVlJRaWNpLzkwY25GUFB1VUptUzhyZEVKNjc2eTE4eWM9 LS1KeXVKTmhwOXV4UTBtVG93Vm02LzNRPT0%3D--2a136187d49a2b59a086f9a8b85a9474a1146ceb
May 12, 2021 18:45:14.855403900 CEST	2275	IN	HTTP/1.1 200 OK Server: SiteW Webserver 1.2.0 Date: Wed, 12 May 2021 16:45:14 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
4	192.168.2.4	49759	178.32.55.155	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 18:45:14.557034969 CEST	2245	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=bEtrdHZRRU1zMXB2aW5hUjZtMFdkL3FDU0NxdnRpL2M5T0FFcDVSNmdNYmNLOXFmeWc3UE s2dHBER2tXWTNyYnN1bFVyRkM5SUVEV0FuVGVJYUVuWXBWcmttalVlektPQkFBL3gxTG9jUEk3UHk4cjdFL2xYektn OWhwWkM2ZEJOTytMaXZzRFUyRlJseWdDenk0dy9VcWJiVVNQMWs4WDZFN0RoNmszZjd3MENYZzlROHF3 TVJhV21JTy9sSWpNd3ExYzczbE5lb1hROS9WejlQaXNKUW1CVVhxNFlqTW1XV09LcGlTeU5WNkh4dXNW bzJOOC9Ea3JGVVQ1M29zZGpHZ2RnbGZYSENRVlJRaWNpLzkwY25GUFB1VUptUzhyZEVKNjc2eTE4eWM9 LS1KeXVKTmhwOXV4UTBtVG93Vm02LzNRPT0%3D--2a136187d49a2b59a086f9a8b85a9474a1146ceb

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 18:45:14.606975079 CEST	2249	IN	HTTP/1.1 200 OK Server: SiteW Webserver 1.2.0 Date: Wed, 12 May 2021 16:45:14 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
May 12, 2021 18:45:14.810633898 CEST	2264	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+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=bEtrdHZRRU1zMXB2aW5hUjZtMFdkL3FDU0NxdnRpL2M5T0FFcDVSNmdNYmNLOXFmeWc3UE s2dHBER2tXWTNyYnN1bFVyRkM5SUVEV0FuVGVJYUVuWXBWcmttalVlektPQkFBL3gxTG9jUEk3UHk4cjdFL2xYektn OWhwWkM2ZEJOTytMaXZzRFUyRlJseWdDenk0dy9VcWJiVVNQMWs4WDZFN0RoNmszZjd3MENYZzlROHF3 TVJhV21JTy9sSWpNd3ExYzczbE5lb1hROS9WejlQaXNKUW1CVVhxNFlqTW1XV09LcGlTeU5WNkh4dXNW bzJOOC9Ea3JGVVQ1M29zZGpHZ2RnbGZYSENRVlJRaWNpLzkwY25GUFB1VUptUzhyZEVKNjc2eTE4eWM9 LS1KeXVKTmhwOXV4UTBtVG93Vm02LzNRPT0%3D--2a136187d49a2b59a086f9a8b85a9474a1146ceb
May 12, 2021 18:45:14.860771894 CEST	2277	IN	HTTP/1.1 200 OK Server: SiteW Webserver 1.2.0 Date: Wed, 12 May 2021 16:45:14 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
5	192.168.2.4	49760	178.32.55.155	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 18:45:14.557491064 CEST	2246	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+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=bEtrdHZRRU1zMXB2aW5hUjZtMFdkL3FDU0NxdnRpL2M5T0FFcDVSNmdNYmNLOXFmeWc3UE s2dHBER2tXWTNyYnN1bFVyRkM5SUVEV0FuVGVJYUVuWXBWcmttalVlektPQkFBL3gxTG9jUEk3UHk4cjdFL2xYektn OWhwWkM2ZEJOTytMaXZzRFUyRlJseWdDenk0dy9VcWJiVVNQMWs4WDZFN0RoNmszZjd3MENYZzlROHF3 TVJhV21JTy9sSWpNd3ExYzczbE5lb1hROS9WejlQaXNKUW1CVVhxNFlqTW1XV09LcGlTeU5WNkh4dXNW bzJOOC9Ea3JGVVQ1M29zZGpHZ2RnbGZYSENRVlJRaWNpLzkwY25GUFB1VUptUzhyZEVKNjc2eTE4eWM9 LS1KeXVKTmhwOXV4UTBtVG93Vm02LzNRPT0%3D--2a136187d49a2b59a086f9a8b85a9474a1146ceb
May 12, 2021 18:45:14.607285976 CEST	2249	IN	HTTP/1.1 200 OK Server: SiteW Webserver 1.2.0 Date: Wed, 12 May 2021 16:45:14 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

