ID: 433276
Cookbook: browseurl.jbs
Time: 15:12:29
Date: 11/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents 2
Analysis Report https://stgdjas.simplesite.com/ 3
Overview 3
General Information 3
Detection 3
Signatures 3
Classification 3
Process Tree 3
Malware Configuration 3
Yara Overview 3
Dropped Files 3
Sigma Overview 3
Signature Overview 3
AV Detection: 4
Phishing: 4
Mitre Att&ck Matrix 4
Behavior Graph 4
Screenshots 5
Thumbnails 5
Antivirus, Machine Learning and Genetic Malware Detection 6
Initial Sample 6
Dropped Files 6
Unpacked PE Files 6
Domains 6
URLs 6
Domains and IPs 7
Contacted Domains 7
Contacted URLs 7
URLs from Memory and Binaries 7
Contacted IPs 7
Public 7
General Information 8
Simulations 8
Behavior and APIs 8
Joe Sandbox View / Context 8
IPs 8
Domains 9
ASN 9
JA3 Fingerprints 9
Dropped Files 9
Created / dropped Files 9
Static File Info 39
No static file info 39
Network Behavior 39
Network Port Distribution 39
TCP Packets 40
UDP Packets 40
DNS Queries 40
DNS Answers 40
HTTPS Packets 41
Code Manipulations 48
Statistics 48
Behavior 48
System Behavior 48
Analysis Process: iexplore.exe PID: 5856 Parent PID: 800 49
General 49
File Activities 49
Registry Activities 49
Analysis Process: iexplore.exe PID: 5828 Parent PID: 5856 49
General 49
File Activities 49
Registry Activities 49
Disassembly 49

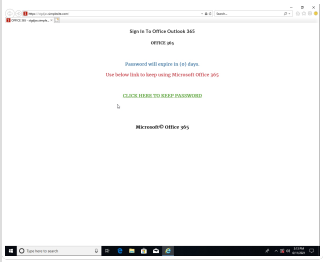
Analysis Report https://stgdjas.simplesite.com/

Overview

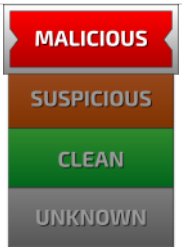
General Information

Sample URL:	http://https://stgdjas.simplesite.com/
Analysis ID:	433276
Infos:	

Most interesting Screenshot:



Detection



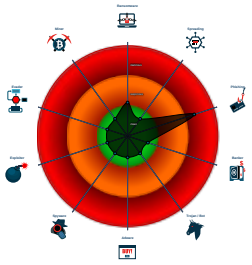
HTMLPhisher

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

Signatures

- Antivirus detection for URL or domain
- Yara detected HtmlPhish10
- Phishing site detected (based on log…
- HTML body contains low number of …
- HTML title does not match URL
- Suspicious form URL found

Classification



Process Tree

- **System is w10x64**
- iexplore.exe (PID: 5856 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5828 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5856 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\6QB31PCD.htm	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\44816H94.htm	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Phishing:

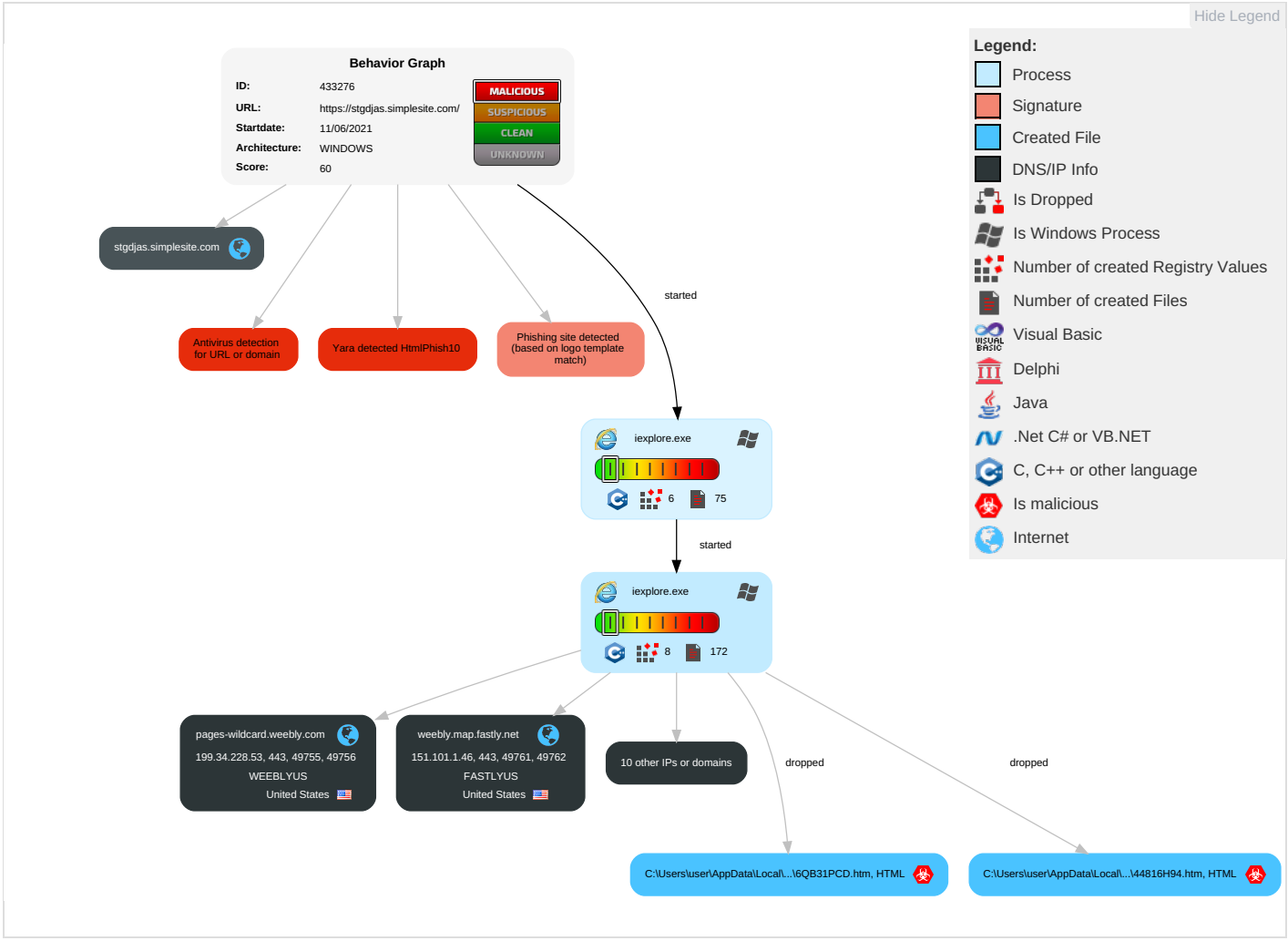
Yara detected HtmlPhish10

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	Impac
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modif Syste Partiti
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Devic Lockc
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delet Devic Data

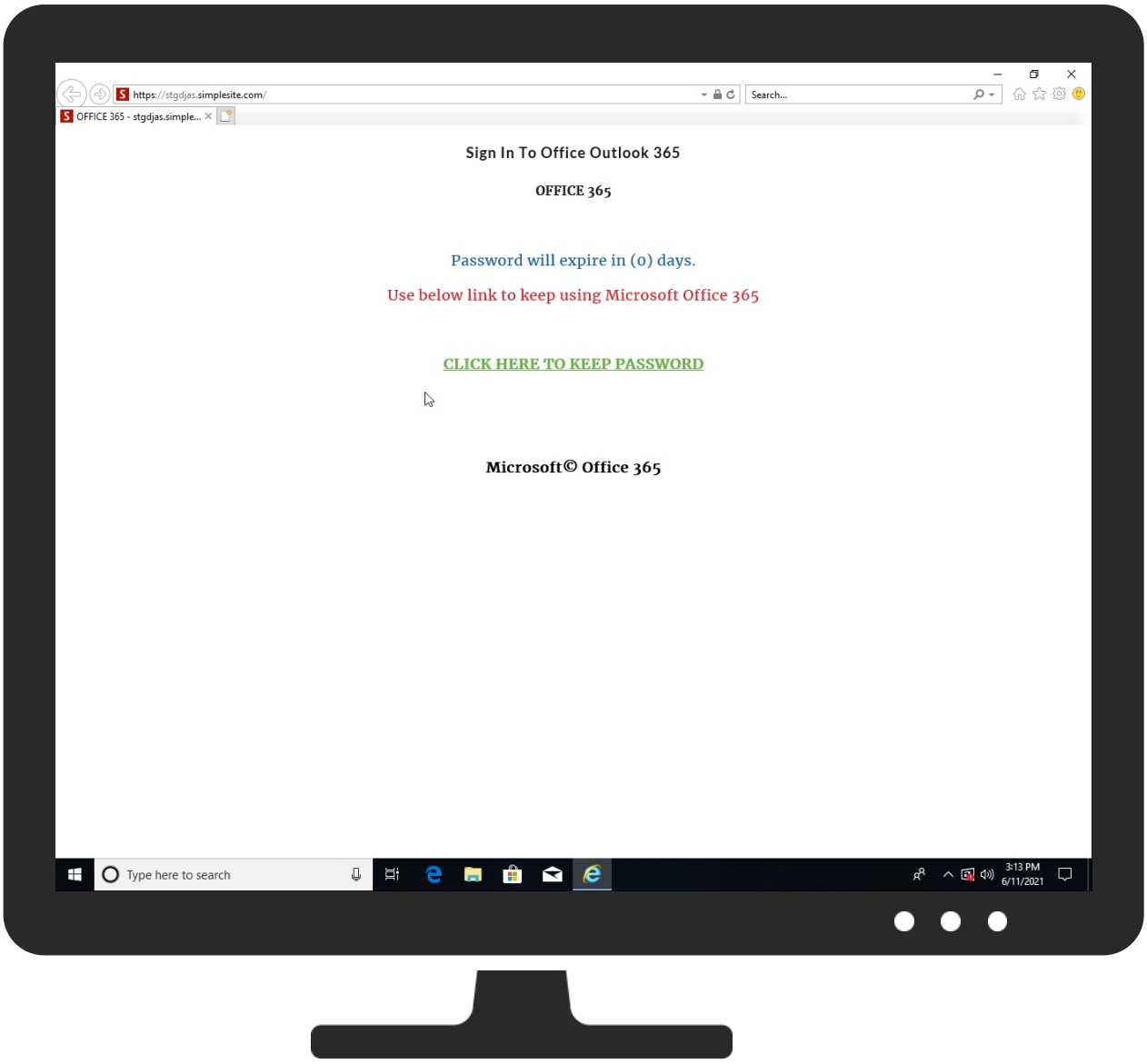
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://stgdjas.simplesite.com/	1%	Virustotal		Browse
http://https://stgdjas.simplesite.com/	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://offi4hf.weebly.com/	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	