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 18:45:14.812062979 CEST	2265	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=bEtrdHZRRU1zMXB2aW5hUjZtMFdkL3FDU0NxdnRpL2M5T0FFcDVSNmdNYmNLOXFmeWc3UE s2dHBER2tXWTNyYnN1bFVyRkM5SUVEV0FuVGVJYUVuWXBWcmttalVlektPQkFBL3gxTG9jUEk3UHk4cjdFL2xYektn OWhwWkM2ZEJOTytMaXZzRFUyRlJseWdDenk0dy9VcWJiVVNQMWs4WDZFN0RoNmszZjd3MENYZzlROHF3 TVJhV21JTy9sSWpNd3ExYzczbE5lb1hROS9WejlQaXNKUW1CVVhxNFlqTW1XV09LcGlTeU5WNkh4dXNW bzJOOC9Ea3JGVVQ1M29zZGpHZ2RnbGZYSENRVlJRaWNpLzkwY25GUFB1VUptUzhyZEVKNjc2eTE4eWM9 LS1KeXVKTmhwOXV4UTBtVG93Vm02LzNRPT0%3D--2a136187d49a2b59a086f9a8b85a9474a1146ceb
May 12, 2021 18:45:14.862029076 CEST	2277	IN	HTTP/1.1 200 OK Server: SiteW Webserver 1.2.0 Date: Wed, 12 May 2021 16:45:14 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
6	192.168.2.4	49757	178.32.55.155	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 18:45:14.557730913 CEST	2247	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+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=bEtrdHZRRU1zMXB2aW5hUjZtMFdkL3FDU0NxdnRpL2M5T0FFcDVSNmdNYmNLOXFmeWc3UE s2dHBER2tXWTNyYnN1bFVyRkM5SUVEV0FuVGVJYUVuWXBWcmttalVlektPQkFBL3gxTG9jUEk3UHk4cjdFL2xYektn OWhwWkM2ZEJOTytMaXZzRFUyRlJseWdDenk0dy9VcWJiVVNQMWs4WDZFN0RoNmszZjd3MENYZzlROHF3 TVJhV21JTy9sSWpNd3ExYzczbE5lb1hROS9WejlQaXNKUW1CVVhxNFlqTW1XV09LcGlTeU5WNkh4dXNW bzJOOC9Ea3JGVVQ1M29zZGpHZ2RnbGZYSENRVlJRaWNpLzkwY25GUFB1VUptUzhyZEVKNjc2eTE4eWM9 LS1KeXVKTmhwOXV4UTBtVG93Vm02LzNRPT0%3D--2a136187d49a2b59a086f9a8b85a9474a1146ceb
May 12, 2021 18:45:14.607513905 CEST	2250	IN	HTTP/1.1 200 OK Server: SiteW Webserver 1.2.0 Date: Wed, 12 May 2021 16:45:14 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
May 12, 2021 18:45:14.807504892 CEST	2262	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=bEtrdHZRRU1zMXB2aW5hUjZtMFdkL3FDU0NxdnRpL2M5T0FFcDVSNmdNYmNLOXFmeWc3UE s2dHBER2tXWTNyYnN1bFVyRkM5SUVEV0FuVGVJYUVuWXBWcmttalVlektPQkFBL3gxTG9jUEk3UHk4cjdFL2xYektn OWhwWkM2ZEJOTytMaXZzRFUyRlJseWdDenk0dy9VcWJiVVNQMWs4WDZFN0RoNmszZjd3MENYZzlROHF3 TVJhV21JTy9sSWpNd3ExYzczbE5lb1hROS9WejlQaXNKUW1CVVhxNFlqTW1XV09LcGlTeU5WNkh4dXNW bzJOOC9Ea3JGVVQ1M29zZGpHZ2RnbGZYSENRVlJRaWNpLzkwY25GUFB1VUptUzhyZEVKNjc2eTE4eWM9 LS1KeXVKTmhwOXV4UTBtVG93Vm02LzNRPT0%3D--2a136187d49a2b59a086f9a8b85a9474a1146ceb