Source	Detection	Scanner	Label	Link
http://https://fontawesome.comhttps://fontawesome.comFont	0%	Avira URL Cloud	safe	
http://https://www.gstatic.cn/charts/%	0%	URL Reputation	safe	
http://https://www.gstatic.cn/charts/%	0%	URL Reputation	safe	
http://https://www.gstatic.cn/charts/%	0%	URL Reputation	safe	
http://https://www.internalfb.com/intern/invariant/	0%	URL Reputation	safe	
http://https://www.internalfb.com/intern/invariant/	0%	URL Reputation	safe	
http://https://www.internalfb.com/intern/invariant/	0%	URL Reputation	safe	
http://https://www.google.%/ads/ga-audiences?	0%	URL Reputation	safe	
http://https://www.google.%/ads/ga-audiences?	0%	URL Reputation	safe	
http://https://www.google.%/ads/ga-audiences?	0%	URL Reputation	safe	
http://https://stgdjas.simple	0%	Avira URL Cloud	safe	
http://fontforge.sf.net)IoniconsIoniconsMediumMediumFontForge	0%	Avira URL Cloud	safe	
http://fontforge.sf.net)	0%	Avira URL Cloud	safe	
http://hammerjs.github.io/	0%	Avira URL Cloud	safe	
http://www.bohemiancoding.com/sketch	0%	URL Reputation	safe	
http://www.bohemiancoding.com/sketch	0%	URL Reputation	safe	
http://www.bohemiancoding.com/sketch	0%	URL Reputation	safe	
http://https://offi4hf.w	0%	Avira URL Cloud	safe	
http://https://www.gstatic.cn/charts/debug/%	0%	URL Reputation	safe	
http://https://www.gstatic.cn/charts/debug/%	0%	URL Reputation	safe	
http://https://www.gstatic.cn/charts/debug/%	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://fontforge.sf.net)Created	0%	Avira URL Cloud	safe	
http://https://offi4hf.weebly	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
css.simplesite.com	52.222.158.15	true	false		high
pages-wildcard.weebly.com	199.34.228.53	true	false		high
scontent.xx.fbcdn.net	31.13.92.14	true	false		high
stgdjas.simplesite.com	52.222.158.113	true	false		high
sp-20200214123011524900000000a-1069308460.us-west-2.elb.amazonaws.com	52.43.249.183	true	false		high
www.simplesite.com	52.222.158.77	true	false		high
weebly.map.fastly.net	151.101.1.46	true	false		unknown
ec.editmysite.com	unknown	unknown	false		high
cdn2.editmysite.com	unknown	unknown	false		high
fpdownload.macromedia.com	unknown	unknown	false		high
offi4hf.weebly.com	unknown	unknown	false		high
connect.facebook.net	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://stgdjas.simplesite.com/	false		high
http://https://offi4hf.weebly.com/	false	• SlashNext: Fake Login Page type: Phishing & Social Engineering	high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
31.13.92.14	scontent.xx.fbcdn.net	Ireland		32934	FACEBOOKUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
151.101.1.46	weebly.map.fastly.net	United States		54113	FASTLYUS	false
52.43.249.183	sp-20200214123011524900000000a-1069308460.us-west-2.elb.amazonaws.com	United States		16509	AMAZON-02US	false
199.34.228.53	pages-wildcard.weebly.com	United States		27647	WEEBLYUS	false
52.222.158.15	css.simplesite.com	United States		16509	AMAZON-02US	false
52.222.158.77	www.simplesite.com	United States		16509	AMAZON-02US	false
52.222.158.113	stgdjas.simplesite.com	United States		16509	AMAZON-02US	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	433276
Start date:	11.06.2021
Start time:	15:12:29
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 9s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://stgdjas.simplesite.com/
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:	3
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal60.phis.win@3/92@9/7
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browsing link: https://offi4hf.weebly.com/
Warnings:	Show All

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\stgdjas.simplesite[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	39
Entropy (8bit):	2.469670487371862
Encrypted:	false
SSDEEP:	3:D90aK1r0aK1r0aKb:JFK1rFK1rFKb
MD5:	B9C5EB570521110110BB7DFF12AF780D
SHA1:	27F5BEBC2200FD8D0B51A93D1357EA954BE44079
SHA-256:	90171F10A6467C9DC31143859BAB69D045B67B39E2E49D92BB7168B383C4D1AB
SHA-512:	BC81539E62D643808CBDA3D86050058F379B2F0347CE65CBBA9797D386401C886B22AC4C0B2BE68197AE10C83A1E22A14232CD531C8D139DD3C031DB423EA3
Malicious:	false
Reputation:	low
Preview:	<root></root><root></root><root></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\URW0GA4Q\offi4hf.weebly[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	10244
Entropy (8bit):	5.6608244767188625
Encrypted:	false
SSDEEP:	192:3SSOeYY02JtSSOeYY02JtSSOeYY02JgSS1LeeFCH8MQm:CSOS02JQSOS02JQSOS02J/S1LQcMQm
MD5:	C7157AD237F433E0CC6B2B0AC1297A51
SHA1:	3BA320558BB32CD8852B2781B729FE82118D6F9A
SHA-256:	45DB72B4E21C4D6FEC5900FDFDB41A4174BFD32899BFD0D336CEAB5D0ED75406
SHA-512:	550A70496ADBB4B7DB3735912FD99D916B0967C47BFC7DB9853EFEDE5F6E380BF06DE4FD8F525C584A76E779529363CD88D5D860B6B2BC842935EF6D139AED8
Malicious:	false
Reputation:	low
Preview:	<root></root><root></root><root></root><root><item name="snowplowOutQueue_snowday__wn_post2" value="[{"evt":{"e":"pv","url":"https://offi4hf.weebly.com/","page":"137998350:543172077923215215","tv":"js-2.6.2","tna":"_wn","aid":"_wn","p":"web","tz":"Europe/Berlin","lang":"en-US","cs":"utf-8","f_pdf":"0","f_qt":"0","f_realp":"0","f_wma":"0","f_dir":"0","f_fla":"1","f_java":"1","f_gears":"0","f_ag":"0","res":"1280x1024","cd":"24","cookie":"1","eid":"6eead8f9-8b62-4295-9247-8a623ac1d7f1","dtm":"1623417226145",

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{C7133109-CAB6-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8503312052902379

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{C7133109-CAB6-11EB-90EB-ECF4BBEA1588}.dat	
Encrypted:	false
SSDEEP:	192:r7ZcZa2tWHteifkMuzMhOmBCADBsfTMfjX:rNcZkNP1LZkc
MD5:	DFA7025497E5BCC883522501F5F82015
SHA1:	0988705F3D2E516C2CC3176009539CC756B7B850
SHA-256:	F31522D6710ECEFD1A95FC83355640F993AD6DB72F5C9F2BEB35690BE4DAA415
SHA-512:	C51325F3BB91EB54717A01B6657A5FA7903551D5EBEB1CF147098BBF6A671F802B3DBEF3A694EEED1F6881BF1449DBEFB98565CF2150765D00508B582AA0D02
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\{C713310B-CAB6-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	51044
Entropy (8bit):	2.2426005981471375
Encrypted:	false
SSDEEP:	192:r1ZWQW6Uk7jp2ZWAM/w9jlD+AK10hgoPRQ+AK10hgoBRqYRQl47yypatJPk7aMov:r7jh5n4IVIZh+3n+3TLpRpoPBMiR
MD5:	A810EB1E231BFBB6B934DBA0D8B7F312
SHA1:	7BA3D7EFE73766A7296DED151A15C51FF61F1FA3
SHA-256:	43B64A77A16211E7CE86D4A9C42C09CC9BF5C2F93E997BC0C9D9F4DE5EAFBE37
SHA-512:	8C19DC1095B57387C11D997EF087E82074CB4CCF25C8FAF8CEF706DBC521EBFE3C9FB45B4DB37D6CA3D95FB2AD5CA433BE6C6218A4A17CD0E04D7EEED9A6C0A1
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\{CDB12750-CAB6-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5647447472559217
Encrypted:	false
SSDEEP:	48:IwNjGcprAGwpaljG4pQtGrapbSkGQpKOG7HpR5TGIpG:rNZZIQlV6NBS8AJT/A
MD5:	781B7944338CE3A90A75922C21E4F305
SHA1:	2CB10A1E487DBE303D61C697DE5D3FCF242B0AC3
SHA-256:	43D45641A4B7B163E002D25B080564249B81C6EB2887D66FB44F85293A72BA37
SHA-512:	0F415BCD1003FEE204091E48159E9D797214673CE75E431B0454BD83B2C28C09A3F4D0DEF89445CAA4998E67CBD5D773DD9B8C4EAE0EFDBDD598AFE5799B26A
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.056673058762057
Encrypted:	false
SSDEEP:	12:TMHdNMNxOEQWEgWErnWimI002EtM3MHdNMNxOEQWEgWErnWimI00OYGVbkEtMb:2d6NxOHm1SZHKd6NxOHm1SZ7YLb
MD5:	F6BDCFCC113C74F777A84DCDDB4F95B7
SHA1:	3F644336CDFB16A46B336894744D5033308CE47F
SHA-256:	9A5E37E46C2DA0FC57B62D4EF06D496BA12A053D4E038C2FF2AF9107AED8A48C
SHA-512:	3C41D6FF4CCB8E6083FF7A68A6F07269694CB15A8B0A59836C4057D428D41949C08DA9FA35AD0392356AB7F4CAB00AFAFC79C0E60B54E71CE670EEFF535CD13

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x9da3590f,0x01d75ec3</date><accdate>0x9da3590f,0x01d75ec3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x9da3590f,0x01d75ec3</date><accdate>0x9da3590f,0x01d75ec3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Twitter.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.116907998821623
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kTcBjcBrnWimI002EtM3MHdNMNxe2kTcBZnWimI00OYGkak6EtMb:2d6Nxr8YqSZHKd6Nxr8ySZ7Yza7b
MD5:	04FEA26DBEB248C4634C0B72297AE0FA
SHA1:	A7FD018D15DF98AF931C60DF5428EE1929F41C60
SHA-256:	BA636818C37ED54FD8058EA2E56DCC0751A0DA7437CD34CBD007A21F6A45FA54
SHA-512:	7912355C24AFDEBC06C7B1EA92B5EA105ADA003929127A3247272A9B3805062DDD1062B134DA70E0AE49A6485786704ED5D2650B418AF586ED3AE2A7B989D79
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x9d845a8f,0x01d75ec3</date><accdate>0x9d845a8f,0x01d75ec3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x9d845a8f,0x01d75ec3</date><accdate>0x9d8b817c,0x01d75ec3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Amazon.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	662
Entropy (8bit):	5.075095088023993
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLQWEgWErnWimI002EtM3MHdNMNxvLQWEgWErnWimI00OYGmZEtMb:2d6NxvEm1SZHKd6NxvEm1SZ7Yjb
MD5:	7E820A97213CEDB1FA0D12794CDB17D1
SHA1:	C6D0DB80BA14CA6F93BE4B755029828BCF3FCACD
SHA-256:	5C1DC346133FC1BF8151A4A51313E17F3BD455A69F5D8714491A9684016D1A51
SHA-512:	0C7812495CB1FB80CDBD1A95A05AF6631F3E4F84C2E9E901444FB00CF29D1BEC42A0F1335F3A385A3385F9C33B0F386A1E430F9FC576F652C592899D8F46D786
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x9da3590f,0x01d75ec3</date><accdate>0x9da3590f,0x01d75ec3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x9da3590f,0x01d75ec3</date><accdate>0x9da3590f,0x01d75ec3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Wikipedia.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	647
Entropy (8bit):	5.084490354739629
Encrypted:	false
SSDEEP:	12:TMHdNMNxiIc3nWimI002EtM3MHdNMNxiIc3nWimI00OYGd5EtMb:2d6Nxpc3SZHKd6Nxpc3SZ7YEjb
MD5:	8D9D98E2759D1263BBE4C6EEC4093D61
SHA1:	E168D1E5F8F75EA1A2BA39B9EC73308A25AD8C9C
SHA-256:	27C5347C093452F171F6A3B8E73494FE21A5D184DDFFADC16C6EBAF0B88ED889
SHA-512:	9B8731AA2E6A4A6D3A101DEB22C2292ADCB6BD126240594DAAF163D1C4474C4BF0CDEA7F67D77B12AD7879F52258C446937647E6F42B7FB18AD819103E76E8E6
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x9d99cf98,0x01d75ec3</date><acc date>0x9d99cf98,0x01d75ec3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x9d99cf98,0x01d75ec3</date><accdate>0x9d99cf98,0x01d75ec3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Live.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.0909745119263174
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwQWEgWErnWimI002EtM3MHdNMNxhGwQWEgWErnWimI00OYG8K075Es:2d6NxQzm1SZHKd6NxQzm1SZ7YrKajb
MD5:	36C6C41D12D5CE12570A0DFD7E8DA425
SHA1:	BD4E8C92ED4DDF60B93934F3309E8720A59BC823
SHA-256:	65276965AFDB5992B1FD1459F4E2E1026EB50453660EF52365008014C96F951E
SHA-512:	99E4C8CBEBE337EC0DFD865F643A334D00A62752E13584ECAFA9273CF496A9591AB1E05269804E375A29C2467DE832DB8215063110E4578215378B89E363AD78
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x9da3590f,0x01d75ec3</date>< accdate>0x9da3590f,0x01d75ec3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x9da3590f,0x01d75ec3</date><accdate>0 x9da3590f,0x01d75ec3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Youtube.url"/> </tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.0704690157945995
Encrypted:	false
SSDEEP:	12:TMHdNMNx0nIc3nWimI002EtM3MHdNMNx0nIc3nWimI00OYGxEtMb:2d6Nx0Ic3SZHKd6Nx0Ic3SZ7Ygb
MD5:	A8FC9A6660BD67FF9C2CCEDDCC990276
SHA1:	76DC2B9AD91A7140DD23C93DDDA3A4AE994B352D
SHA-256:	3A7929984B4EEDFD0CE3DFE8BAC522667B3F504CAF62F4064F105AB513EF4914
SHA-512:	C5137C45C425A0502ADBD5304D3DBA2557FECDB32DFE87871D5304689B001A193C267A5DFA7D742E27EEAC8ACEB1416BDF677FCE3CB4DDF4E20B1BE023079 98
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x9d99cf98,0x01d75ec3</date><a ccdate>0x9d99cf98,0x01d75ec3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x9d99cf98,0x01d75ec3</date><accdate>0x9 d99cf98,0x01d75ec3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Reddit.url"/></tile> </msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.109005242544494
Encrypted:	false
SSDEEP:	12:TMHdNMNxxIc3nWimI002EtM3MHdNMNxxIc3nWimI00OYG6Kq5EtMb:2d6Nxmc3SZHKd6Nxmc3SZ7Yhb
MD5:	221C46BABD5F6FD3CB6A37E5B39C8A05
SHA1:	1E4BA864115273D6812E782902BF87D61B27E0E1
SHA-256:	4BB2E8B04C8DF51DE33FA52B2A0D6ED47675DBB36E2AAF6617B3A10C429BF1ED
SHA-512:	9E1F3BC7D27EC1F3CFAA9F7994C2A19FCB03B911A341A3EAB7AF872A2DC15154F542CE6AF47D48E5E35372B7EFC961507F6934A5242084AC51DB64F39D5B692 7
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x9d99cf98,0x01d75ec3</date>< accdate>0x9d99cf98,0x01d75ec3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x9d99cf98,0x01d75ec3</date><accdate>0 x9d99cf98,0x01d75ec3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\NYTimes.url"/> </tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	659
Entropy (8bit):	5.087839614877717
Encrypted:	false
SSDEEP:	12:TMHdNMNxcIc3nWimI002EtM3MHdNMNxcIc3nWimI00OYGVEtMb:2d6Nx3c3SZHKd6Nx3c3SZ7Ykb
MD5:	FDBCEB96C936686C61BEB8EBB2DBD978
SHA1:	958B81F0A00C100A0C8729075B6745F8626A3BF5
SHA-256:	0CFE6CFDD466C7D304B5A6ABAF78B9556D5CB474C417212BBBCB4EE12482E184
SHA-512:	1462785DCD211FCDFA3B0FE3313899B70C2758506D413C63CF2DBD44510CFBA6D2C0DC50BAEFF43A494F46A4A6AC0DB0EF36202AD1D083A83F7B73B9293DF(8C
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x9d99cf98,0x01d75ec3</date><accdate>0x9d99cf98,0x01d75ec3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x9d99cf98,0x01d75ec3</date><accdate>0x9d99cf98,0x01d75ec3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Facebook.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.070062376811014
Encrypted:	false
SSDEEP:	12:TMHdNMNxfnIc3nWimI002EtM3MHdNMNxfnIc3nWimI00OYGe5EtMb:2d6NxAc3SZHKd6NxAc3SZ7YLjb
MD5:	8D061179428B032ED4D7274C2F9C5380
SHA1:	AAA13D7878E39446626B3AC8589502DC824C3481
SHA-256:	F63E881C4C9781AB5EAC193183FA1E7E8A491B3685C81545E11E4D0A0FB6C425
SHA-512:	EFD07560512C51260D75A16975F4E5E2464BC022C0A8390E2E2DC1BFC78004FD10B8D0A639014C1BE1E2BD9C8B21BB7FD05A872EE018CD29E20782DEC28896(
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x9d99cf98,0x01d75ec3</date><accdate>0x9d99cf98,0x01d75ec3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x9d99cf98,0x01d75ec3</date><accdate>0x9d99cf98,0x01d75ec3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Google.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\gee00pr\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	6149
Entropy (8bit):	5.604606838941621
Encrypted:	false
SSDEEP:	96:Q4hwJzrZchDlyAXQ8yUdduBiloycKeRg8xbtsOc:rhwJzruDxkUzuBiay7eu84
MD5:	80E4D2B3D97C000C65E267D735A100BB
SHA1:	29ADACF02658C6649FB3E44678432A9C6BCE419D
SHA-256:	21067078389A90C85A664DCF15E6EA2C2A3F5E13F73B42F62DC6A913E0BCFAA8
SHA-512:	498BF7FEE91016EBD61A3720E5F9608490085E63449E806581AF0CEFD7F86045F64F8C1C7BD53A68E8CC7EF2AAD423429E78660B627A2D392F2819109DE01EEA
Malicious:	false
Reputation:	low
Preview:	2.h.t.t.p.s.:./.7.s.t.g.d.j.a.s...s.i.m.p.l.e.s.i.t.e...c.o.m./.f.a.v.i.c.o.n.-.1.9.4.x.1.9.4...p.n.g.K....PNG.....IHDR.....,?.....gAMA.....a.....sRGB.....NPLTE.....xl..... .....!..../.....4 .aR.M<.H;....aU.W.....IDATx.... .E.F...x.....x29.....I.~H*..W5....$...B.P(...B.P(...B.P..}W\.$u..C.hX.....,....,v.e.T..-gE.....WYQ!g. .8...*|.T.dH.@..#.)N.v ...@.h..U@.~..".9.0..(~.f.8.....r....<.F..H..AA.#..3.B.F.....*...X_}LP.....: .....m..W .6.....k.....%.k..s.A(...9)E..&....\.....i....v$.....v.../..hUe.k9*..}~..F....,v.vQ.A5..... I...j.....X..4...g.82!X.....b...6.3T.n...,}a..4..q...8.{0.0...*.Hs.Q.{N.0%=k..<...Ub.I..#..K.v.....@..(...!...\..~C..... .....P.*..s.....-G*I...5S.u.KRI.....`60.[.<....~.,U.a.....2O.....v... <)..5...ME{....*.....TT$a..0.z....3..CQ..4.=.2.....4..3w._...&'..I.N...f.<!..C.yBx2.b.....<nV....!u.....wB.....O..!O..;.....F.;b.....E...0H.{b.4.A4>...e.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\2FBPUZBU.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):	45181
Entropy (8bit):	4.706387835098436
Encrypted:	false
SSDEEP:	768:598NfFi6ZiF48afFi6ZiF3lSuI8Qt6ZoE4Eo29ug:5u0faMfjjjoEv9ug
MD5:	62112A4C47BF298D6B59B0F93E1B64F5
SHA1:	6A5E22752A943CEB518BAB65F4C1C228F1D242BB
SHA-256:	0B55E1C916AEE97834D8534065F5E3673DD2321EB2F488C72F2981603CA75E29
SHA-512:	0EDDF796A8FCA8D4B0DBE8799606A79159EFC8371178483D4CA5173E8048F1FF3E0AE983F29A742040EB4C5EA4722C3134DDCC6D365E6807C4358D4DD2CB18 5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://stgdjas.simplesite.com/
Preview:	..<script type="text/javascript">. var thisDomain = ";. if (thisDomain.length > 0) {. document.domain = thisDomain;. }.</script>..<!DOCTYPE html><html l ang="en-US">.<head>. <title>OFFICE 365 - stgdjas.simplesite.com</title>.<meta property="fb:app_id" content="1880640628839943" />.<meta property="og:site_name" content="Sign In To Office Outlook 365" />.<meta property="article:publisher" content="https://www.facebook.com/simplesite" />.<meta property="og:title" content="Sign In To Office Outlook 365 ~ " />.<meta name="twitter:title" content="Sign In To Office Outlook 365 ~ " />.<meta property="og:locale" content="en_US" />.<meta property="og:u rl" content="http://stgdjas.simplesite.com/" />.<meta property="og:description" content="Password will expire in (0) days...Use below link to keep using Microsoft Office 365....CLICK HERE TO KEEP PASSWORD .....Microsoft. Office 365" />.<meta name="twitter:description" content="Password will expire in (0) days...Use below link

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\44816H94.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with CRLF, LF line terminators
Category:	downloaded
Size (bytes):	22675
Entropy (8bit):	5.323776605341182
Encrypted:	false
SSDEEP:	384:rhWIRIOITIwIgIiKZgNDfIwIGI5IVJ7SHuzIRIOITIwIgIiKZgNDfIwIGI5IVJ7w:oIRIOITIwIgIiKZgNDfIwIGI5IVJ7Sq+
MD5:	621D92CD1F1F8A7D1D13E5D7273B7EED
SHA1:	35AE2299F4B75F3AD1DD359D5823090C9796DA6E
SHA-256:	89A452C15260197720507D9D41A4B64C2D2BBDD500DF278F695BA9BA409DAEC4
SHA-512:	DB0466606EBD49C3993F518B1A4652A2CB4C2DC78FFEED78D02D259E23A3995AF5208EE56245C65C2BE7244BCD3010E2930AE98DC54E94D32110AB84A4DC19 4
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_10, Description: Yara detected HtmlPhish_10, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\44816H94.htm, Author: Joe Security
Reputation:	low
IE Cache URL:	http://https://offi4hf.weebly.com/
Preview:	<!DOCTYPE html>.<html lang="en">..<head>...<title>Sign In</title><meta property="og:site_name" content="" />.<meta property="og:title" content="My Site" />.<meta property="og:description" content="" />.<meta property="og:image" content="https://offi4hf.weebly.com/uploads/1/3/7/9/137998350/mirosoft-1sign-in-1_orig.png" />.<meta property="og:image" content="https://offi4hf.weebly.com/uploads/1/3/7/9/137998350/homail-n2-origsign-in-options-2-1_orig.png" />.<meta property="og:url" content= "https://offi4hf.weebly.com/" />....<meta http-equiv="Content-Type" content="text/html; charset=utf-8"/>. <meta name="viewport" content="width=device-width, initial-scal e=1.0"/>.. <link href="//fonts.googleapis.com/css?family=Karla:400,700|Oswald:700|Roboto+Mono:400,400i,700,700i" rel="stylesheet">. <script src="/files/theme/ MutationObserver.js"></script>. <style>. .navbar__logo .icon,. .navbar__center .navbar__logo:after {. color: #2990ea !important;. }.. .header-prompt . navbar__li