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 18:45:14.857486010 CEST	2276	IN	HTTP/1.1 200 OK Server: SiteW Webserver 1.2.0 Date: Wed, 12 May 2021 16:45:14 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
7	192.168.2.4	49758	178.32.55.155	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 18:45:14.558320045 CEST	2248	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=bEtrdHZRRU1zMXB2aW5hUjZtMFdkL3FDU0NxdnRpL2M5T0FFcDVSNmdNYmNLOXFmeWc3UEs2dHBER2tXWTNyYnN1bFVyRkM5SUVEV0FuVGVJYUVuWXBWcmttalVlektPQkFBL3gxTG9jUEk3UHk4cjdFL2xYektnOWhwWkM2ZEJOTytMaXZzRFUyRlJseWdDenk0dy9VcWJiVVNQMWs4WDZFN0RoNmszZjd3MENYZzlROHF3TVJhV21JTy9sSWpNd3ExYzczbE5lb1hROS9WejlQaXNKUW1CVVhxNFlqTW1XV09LcGlTeU5WNkh4dXNWbzJOOC9Ea3JGVVQ1M29zZGpHZ2RnbGZYSENRVlJRaWNpLzkwY25GUFB1VUptUzhyZEVKNjc2eTE4eWM9LS1KeXVKTmhwOXV4UTBtVG93Vm02LzNRPT0%3D--2a136187d49a2b59a086f9a8b85a9474a1146ceb
May 12, 2021 18:45:14.608166933 CEST	2251	IN	HTTP/1.1 200 OK Server: SiteW Webserver 1.2.0 Date: Wed, 12 May 2021 16:45:14 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
May 12, 2021 18:45:14.808880091 CEST	2263	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=bEtrdHZRRU1zMXB2aW5hUjZtMFdkL3FDU0NxdnRpL2M5T0FFcDVSNmdNYmNLOXFmeWc3UEs2dHBER2tXWTNyYnN1bFVyRkM5SUVEV0FuVGVJYUVuWXBWcmttalVlektPQkFBL3gxTG9jUEk3UHk4cjdFL2xYektnOWhwWkM2ZEJOTytMaXZzRFUyRlJseWdDenk0dy9VcWJiVVNQMWs4WDZFN0RoNmszZjd3MENYZzlROHF3TVJhV21JTy9sSWpNd3ExYzczbE5lb1hROS9WejlQaXNKUW1CVVhxNFlqTW1XV09LcGlTeU5WNkh4dXNWbzJOOC9Ea3JGVVQ1M29zZGpHZ2RnbGZYSENRVlJRaWNpLzkwY25GUFB1VUptUzhyZEVKNjc2eTE4eWM9LS1KeXVKTmhwOXV4UTBtVG93Vm02LzNRPT0%3D--2a136187d49a2b59a086f9a8b85a9474a1146ceb
May 12, 2021 18:45:14.858891964 CEST	2276	IN	HTTP/1.1 200 OK Server: SiteW Webserver 1.2.0 Date: Wed, 12 May 2021 16:45:14 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
8	192.168.2.4	49764	87.98.141.83	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 18:45:15.088188887 CEST	2279	OUT	GET /json/site_owner/?callback=jQuery11240627140223264869_1620837913434&site=www.keeplaffingwemake99383tyiwye.net&_=1620837913435 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 18:45:15.151248932 CEST	2280	IN	HTTP/1.1 200 OK Server: SiteW Webserver 1.2.0 Date: Wed, 12 May 2021 16:45:15 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=UWxSQmxKWG5oVUgyRmlqdThRdGhETWFEOVZac29tWU5xUXVRL2t2WHdDZlg0REs0UE5sRjgrakVvZm10SG5DZWRxY090cXRUbkVuY25XRzVhTytGTTdHS1FKYjVncFk2OWJ1ZE1pZ01kZDIwV2E1Z3FoSmF0SFZ3K2R4alhrL3BkYWwvRnRxTCtzelp5MWh4dEhFUDlRPT0tLUJKcmVyOU9lUitWNWZBMTZPWjE2bEE9PQ%3D%3D--4ba458090da4b0dfde38e4f014ef07bd63746cdf; path=/; HttpOnly X-Request-Id: 22f7ba6a-81b7-4cfa-94df-a177fb5ed0b3 X-Runtime: 0.011095 Content-Encoding: gzip Data Raw: 34 66 0d 0a 1f 8b 08 00 00 00 00 00 00 03 cb 0a 2c 4d 2d aa 34 34 34 32 31 30 33 32 37 34 31 30 32 32 36 32 33 b1 30 b3 8c 37 34 33 32 b0 30 36 b7 34 34 36 31 36 d1 a8 56 ca c9 4f 4f 4f 4d 51 b2 4a 4b cc 29 4e ad d5 b4 06 00 3a 31 4a 6b 3b 00 00 00 0d 0a 30 0d 0a 0d 0a Data Ascii: 4f,M-444210327410226230743206446l6VOOOMQJK)N:1Jk;0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	46.105.199.115	80	192.168.2.4	49745	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 18:45:23.585593939 CEST	2930	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
May 12, 2021 18:45:13.792887926 CEST	188.165.33.133	443	192.168.2.4	49746	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	Fri Jul 30 10:01:39 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 18:45:13.795612097 CEST	188.165.33.133	443	192.168.2.4	49747	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 18:45:14.186767101 CEST	188.165.33.133	443	192.168.2.4	49756	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 18:45:14.189214945 CEST	188.165.33.133	443	192.168.2.4	49755	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 18:45:14.191768885 CEST	188.165.33.133	443	192.168.2.4	49753	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 18:45:14.194281101 CEST	188.165.33.133	443	192.168.2.4	49754	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 18:45:14.355189085 CEST	188.165.33.133	443	192.168.2.4	49752	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 18:45:36.069046021 CEST	104.16.18.94	443	192.168.2.4	49779	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 18:45:36.166779041 CEST	104.16.18.94	443	192.168.2.4	49780	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 18:45:37.684139013 CEST	152.199.23.37	443	192.168.2.4	49783	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 18:45:37.690510988 CEST	152.199.23.37	443	192.168.2.4	49781	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 18:45:37.690649986 CEST	152.199.23.37	443	192.168.2.4	49786	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 18:45:37.691324949 CEST	152.199.23.37	443	192.168.2.4	49784	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 18:45:37.691643000 CEST	152.199.23.37	443	192.168.2.4	49782	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 18:45:37.833502054 CEST	152.199.23.37	443	192.168.2.4	49785	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 18:45:37.877073050 CEST	192.229.221.185	443	192.168.2.4	49790	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		