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\71584491.design.v1622630893[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	270609
Entropy (8bit):	5.181803216529539
Encrypted:	false
SSDEEP:	1536:sEf8fplaBh2rDN/ftOo3iPJxTnfQiezE1uls43Clv7:E7NyPwieKvN
MD5:	71895EAA9C16A5272649676E9F2BC986
SHA1:	572E5648EA4768FEF2C2034733D2C98D9C28C648
SHA-256:	EBFB2490A2C7E480D2A9D7C969084FD44E3E262E08B4FC0B24C79385BA047E50
SHA-512:	FADD6C04A519B98186477D7E2ABA409C4F4C2A3347275953512E7607E208342576EA95E4C4D76AB9438DD6DD454DD6650AC8C3375B1550D1CBED85F330928D9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://css.simplesite.com/e4/05/71584491.design.v1622630893.css?h=ebfb2490a2c7e480d2a9d7c969084fd44e3e262e08b4fc0b24c79385ba047e50

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\71584491.design.v1622630893[1].css	
Preview:	/* LESS Output Begin */.../* MD5-Hash:[d41d8cd98f00b204e9800998ecf8427e] */..@import url(https://fonts.googleapis.com/css?family=Lato:700|Merriweather&subset=cyrillic,latin-ext,vietnamese);.nivoSlider{position:relative;width:100%;height:auto;overflow:hidden}.nivoSlider img{position:absolute;top:0;left:0;max-width:none}.nivo-main-image{display:block!important;position:relative!important;width:100%!important}.nivoSlider a.nivo-imageLink{position:absolute;top:0;left:0;width:100%;height:100%;border:0;padding:0;margin:0;z-index:6;display:none;background:#fff;filter:alpha(opacity=0);opacity:0}.nivo-slice{display:block;position:absolute;z-index:5;height:100%;top:0}.nivo-box{display:block;position:absolute;z-index:5;overflow:hidden}.nivo-box img{display:block}.nivo-caption{position:absolute;left:0;bottom:0;background:#000;color:#fff;width:100%;z-index:8;padding:5px 10px;opacity:.8;overflow:hidden;display:none;-moz-opacity:.8;filter:alpha(opacity=8);-webkit-box-sizing:border-box;-moz-box-sizing

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\L0xoDF4xlVMF-BfR8bXMIjhOsXG-q2oeuFoqFrlnANW6Cp8[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 16816, version 1.1
Category:	downloaded
Size (bytes):	16816
Entropy (8bit):	7.964169744371369
Encrypted:	false
SSDEEP:	384:9OWQ5QLa70ZbhxyJ7fONxlTWsc0PN5ojCMhcgD+DTXUjm:cvZ0Zdxyv23GN5ojCMa0m
MD5:	A1CC60361C99F033672F308F0398A6D0
SHA1:	7744101997EAA0C3A8A8CDBA518780FFAE662FA4
SHA-256:	6B7ECCAF20B191C69B769802BD09D73DE2D8133168C94EF482F6B0015946601A
SHA-512:	FE56D94D934DA78821F7256F7294CB5A988652D61500594F0449A4A368345FEF2AF6AFC689EF3A5054333BD762D5B60774203043DAB912429FF5D47BEBA630AF
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/robotomono/v13/L0xoDF4xlVMF-BfR8bXMIjhOsXG-q2oeuFoqFrlnANW6Cp8.woff
Preview:	wOFF.....A.....].....GSUB...D...5...6....OS/2...|...P...`...CSTAT.....:...D.I..cmap.....y...68.<.gasp.....glyf.....9e..S&X...head..<....6...6.;..hhea..=,.....$....hmtx..=L...@....C.>.loca..>.....>.Emaxp..@H..... ...bname..@d...&...r<p].post..A..... .c.eprep..A.....h...x.c`d``.b0b0a`qq..a.J.,.aPl/J.fP.I,.cPa`a.....:...x.c`a..8.....u..1...<.f.....0....@....T..302.....*..G.....\|.....:F.U}.ux.....P.....BD.....@...I.)l.9..\}.3.Q3...>D.*....K..x....XY.E..9.}...m.m.m....N..3...p#.q.0uc.?>.;.M.xo.....H..=.d..=.gb..Zx#\|.>._...O..!....o.....>JJN~..... ....hZ*..#.....t....'Pv!...$o..YI...OJxp....Tt$:....D....Q.(c..~.X.B...b.(.9P...L./....6@1=.TK.M..Fy.U.UE.t.Qge..L7..U.~-...0.Q\.....`G....]\..a...]...4D..d..)y.W9..7..#...X..3...L6.T.L7..3.5K{s,4.|.,RXQ.,...K-..Jk.....|..f[.U.....U..f6.....x.{.|.G.....mK.XZ13.%[...8`...v.aj.4i.&...`.r.i..).W....p.=.^.k....Wi...+.....;.y".....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\L0xoDF4xlVMF-BfR8bXMIjhOsXG-q2oeuFoqFrmAB9W6Cp8[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 16904, version 1.1
Category:	downloaded
Size (bytes):	16904
Entropy (8bit):	7.973722875660465
Encrypted:	false
SSDEEP:	384:zu3nOt0wpvccn4u47Q8U8vUQAk57FsHzJ2japGj1FH3yW:zu3neHkc4uAQocQAUaJkzCW
MD5:	4F6A4879558CA07BF08F179B3C82B587
SHA1:	8543507404E4A03F5B5423497F7A5354E2F5CF39
SHA-256:	84C8F09BDEEF4788E949A78C576CED2BE9578CE238FB405D7CAFB03F4484D08B
SHA-512:	30818A2259235211528 90F85744E607610FD9166095CC6BA1DA307DBEFBE55E2765EFF71D043552E96FC197006CED3DD4D173B7366C71865C0447257B37BD01C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/robotomono/v13/L0xoDF4xlVMF-BfR8bXMIjhOsXG-q2oeuFoqFrmAB9W6Cp8.woff
Preview:	wOFF.....B.....^.....GSUB...D...5...6....OS/2...|...P...`.&.cSTAT.....7...@...,cmap.....y...68.<.gasp.....glyf.....9...SN5.+.head..=P...6...6.<..hhea..=.....$....hmtx..=....6.....:.6.loca..>.....maxp..@..... ...bname..@....-....B.a.post..A..... .c.eprep..B.....h...x.c`d``.b0b0a`qq..a.J.,.aPl/J.fP.I,.cPa`a.....:...x.c`a.....u..1...<.f.....0....@....T..3(2.....*..G.....\|.....:F.i...x.c`.B..&....0...T..Q..df.$.0r..Y...$.0.0..Q .. ..x....XY.E..9.}...m.m.m....N..3...p#.q.0uc.?>.;.M.xo.....H..=.d..=.gb...Zx#\|.>._...O..!....o.....>JJN~..... ....hZ*..#.....t....'Pv!...$o..YI...OJxp....Tt$:....D....Q.(c..~.X.B...b.(.9P...L./....6@1=.TK.M..Fy.U.UE.t.Qge..L7..U.~-...0.Q\.....`G....]\..a...]...4D..d..)y.W9..7..#...X..3...L6.T.L7..3.5K{s,4.|.,RXQ.,...K-..Jk.....|..f[.U.....U..f6.....x.{.|\U..;..7o&....o.%...=M%M....[.*..]..... .wX7..(..,.-..o.....O.L..{.{.....E.3.R,U

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\TK3_WkUHHAIjg75cFRf3bXL8LICs169vsUhiYw[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 28024, version 1.1
Category:	downloaded
Size (bytes):	28024
Entropy (8bit):	7.9789501299216585
Encrypted:	false
SSDEEP:	768:Z+cR1jJ5+wAzCSNNAkFPDjYeiAS+JCih5FCUE5PLc:tXw1zA1qcirKLc
MD5:	DBB638C569A7DB32970F5D6FE3B74043
SHA1:	B6DA307F2EC7E6A2A0D6C44B6C4490CA019D59C0
SHA-256:	3BA58C380713A18E36F466F6165D73459CD064A2422C7E730DD1B28DFE79CD5E
SHA-512:	20A907F1B7C086C7B3FB711454F24A6925D233A7BD0EFE25CCB0C4EFAD2515FFBB8F6021809465A936FE39AF04A8D69AE80DD669313D6D9231A5B505292C36B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/oswald/v36/TK3_WkUHHAIjg75cFRf3bXL8LICs169vsUhiYw.woff

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\TK3_WkUHHAIjg75cFRf3bXL8LICs169vsUhiYw[1].woff	
Preview:	wOFF.....mx.....GDEF.....d..GPOS.....T.'.GSUB.....7...VMAU.OS/2.....O...`..^.STAT...8...&...*y.i.cmap...`.....`..HHcvt ...8...E.....&fpgm..... .6..gasp...D.....glyf...L..N.....+.head..d....6...6....hhea..dH.....$....hmtx..dh.../....#.GJloca..g.....maxp..kp... ... .H.;name..k....'...X8.Y.post..l..... ...2prep..l..... <l.x.....`....~?)...H.Di..Ri..@.="((h..".....=H....)4.fn%i3.CFq.$NY.....oI.<.W|._A....Z..]{..,S\..[...]<x.'....S.*d.....x....%I.....U..v.m....9.g.Ck#..9.m.l.q.w.V.x.*+..S.I...j.....@5._; z.j**.....3r.B..E.(D.p..^.s.....Z..G.9/r^p.....".}<.|.|uT.....#..t.F.#....#....?...zF.W...K..V....OG"..M4.....}{'.....w...../.....A.L..s.y..5.....?.I.9.Ea.p(...O.(O....(.u.....D....j E..*_g..5.y.@-t..Uk..(.....u....O..|=.7t...d..I-.Z..z.R.....Fo[W...,.P..Uv.....S_....ol...6.F.;{..d{....t.sz.-...!{.M.g.D..J.t...$.<._U.+.D..2.....n.....n...-.le.5.m

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\TK3_WkUHHAIjg75cFRf3bXL8LICs1_FvsUhiYw[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 27732, version 1.1
Category:	downloaded
Size (bytes):	27732
Entropy (8bit):	7.980352882318215
Encrypted:	false
SSDEEP:	768:Ay/ZjJ8TCXeCeTHacLH9yStJhsuhiY/WkLIu:zN+S7eDLPn1/Wdu
MD5:	4D221D65C35764F921A2091F9C7D13EE
SHA1:	FDE83D0301134B6E2C8F704C264C1581755AB80A
SHA-256:	E65D08671752DA0AAF460AF9E2A702B11D784FDC6BAC707F7803FBFE4DF9658E
SHA-512:	12010CAB0A62B369B71F8FCDF32705B018C469DB52C0888F822C6CA5F5FD3B6885934A91588718916D63B8C86107DB1ED0BD40E78BF1709F974ABDC605EF85F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/oswald/v36/TK3_WkUHHAIjg75cFRf3bXL8LICs1_FvsUhiYw.woff
Preview:	wOFF.....IT.....GDEF.....d..GPOS.....K....).PNGSUB...`...7...VMAU.OS/2.....O...`.K^.STAT.....&...*y.j.cmap.....`..HHcvt .....D.....%..fpgm...,..... .6..gasp.....glyf.....M.....head..b....6...6....hhea..c(.....$....hmtx..cH...1....K.?.loca..f\|.....maxp..jT... ... .H.;name..jt.....B4.Q.post..k..... ...2prep..k.....<l.x.....`. ...~?)...H.Di..Ri..@.="((h..".....=H....)4.fn%i3.CFq.$NY.....oI.<.W|._A....Z..]{...,S\..[...]<x.'....S.*d.....x.t.3.XA....>..m.m..&vR...lb....z.};g.:.x... .i.....]<c.R....1..9+.....v..g..q.o...Hk .....{[3.#.y.....c%....vVt.#.:...52[..9L..fX...p..ez...*..6s..t.-..6m-m6ky....**..I...zX...N...zGC..i.ja-.....[..d...u.u..*.E..T.{e.Q..V%.Z.ibU.9....S.....@Sf....a-.X.....$7..]^..O|a+.I.. .....^..P.....T....)3y*.d..d.,,....#r.WrL...q2'.?24N...+9...P6N..G8..|=..rEa...hm.m.m.vR...c....m.y....g{.~w..3....]IfU....G....+..".cU...8{0.a....Y.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\arrow-light[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	886
Entropy (8bit):	5.035010292982074
Encrypted:	false
SSDEEP:	12:TMHdt0ubqt7/KYslXXHlPeaxMwm5EIDXqBJVJ/hlIJi2y1dQ9/01klp0u:2dtjbqt7L8FPeaxMwm+ID63zbF+MOf0u
MD5:	552EB2E04260FC0733E5633D15C6AEAA
SHA1:	0A9EFCC3B0EBABB23A49A00061FD8200EDED1613
SHA-256:	705FF3240DE004523FF9D628B28AAD705AD3F0CEB046312495265A4042C67570
SHA-512:	16CD125A26B1604144D6A64F45D1064FF2A71DA412CF61C829914E00C2E4AA275A172D0872A9533F79D5FC2D2BE82A7DFE3FE5F12048C23AF927A7CB35D571C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://offi4hf.weebly.com/files/theme/images/arrow-light.svg?1623367237
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="no"?><svg width="22px" height="11px" viewBox="0 0 22 11" version="1.1" xmlns="http://www.w3.org/2000/svg" xmln s:xlink="http://www.w3.org/1999/xlink">. Generator: Sketch 39.1 (31720) - http://www.bohemiancoding.com/sketch -->. <title>Group</title>. <desc>Created with S ketch.</desc>. <defs></defs>. <g id="UI-Kit" stroke="none" stroke-width="1" fill="none" fill-rule="evenodd" stroke-linecap="square">. <g id="Ui-Kit" transfor m="translate(-61.000000, -697.000000)" stroke="#FFFFFF" stroke-width="1.5">. <g id="Group" transform="translate(62.000000, 698.000000)">. <path d="M0,5 L19,5" id="Line"></path>. <path d="M16,0.5 L20,5.02" id="Line"></path>. <path d="M16,9.02493763 L20,5.02493763" id="Line"></path>. </g>. </g>. </g>.</svg>.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\css[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	579
Entropy (8bit):	5.36499526631253
Encrypted:	false
SSDEEP:	12:jFF5O6ZN6pT4ALqFF5O6ZRoT6pTyjALqFF5O6ZN76pTTFLY:53OYNjAa3OYsXMa3OYN7O8
MD5:	936289D85DFC0C483C7FACBB4B5B4EF0
SHA1:	DE79428618D76536C0D021BC05778B9D971E9AC2
SHA-256:	089131070F90020BE376087C2AC2117A96057BFF81E87C3376202BF5E406C92D
SHA-512:	018A2DAA6D194F5181AEF93A0970FBBED590D990BBD223544675960BA1EDD05F7DEFFFAFEC89F51D9DA399D998AE3A8E50EA30BD726EDBDE34E50909291E88 24
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\css[1].css	
Preview:	@font-face {. font-family: 'Oswald';. font-style: normal;. font-weight: 300;. src: url(https://fonts.gstatic.com/s/oswald/v36/TK3_WkUHHAIjg75cFRf3bXL8LICs169vsUhiYw.woff) format('woff');.}.@font-face {. font-family: 'Oswald';. font-style: normal;. font-weight: 400;. src: url(https://fonts.gstatic.com/s/oswald/v36/TK3_WkUHHAIjg75cFRf3bXL8LICs1_FvsUhiYw.woff) format('woff');.}.@font-face {. font-family: 'Oswald';. font-style: normal;. font-weight: 700;. src: url(https://fonts.gstatic.com/s/oswald/v36/TK3_WkUHHAIjg75cFRf3bXL8LICs1xZosUhiYw.woff) format('woff');.}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\frontendApp.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	832430
Entropy (8bit):	5.342938058319246
Encrypted:	false
SSDEEP:	12288:ekhvBmz6SZTHfqO3icT9Hdmlha16ugogs/6XiZu2sJWdBU/xYYJpSp/blRf:BBw/A3JWdgxYYDSZblJ
MD5:	24E1B01A60106379078E08EB2A131156
SHA1:	8588A1A1E76B5BA5598EFD29C7CB32F6D5139F5C
SHA-256:	4A12751F5E6ABE190738CCE1F72F94DD2E97AB1CD086F983BCDF7DBA97166D9A
SHA-512:	9093F7270F94592928763ABA5553D596742F874083D9FA81B740F808DAFC4AA21A2AB63BED3398972F84019D7C67CC6B8F4F0DABF7943C2DCB00A69E58255D18
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://css.simplesite.com/c/js/frontendApp.min.js?_v=24e1b01a60106379078e08eb2a131156
Preview:	!function(){function t(t){this.setOptions(t);var e=this;this.timerDelegate=function(){e.onTimerEvent()},this.subjects=[],this.subjectScopes=[],this.target=0,this.state=0,this.lastTime=null}function e(e,i,n,o,s){this.els=t.makeArray(e),this.property="opacity"==i&&window.ActiveXObject?"filter":t.camelize(i),this.from=parseFloat(n),this.to=parseFloat(o),this.units=null!=s?s:"px"}function i(e,i,n,o){this.els=t.makeArray(e),this.property=t.camelize(i),this.to=this.expandColor(o),this.from=this.expandColor(n),this.origFrom=n,this.origTo=o}function n(e,i,n,o,s){this.els=t.makeArray(e),this.property=t.camelize(i),this.from=n,this.to=o,this.threshold=s||.5}function o(s,r,a){if(s=t.makeArray(s),this.subjects=[],0!=s.length){var l,c,u;if(a)u=this.parseStyle(r,s[0]),c=this.parseStyle(a,s[0]);else{c=this.parseStyle(r,s[0]),u={};for(l in c)u[l]=o.getStyle(s[0],l)}var l;for(l in u)u[l]==c[l]&&(delete u[l],delete c[l]);var l,h,d,p,f,m;for(l in u){var g=String(u[l]),v=String(c[l]);if(null!=c[l]){if(f=i