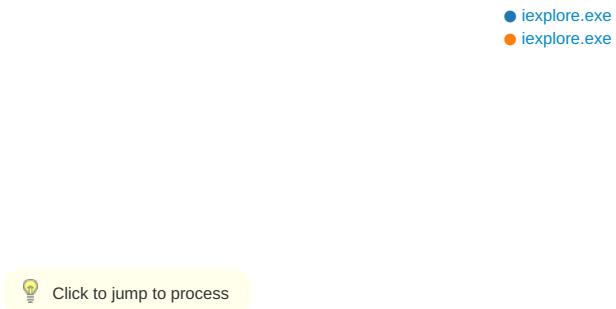
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 12, 2021 18:45:37.877329111 CEST	192.229.221.185	443	192.168.2.4	49789	CN=identitycdn.msauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US CN=DigiCert 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 18:45:39.559458971 CEST	178.32.55.155	443	192.168.2.4	49793	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 18:45:39.560950041 CEST	178.32.55.155	443	192.168.2.4	49792	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 18:45:40.340286970 CEST	46.105.199.115	443	192.168.2.4	49801	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 18:45:40.340419054 CEST	46.105.199.115	443	192.168.2.4	49802	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 18:45:40.340512991 CEST	46.105.199.115	443	192.168.2.4	49800	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 18:45:40.341052055 CEST	46.105.199.115	443	192.168.2.4	49799	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



System Behavior

Analysis Process: iexplore.exe PID: 6396 Parent PID: 800

General

Start time:	18:45:10
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:	0x7ff736a40000
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: 6484 Parent PID: 6396

General

Start time:	18:45:11
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:6396 CREDAT:17410 /prefetch:2
Imagebase:	0x1020000
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