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\jquery-1.10.2.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	93064
Entropy (8bit):	5.3000011389598916
Encrypted:	false
SSDEEP:	1536:34mCgi8DyCuXXFiJ+L0kJQsJVPEKLQRZdC/RlfDknv+p0WzH/IoSZ7qABZnu0sFv:3GsKXlI2p0WPSbDrstfam
MD5:	BDCE12C949E78D570C8D44E9C2B23508
SHA1:	9AFDC4FEC954646BD6270CAF82F107FDEF605BC5
SHA-256:	C73B004EBF31B395CF237C3D2B13C1E576F385E04660CEB5F7BE163FF3C201DC
SHA-512:	B96588D93FB86228ECC8F501BEE6DB5F199B20B086FC88C683BBE1FEB6C343DEC3F99467E1D3140B7F4731D07ADF2F918F0CA88BB257D10B5AB8879FF9CE8ED3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.simplesite.com/c/js/jquery-1.10.2.min.js
Preview:	/*! jQuery v1.10.2 | (c) 2005, 2013 jQuery Foundation, Inc. | jquery.org/license.*/.(function(e,t){var n,r,i=typeof t,o=e.location,a=e.document,s=a.documentElement,l=e.jQuery,u=e.$,c={},p=[],f="1.10.2",d=p.concat,h=p.push,g=p.slice,m=p.indexOf,y=c.toString,v=c.hasOwnProperty,b=f.trim,x=function(e,t){return new x.fn.init(e,t,r)},w=/[+-]?(?:\d*\.\|)\d+(?:[eE][+-]?\d+\|)/.source,T=/\S+/g,C=/^[\s\uFEFF\xA0]+\|[\s\uFEFF\xA0]+$/g,N=/^(?:\s*(<[\w\W]+>)[^>]*|#([\w-]*))$/,k=/^<(\w+)\s*\/?>(?:<\/\1>\|)$/,E=/^[\],:{}\s]*$/,S=/(?:^|:|,)(?:\s*\[)+/g,A=/\\(?:["\\\/bfnrt]|u[\da-fA-F]{4})/g,j=/"[^"\\\r\n]*"|true|false|null|-?(?:\d+\.|)\d+(?:[eE][+-]?\d+|)/g,D=/^-ms-/,L=/-([\da-z])/gi,H=function(e,t){return t.toUpperCase()},q=function(e){(a.addEventListener||"load"===e.type||"complete"===a.readyState)&&(_(),x.ready())},_=function(){a.addEventListener?(a.removeEventListener("DOMContentLoaded",q,!1),e.removeEventListener("load",q,!1)):(a.detachEvent("onreadystatechange",q),e.detachEvent("onload",q))};x.fn=x.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\jsapi[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	260
Entropy (8bit):	5.342360473530174
Encrypted:	false
SSDEEP:	6:wRkrQWR0iYBtqWt2aSyujLKdqEijyxGoP:ekrY1tdkytVF
MD5:	06106E5E611CF7B9ACD40CEA9A58B97D
SHA1:	FCFD21286EDAFCEA56FEF947A775A43B539E051F
SHA-256:	BCD7F82C414EC1F4FDF22CC7084E073D6B9C549F2C05C1CE73944611CB70769F
SHA-512:	47700733A2421E2AFB3302B1CA79688BF14CD82E99EA1CD2C17CA6DB605EB9B41E8368A210AA98AD2FA92175C88CF706E2CC51754F6C54513D9B45FB374DA0A
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\jsapi[1].htm	
Preview:	<HTML><HEAD><meta http-equiv="content-type" content="text/html;charset=utf-8">.<TITLE>301 Moved</TITLE></HEAD><BODY>.<H1>301 Moved</H1>.The document has moved.<A HREF="https://www.gstatic.com/charts/loader.js?callback=gloader_ready">here</A>...</BODY></HTML>..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\qkBIXvYC6trAT55ZBi1ueQVIjQTD-JqaHUlM[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 16836, version 1.1
Category:	downloaded
Size (bytes):	16836
Entropy (8bit):	7.964358790587357
Encrypted:	false
SSDEEP:	384:EPfhRZeGrrC/TtyTrlHh42xMzYJ1sES+wNZvl1:EPfbgGvC/Ttol62xMcAj
MD5:	06D6D35949A50C1BF5422AA4D0673375
SHA1:	C69691EA2AC85EE808436FC94D3D50B48BD701D2
SHA-256:	6023B778EBBF9E20115974FBDEC5780D569829D3C3ED6229EE408A804F17D8C6
SHA-512:	735028D258739D34C71B0D2DA5E7D568CAC7A3669DA650AC3D6699A89B7E7466B5C6FCF5EB13CA8A486D37C369B3E8121B5EF72A91FF2074FFB0E245BFF5E7 9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/karla/v15/qkBIXvYC6trAT55ZBi1ueQVIjQTD-JqaHUlM.woff
Preview:	wOFF.....A.....iH.....GDEF...l.....&,.$.GPOS...0...d....N.'.GSUB.....8..OS/2...d...Y...`tMExSTAT.....=...L....cmap.....}.....gasp.....glyf.....0`..O..).head..9....6...6.=.zhhea..: ... ...$...)hmtx..:@...D...8...Bloca..=.....T.@.maxp..@|..... ....name..@....."3[U.post..A..... ...2prep..A.....h...x.-.B.....s..-.vS..lOYs.1l.5...%. [..?.. .....8(....B..B.,G.lF.....\....<.<..V....Ox..J..?..ilk.HG....~ .. .:*..%c.+.. S....-s.'.X$KX.kX/..*{.+.8..8...fp...3:....h6b.m..... ...D".x.}...\Q.E.}..3...Om..j..m....j{..v.",...+.....9.\.I .....f-ZuR...F(Y...n...3B.x6.....D..F.tDa..{}.W.T.c...id.^f..e..m.9g.....qF93.y..g..6.(.KD79.Id.....P.2..,....\|Y*...\|9....U-.V...PS.m...).s/...A.d....^.h..(.'.MtH.J...^W:..l.[....0.\|..G.... ..g...trA.C.....#<.h.;.(...ak..N..v.. .Ag.$..y....yP.D.....g.~.:..}D.m....H2..Mc7.A./.=..s.N.n..C..~2Aj0e5.....x..?.\.6..es.6.....q.....zh.....t.....:.D..E.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\qkBKXvYC6trAT7RQNNK2EG7SIwPWMNmlUHlGb7U[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 17652, version 1.1
Category:	downloaded
Size (bytes):	17652
Entropy (8bit):	7.968434231204158
Encrypted:	false
SSDEEP:	384:+Ngsw3AALigI3iywXYPYSP69b2D9OTT12uyNR:+OswQ+irivYPYSYGQ+X
MD5:	43E4351B978AC9A34431E049161EFC37
SHA1:	5CF5B1069188B228AB94DE4EBC947C9F41376187
SHA-256:	76710356049BECC409C017835AB6E8B4E4A33C7BEDE1E72EBF02C0FE53E8E291
SHA-512:	1306906AF5F2280C2B3A93E4E3AE81E2F3D0D4AC018AA2425BA6892CDC6F98ABC31921AF1228A8FFB09CF28BF8B83BFCC0A951867527358CD65EF98F69A8E72 A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/karla/v15/qkBKXvYC6trAT7RQNNK2EG7SIwPWMNmlUHlGb7U.woff
Preview:	wOFF.....D.....h|.....GDEF...l.....#.&.GPOS...$...q.....h.QGSUB.....-OS/2.....\...`u\|E_STAT.....=...H.I.!cmap...P...}.....gasp.....glyf.....3...N.. .B.head..<....6...6....hhea..=(...#...$.+.jhmtx..=L...j...8...loca..@.....|..maxp..C..... ....name..C.....04BS.post..D..... ...2prep..D.....h...x...1.A.....y.ldT."..dOY....d6.-..(.>.nP2I.....~.. .R.....#A..o...]..k6v...9.#g{.joN.y.'/.v...O E..I%..*..e.....-.I+..j...m.e...zv...hbgZ .... .o.....JG..>..c...61!r...x.}....A....}....}....5..m.EP...v..oXn.l.5..?s...Y.I1..z*.M.nJ.? u.....;a.R.&I.Sf..q..%..5.f.....Vh...n.B.j<.d.L..1.L...L23."...0..M..c>{..A..o.7.[.=/.V.]......IIJV..*M..PP.*...|....Z..l6..<5T.....jb7...s.R.K.V...k..}..E(....U*1.5H.....2G..!N....>f..3.h." U{l.r.!.9Gs.....,s.Md..~+`3`.`~.V..P.....F...7e.....R..xE].....D9.rCM....;>R.....P.|....%@.>.....+.J.,..D.sg.1....rc.....P...qC.)!5...8y..=l....aC.5rn.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\sdk[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	230982
Entropy (8bit):	5.453484742206776
Encrypted:	false
SSDEEP:	3072:xZMnQPPQ6sK4+sdHPAi/y0NeSeffmj+0Er:A+PQ6sR+sdHn/y0NFeffmEr
MD5:	8BFBD3D1CDDD3BBE8108CEB8DABE81ED
SHA1:	56CE42935F4FDEC2DFA2E956C1D3782A74FF21CB
SHA-256:	FBF22BE26CEAF5384E4E26124DB8340AB550E52F5B5E6CAB1182EC567C6405AD
SHA-512:	431D4CAD246B2C09A4BE8A43441F85F3FF958F337F5D22091F3C95E4436D7B64E0F064B02AC2A310CF71711A46692FA9BCB77769963ECB866F25C5944B09E4AE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://connect.facebook.net/en_US/sdk.js?hash=6d915dd7dfb8d12e71575522c27a214a

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\sdk[1].js	
Preview:	/*1623414165,,JIT Construction: v1003951569,en_US*/../**. * Copyright (c) 2017-present, Facebook, Inc. All rights reserved.. *. * You are hereby granted a non-exclusive, worldwide, royalty-free license to use,. * copy, modify, and distribute this software in source code or binary form for use. * in connection with the web services and APIs provided by Facebook.. *. * As with any software that integrates with the Facebook platform, your use of. * this software is subject to the Facebook Platform Policy. * [http://developers.facebook.com/policy/]. This copyright notice shall be. * included in all copies or substantial portions of the software.. *. * THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR. * IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTAB ILITY, FITNESS. * FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR. * COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER. * IN AN ACTION OF CO

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\simplesite-webfont-2[1].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), icomoon family
Category:	downloaded
Size (bytes):	55496
Entropy (8bit):	6.396305200414213
Encrypted:	false
SSDEEP:	768:KfDTG2CCBlaiDK/hd8jYUf3hk7AGJt7th4b5beREog++M3tW+lOA38mTRtZdwm:8DC2nnDCMvKsy4b5Ego3TlOA38IRtZG
MD5:	021B62820C595CFB9C92772243EA042E
SHA1:	44869A9DD3E758A0334CAACAB4AF01B1091BEBE7
SHA-256:	58BCBD4EB40DEFDD10E5CEEC3A589E77B0AC875E1BE699FB1EACDA86D138DCE1
SHA-512:	476A0F03889D6F366E454E3CBA10E513533A0B6CABD582BFD4B4E13F0249018A426B919B632566C363E18068A0033956B1C7924ADAFC3CB28CDE0B3B5675B208
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://css.simplesite.com/d/fonts/simplesite-webfont-2.eot
Preview:	....$.....LP.....B.....i.c.o.m.o.o.n.....R.e.g.u.l.a.r.....V.e.r.s.i.o.n. .1...2.....i.c.o.m.o.o.n.....0OS/2.....`cmap.V.[.....Tgasp.....p ....glyf..Q....x...phead..~.....6hhea..... ...$hmtx.H.....D...dloca.....maxp.....\... name.L.....|....post..... .....3.....@.....@...@..... .....8..... ....79.....79.....79.....2.....|.....3!2.....#!".....'.&47.6....<...}.....o..... .....F...~.....#.,.5.>.G.P.Y.b.k.t....%.0.'70.7'.0&'70..%.0..'067%.0&'70..'.0&730../.067.0..7'067.0..7'067.0..7'06..0&..70...0&'.70...0&'.70..'06'..0..'067.".1.0.....6 7>.7>.706...10..'.....P>.S...M4.C1.P.I>.L/.!&5..$"S2..4...3..2..(,,1#<.y.K?.N/..O>.M3..H,.B0,,..+...*..-..++-2#>.....4.....R[U

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\sites[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	214956
Entropy (8bit):	5.0535689910376265
Encrypted:	false
SSDEEP:	768:tEna6MVmtj++7bqoBtgmuHKBP/ksdB0UB5KUJ0GM5BUUQXE0Csoptr+pPPy7ki2B:tEnMVmtSSdBS5H5Vptr+prRG4w6xf
MD5:	9B0CEA89EFE53D91D78D11FFD47932D9
SHA1:	4923AB33295645E85508386F7B6B884BA671C25A
SHA-256:	004224D90390C7CD683C2B1911C8FF02DA3C2F1DD84DB133333F3D704ADB7355
SHA-512:	7C4A77D774D905F15BB3CBB1211849CED2F33992A77A246E20F7BC82AEA7B0CBA8AAC41C6D4F6BA67F0C38814404B227769F3BC637F6BA721598F72D6701A8D 6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn2.editmysite.com/css/sites.css?buildTime=1623246694
Preview:	@keyframes spin{0%{transform:rotate(0deg)}100%{transform:rotate(360deg)}}/*! Reflex v1.5.0 - https://github.com/leejordan/reflex */.grid{display:inline-block;display:-ms-flexbox;display:flex;*display:inline;zoom:1;-ms-flex-wrap:wrap;flex-wrap:wrap;padding:0;margin:0;position:relative;width:100%;max-width:100%;letter-spacing:-0.31em !important;*letter-spacing:normal !important;word-spacing:-0.43em !important;list-style-type:none}.grid:before,.grid:after{letter-spacing:normal;word-spacing:normal;white-space:normal;max-width:100%}.grid *:before,.grid *:after{letter-spacing:normal;word-spacing:normal;white-space:normal}.grid .grid{-ms-flex:1 1 auto;flex:1 1 auto}.grid *{box-sizing:border-box}.grid *:before,.grid *:after{box-sizing:border-box}[class*="grid__col-"]{display:inline-block;display:-ms-flexbox;display:flex;*display:inline;zoom:1;-ms-flex-direction:column;flex-direction:column;letter-spacing:normal;word-spacing:normal;white-space:normal;position:relative;width:100%;vertical-align:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\social-icons[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	13081
Entropy (8bit):	4.750606398298426
Encrypted:	false
SSDEEP:	192:MlRWcfub2DJmUDmDrW4xH3gSJJbfebOQzamKy:T3gSJJbfebOQzamKy
MD5:	903442C639C9A956E1E7882B672F3386
SHA1:	BBDE618D554E24D83ED437592B53B06D8A59A4CB
SHA-256:	6DFB5B7FC48E634B4178ECDDCE0C99548B4059D2AB965A533A28E0B94DB0699F
SHA-512:	70778EEBACB0F0262BFFD33F6B740C6765EB3D65D6C231C658016BEFDCA27575B7DDED500FB3AF61942521C918047C8EAD6E6CAB59A9AFCD5D3D3124C1F76 53
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\social-icons[1].css	
IE Cache URL:	http://https://cdn2.editmysite.com/css/social-icons.css?buildtime=1623246694
Preview:	@font-face{font-family:"wsocial";src:url(//cdn2.editmysite.com/fonts/wSocial/wsocial.eot?ts=1623245832946);src:url(//cdn2.editmysite.com/fonts/wSocial/wsocial.eot?ts=1623245832946#iefix) format("embedded-opentype"),url(//cdn2.editmysite.com/fonts/wSocial/wsocial.woff?ts=1623245832946) format("woff"),url(//cdn2.editmysite.com/fonts/wSocial/wsocial.ttf?ts=1623245832946) format("truetype"),url(//cdn2.editmysite.com/fonts/wSocial/wsocial.svg?ts=1623245832946#wsocial) format("svg");font-weight:normal;font-style:normal}.wsite-social-dribbble:before{content:"\e60c"}.wsite-com-product-social-dribbble:before{content:"\e60c"}.wsite-social-color .wsite-social-dribbble:before{content:"\e60c";color:#f077a0}.wsite-social-square .wsite-social-dribbble,.wsite-social-square.wsite-social-dribbble{background-color:#f077a0}.wsite-social-square .wsite-social-dribbble:after,.wsite-social-square.wsite-social-dribbble:after{content:"\e60c";color:#ffffff}.wsite-social-mail:before{content:"\e603"}.wsite-com-pro

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\L0xuDF4xlVMF-BfR8bXMlhJHg45mwgGEFl0_3vq_ROW-[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 15160, version 1.1
Category:	downloaded
Size (bytes):	15160
Entropy (8bit):	7.965195072524042
Encrypted:	false
SSDEEP:	384:DkyhipCPPEsQPqpfiEAAySk+Py0hdVBOVIr1cofXB2c+T8:D64nEnaeSLPfhPBX6ofXp28
MD5:	0F03F6F8FEDFDF7B895F8E633A76A511
SHA1:	3F1BDD2CB69992C6CBF901C013C80302F4F6D54E
SHA-256:	2DFC0E868CF7AE3A57FC6C7B5C87B0D5685EBF64548430AB41DE99904B01D9B6
SHA-512:	8D32F7C3BE449177008DA6920AA7443E3E68174F5F2222479032CA47A3467B342DDB6D8FBC3A849C3A94B3175C639FFFCA546C95D60F6246053AABEDD7507145
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/robotomono/v13/L0xuDF4xlVMF-BfR8bXMlhJHg45mwgGEFl0_3vq_ROW-.woff
Preview:	wOFF.....;8.....V.....GSUB...D...5...6....OS/2...|...U...`t.QtSTAT.....=...H.p..cmap.....y...68.<.gasp.....glyf.....2...L...y.head..6....6...6.5..hhea..6.....$ ...*hmtx..6....0....U.N.loca..8.....maxp..9..... ...:name..9..../....>._.post..;..... .m.eprep..;0.....h...x.c`d``.b0b0a`qq..a.J.,.aPl/J.fP.l,.cPa`a.....:...x.c`a9.8.....u..1... <.f.....A.Hy...../G.....IL.....X.X7..1..o.....x.....P.....BDD#.X."..5.....1(,.....g.....P..P/:.?....0.O...x....XY.E..9.}...m.m.m....N..3...p#.q.0uc.?>.;.M.xo.....H..=.d..=.gb. ..Zx#|.>._...O..!....o.....>JJN~..... ....hZ*..#.....t....'Pv!...$o..YI...OJxp....Tt$:....D....Q.(c..~.X.B...b.(.9P...L./....6@1=.TK.M..Fy.U.UE.t.Qge..L7..U.~-...0.Q\.....`G....]\..a...]. .4D..d..)y.W9..7..#...X..3...L6.T.L7..3.5K{s,4.|.,RXQ.,...K-..Jk.....l..f[.U.....U..f6.....x.{.`.G....n....j.Umu7...B1...b.1%..Q..B..H.$...L.....w..{..k....C.w.+V.o

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\MutationObserver[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	24573
Entropy (8bit):	4.180357727668446
Encrypted:	false
SSDEEP:	384:BRS9Bqoq/onyBpIeggNSNreqfBWddUJtTfw:BRS9BqoTnkSNakIAtTfw
MD5:	E52201E96AF18DD02C85EB627C843491
SHA1:	5BCDD1480B9BEBCDDB0D82083BDF03A7435D59A1
SHA-256:	397452D9F6A2EA6A2135B45C9E40139C68AC6661F3BAB4413E7299586CCB408A
SHA-512:	2DDEA7E1C2127A0B7A2F19764A1AC1CFD26E2D3C3189647FA3BB987FFD1107F30A9BF219D24726047FE84EE72802B515F6290CEFBA02DF1D854C70F0D3A37D8C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://offi4hf.weebly.com/files/theme/MutationObserver.js
Preview:	/*!. * Shim for MutationObserver interface. * Author: Graeme Yeates (github.com/megawac). * Repository: https://github.com/megawac/MutationObserver.js. * License: WTFPL V2, 2004 (wtfpl.net).. * Though credit and staring the repo will make me feel pretty, you can modify and redistribute as you please.. * Attempts to follow spec (http://www.w3.org/TR/dom/#mutation-observers) as closely as possible for native javascript. * See https://github.com/WebKit/webkit/blob/master/Source/WebCore/dom/MutationObserver.cpp for current webkit source c++ implementation. */../**. * prefix bugs:. - https://bugs.webkit.org/show_bug.cgi?id=85161. - https://bugzilla.mozilla.org/show_bug.cgi?id=749920. * Don't use WebKitMutationObserver as Safari (6.0.5-6.1) use a buggy implementation.*/.window.MutationObserver = window.MutationObserver || (function(undefined) {. "use strict";. /**. * @param {function(Array.<MutationRecord>, MutationObserver)} listener. * @constructor. */. function

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\S6u9w4BMUTPHh6UVSwaPHw[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 30356, version 1.1
Category:	downloaded
Size (bytes):	30356
Entropy (8bit):	7.984659107266564
Encrypted:	false
SSDEEP:	768:7wRsdJP2Pm1jtroogr9oYiCZ2dBhcb6WiMCkCB6:7wqdJu+1jtgRo9CZOBKb6JMfCB6
MD5:	C3A17DCD22924A57167BDCA954763C01
SHA1:	670A02140DCE20D2C174049489F9FE7FEC20E4F7
SHA-256:	66BDD962AD3C4A394964E44600D43808FC3377E3323E00C86213C2564AAE5651
SHA-512:	DBFC9CD39B4521FAB9CC2FE75B7C9EB9D31DAA9606571726185CBCC7D6A6A913C80F6DDAD8FC16E95C14E3578185E737E0E578DFC99794B18224CC07A23B73C
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\S6u9w4BMUTPHh6UVSwaPHw[1].woff	
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/lato/v17/S6u9w4BMUTPHh6UVSwaPHw.woff
Preview:	wOFF.....v.....@.....GPOS...l...x...X..Y.GSUB.....S...p.S..OS/2...8...Z...`zed.cmap.....Q.[cvt ...L...*.....fpgm...x.....rZr@gasp.....glyf.....]Z....]..$head..n`...6...6...Ghhea..n.....$....hmtx..n....l....0H.loca..q.....BQz.maxp..r.... ... .name..s....1....8.P.post..tP.....g.prep..vH...K...K....x.T..leQ.EW.>~Dc.m.m+....m.....{Sg....(4.;..{...1.....p.b[.u...1.%.".w\..[p..`...:.....3P....[....Z]._.g.l.Lm..%.E.....c.T..fKs..]Yh.T.v.wKW.d.]Q.j.....R..j...`..}.!7.B.|....bb1..A.....c...8'..>..[.....\X...*:&6.8.FujR.:4.!.hJ3..V...miG{:.Nt....C?.2.!.e.#..X.1...c>.X.b.....a....V.....d.{....r....O....L....(.8..Nr.3.....5.s.....y.c..g..5...W.._..?.D.I....G.....k.....`..+X.(.*.....V7zZ...w...y.....T.n..e$".-@.5M..... 1&.....".T...v.....4%.....5s8...~..6.(...nr...~.....}..<.j.D...X ^...&u...@#M4.....1..q..7*.1...L.@.C..Y.,._.....[!.dR....!U<.%..O!.L...Tt1....g..p6z1...D....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\css[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	1409
Entropy (8bit):	5.419300835391617
Encrypted:	false
SSDEEP:	24:5XSOYs2XNXSOYN72Xe3OYN75/ZY3QYsNxaY19/ZY3QYN7NxaY1X/ZOYsNxaaY/ZV:EOL2YOC2MOCjY3QLNDFY3QCNDbOLNJaV
MD5:	4B7CC2B62FE3A473AF48EE3B40BC4C5A
SHA1:	8C0C6FD93B8DFA0E5B3397936FACCCD21CB8478B
SHA-256:	E59592D5CAE8BAF1D26083E8528BE34313750F6E6A2F2944B30337F8DA4C0C0E
SHA-512:	9184A012777C58D206EE2ED2AC0B91FD4C4EFF4649D10F7D47A282D5279119C60D8E488B366A4E07907A4421EBA387FE531BAECE53B7C7D1F7B4EE83C69DE7F
Malicious:	false
Reputation:	low
Preview:	@font-face {. font-family: 'Karla';. font-style: normal;. font-weight: 400;. src: url(https://fonts.gstatic.com/s/karla/v15/qkBIXvYC6trAT55ZBi1ueQVIjQTD-JqaE0lM.woff) format('woff');.}.@font-face {. font-family: 'Karla';. font-style: normal;. font-weight: 700;. src: url(https://fonts.gstatic.com/s/karla/v15/qkBIXvYC6trAT55ZBi1ueQVIjQTDH52aE0lM.woff) format('woff');.}.@font-face {. font-family: 'Oswald';. font-style: normal;. font-weight: 700;. src: url(https://fonts.gstatic.com/s/oswald/v36/TK3_WkUHHAIjg75cFRf3bXL8LICs1xZosUZiYw.woff) format('woff');.}.@font-face {. font-family: 'Roboto Mono';. font-style: italic;. font-weight: 400;. src: url(https://fonts.gstatic.com/s/robotomono/v13/L0xoDF4xlVMF-BfR8bXMIjhOsXG-q2oeuFoqFrlnANW6Cp8.woff) format('woff');.}.@font-face {. font-family: 'Roboto Mono';. font-style: italic;. font-weight: 700;. src: url(https://fonts.gstatic.com/s/robotomono/v13/L0xoDF4xlVMF-BfR8bXMIjhOsXG-q2oeuFoqFrmAB9W6Cp8.woff) format('woff');.}.@font-f

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\css[2].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	762
Entropy (8bit):	5.410592776085871
Encrypted:	false
SSDEEP:	12:jFiwSY3Q6ZRoT6pthf6NLqFiwSY3Q6ZN76pthf6FBnqFiwSO6ZRoT6ptvnX6/Lqo:5XSY3QYsKXXSY3QYN7KsB+XSOYs2X/X2
MD5:	9202A5CB055AAECEA2C5608666B12A82
SHA1:	545D521A3D4A63D3F96E124392285D226AE4E712
SHA-256:	91BD47DF90E8B247DCB60360173C75BE1E825833B9454A6D35E5D8E6652B3C59
SHA-512:	E474B6705E984DCB36840B4F1CC92B61310FC204D3EE2DE85D66462637DC44F9E156C652C6A202F15861FC6A9B7E59AA17D37628C062FA2D9B445CA5F980714
Malicious:	false
Reputation:	low
Preview:	@font-face {. font-family: 'Karla';. font-style: italic;. font-weight: 400;. src: url(https://fonts.gstatic.com/s/karla/v15/qkBKXvYC6trAT7RQNNK2EG7SIwPWMNlCV3lGb7U.woff) format('woff');.}.@font-face {. font-family: 'Karla';. font-style: italic;. font-weight: 700;. src: url(https://fonts.gstatic.com/s/karla/v15/qkBKXvYC6trAT7RQNNK2EG7SIwPWMNmlUHlGb7U.woff) format('woff');.}.@font-face {. font-family: 'Karla';. font-style: normal;. font-weight: 400;. src: url(https://fonts.gstatic.com/s/karla/v15/qkBIXvYC6trAT55ZBi1ueQVIjQTD-JqaHUlM.woff) format('woff');.}.@font-face {. font-family: 'Karla';. font-style: normal;. font-weight: 700;. src: url(https://fonts.gstatic.com/s/karla/v15/qkBIXvYC6trAT55ZBi1ueQVIjQTDH52aHUlM.woff) format('woff');.}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\favicon-194x194[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 194 x 194, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	1611
Entropy (8bit):	7.78128494056801
Encrypted:	false
SSDEEP:	24:Zhh/FMwCalM6DPq7hHDV/QqF0uwtjptHmRO8GfZmwAqpb8VbqfEnxxM5v/lD/z:/xFMChq7hjqNvhfLrgVbqcUz
MD5:	40D716E5BAFC416DFF33E547555256B6
SHA1:	318DBEDF81A53472CF457E1E54FCBBCAFC700682
SHA-256:	CD248206934D648528B8037F28B9A4031451DF5192F30C6A911E7C7D153727D0
SHA-512:	54D762DE8C10A9E24D3E654F1C47A6287806D1BF36980A84617DBD47CA7B38EADE3BA0FC8FAE3B99DF5D33FAC86888B25F8123E1128989629AEC6B2F8FA2DA1
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\favicon-194x194[1].png	
Preview:	.PNG.....IHDR.....,?.....gAMA.....a.....sRGB.....NPLTE.....xl.....!..../.....4 .aR.M<.H;....aU.W.....IDATx.... .E.F...x.....x29.....I.~H*..W5....$...B.P(.. .B.P(...B.P..}W\.$u..C.hX.....,...,v.e.T..-gE.....WYQ!g. .8...*|.T.dH.@..#.)N.v...@.h..U@.~..".9.0..(~.f.8.....r....<.F..H..AA.#..3.B.F.....*...X_}LP.....: .....m..W .6.....k.....%.k..s.A(...9)E..&....\.....i....v$.....v.../..hUe.k9*..}~..F....,.v.vQ.A5.....l...j.....X..4...g.82!X.....b...6.3T.n..,}a..4..q...8.{0.0...*.Hs.Q.{N.0%=k..<...Ub.I..#..K .v.....@..(...!...\..~C..... .....P.*..s.....-G*I...5S.u.KRI.....`60.[.<....~.,U.a.....2O.....v...<)..5...ME{....*.....TT$a..0.z....3..CQ..4.=.2.....4..3w._...&'..I.N...f.<!..C.yBx2.b..... <nV....!u.....wB.....O..!O..;....F.;b.....E...0H.{b.4.A4>...e.\.h.{q.Y.....zd}....Y.R...4.....0.g.Z. .}.&.-.=cr?..\..3&.u\.-9...vK.oq...;R...z...w..$..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\ga[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	46274
Entropy (8bit):	5.48786904450865
Encrypted:	false
SSDEEP:	768:aqNVrKn0VGhn+K7U1r2p/Y60fyy3/g3OMZht1z1prkfw1+9NZ5VA:RHrLVGhnpIwp/Y7cnz1RkLL5m
MD5:	E9372F0EBBCF71F851E3D321EF2A8E5A
SHA1:	2C7D19D1AF7D97085C977D1B69DCB8B84483D87C
SHA-256:	1259EA99BD76596239BFD3102C679EB0A5052578DC526B0452F4D42F8BCDD45F
SHA-512:	C3A1C74AC968FC2FA366D9C25442162773DB9AF1289ADFB165FC71E7750A7E62BD22F424F241730F3C2427AFFF8A540C214B3B97219A360A231D4875E6DDEE6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.google-analytics.com/ga.js
Preview:	(function(){var E;var g=window,n=document,p=function(a){var b=g._gaUserPrefs;if(b&&b.ioo&&b.ioo()||a&&!0===g["ga-disable-"+a])return!0;try{var c=g.external;if(c &&c._gaUserPrefs&&"oo"==c._gaUserPrefs)return!0}catch(f){}a=[];b=n.cookie.split(";");c=/^\s*AMP_TOKEN=\s*(.*?)\s*$/;for(var d=0;d<b.length;d++){var e=b[d].match (c);e&&a.push(e[1])}for(b=0;b<a.length;b++)if("$OPT_OUT"==decodeURIComponent(a[b]))return!0;return!1};var q=function(a){return encodeURIComponent?enco deURIComponent(a).replace(/\(/g,"%28").replace(/\)/g,"%29"):a},r=/^(www\.)?google(\.com?)?(\.[a-z]{2})?$/,u=/(^\|\.)doubleclick\.net$/i;function Aa(a,b){switch(b){case 0:r eturn""+a;case 1:return 1*a;case 2:return!!a;case 3:return 1E3*a}return a}function Ba(a){return"function"==typeof a}function Ca(a){return void 0!=a&&-1<(a.constructor+"") .indexOf("String")}function F(a,b){return void 0==a||"-"==a&&!b||""==a}function Da(a){if(!a||""==a)return"";for(;a&&-1<" \n\r\t".indexOf(a.charAt(0));)a=a.substring(1);for(;a&&-1<" \n\r\t".i

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\homail-n2-origsign-in-options-2-1_orig[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 436 x 112, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	5045
Entropy (8bit):	7.900185156347422
Encrypted:	false
SSDEEP:	96:f1hdBkeUQQmWDuhjyopL3rRuG3654qvJY7XWpjnfW0h+rU5mK8F:NhdB9/QmBpnRM54qxY7X70VMn
MD5:	6CDAB6F5084625431853985153AAD770
SHA1:	CE7B35348B93150D740DD37D64E3935BB6344A03
SHA-256:	590F4E35C425F608A6C0E65A5DDF76D51F4677342F74CD1EBE84F1C55ED98207
SHA-512:	5C514E56576D3028AFAEA3F9C3969CB3E0D105D622CE09693C5417FC3D706E64B411684D3494BCF9191F4D3C6AC176D1D6AC476B180476F9A0F2669AA96F77A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://offi4hf.weebly.com/uploads/1/3/7/9/137998350/homail-n2-origsign-in-options-2-1_orig.png
Preview:	.PNG.....IHDR.....p.....v:.P...|IDATx.....'L.....B.@h. 4.....@h. 4....B.....B.... 4.....@h. 4....B.....@h....wf..H....ROUw.w[.-k.r..'l%y)@....k&..'.n .....h.\.r...4W.\.r...4W.\.r...4W.\.r...4W.\.r...+W.\.r...+W.\.r...+W.\.r...+W.\..?.....u.R..}l.....y.....#.2A.R.n|....o...ld..3..1.M(m.....x..U.K.}|...2.,.....4<...oD+..Y0...M.e#...9.B...{..w .&.....@....?.}...&T...z0.....)..~&..C.G....%.Q..._.=.....z~.Y..~U...eu...nj....G.a^..ny...J.....f....a..;].....1./.Cg.3....3u....<..H...I...x....Sg.4.M.~..gd.d...C.,e6q.h.....2A6E...._Z.o....i. .U..9.o>.'.Wk.`.....g.^....w..vS-?...rS=.o....q.....|..... .I.=.OF~.M...8....dBi.^.....s....:.S.....:...E..6&.5.....z..&.....u...!K.~10.1x..%O:..Q.5..... ...j._01..J..j7....Zo.....-6A.X ....#v.a.A....k...a5[...&....[..6F~..yl4F..I.=.M.....U...F...}.!zz...j#y.&....@..|~..<%o...mm.}..*.....0...=.....=.....l.....E...LD..g

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\ionicons.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	51284
Entropy (8bit):	4.573895834393703
Encrypted:	false
SSDEEP:	384:R48w+hhJhjRqFdtYRjJIjsjaHnNfc2C4741mf5HRzL:R4YhhjQFduRjJ7uHFcu7Smf5xzL
MD5:	1690997909AAE14B023A6580D4A2F33F
SHA1:	A4FD9551382A3B5C9C43E14ADB8C4C4149CD2352
SHA-256:	92AC508220F5BB60EC94E07650528EB66625F82A4740ADA068CDE05365781286
SHA-512:	617658DBE762B0F4C1A6433C90EA2FE21A0D27D431F00B2B216DE28636066FC4653A23D0B6CCCC53B9ABBD5A234E3416DCB8296B7F0DEE0CEBA1B45CE99A2 CF
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://stgdjas.simplesite.com/c/css/ionicons/ionicons.min.css

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\ionicons.min[1].css	
Preview:	@charset "UTF-8";/*!. Ionicons, v2.0.1. Created by Ben Sperry for the Ionic Framework, http://ionicons.com/. https://twitter.com/benjsperry https://twitter.com/ionicframework. MIT License: https://github.com/drifty co/ionicons.. Android-style icons originally built by Google.s. Material Design Icons: https://github.com/google/material-design-icons. used under CC BY http://creativecommons.org/licenses/by/4.0/. Modified icons to fit ionicon.s grid from original..*/@font-face{font-family:"Ionicons";src:url("../fonts/ionicons.eot?v=2.0.1");src:url("../fonts/ionicons.eot?v=2.0.1#iefix") format("embedded-opentype"),url("../fonts/ionicons.ttf?v=2.0.1") format("truetype"),url("../fonts/ionicons.woff?v=2.0.1") format("woff"),url("../fonts/ionicons.svg?v=2.0.1#Ionicons") format("svg");font-weight:normal;font-style:normal}.ion,.ionicons,.ion-alert:before,.ion-alert-circled:before,.ion-android-add:before,.ion-android-add-circle:before,.ion-android-alarm-clock:before,.ion-android-alert:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\jquery.pxuMenu[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	downloaded
Size (bytes):	3697
Entropy (8bit):	4.707743528907903
Encrypted:	false
SSDEEP:	96:r4QJODZATiN1C81vwuMymZgpqVf9oF2VdP5k6ya/e3Hgqj9DdZda1SO:XJ6ZATiq81vDtNh8dP5k6yAeXgqj9B7Y
MD5:	AC373D716AFE4270DF40F60417B0F418
SHA1:	ABA148148C771BB66B0B4AEAB6EAC8EB40352745
SHA-256:	F75570C56743E8C705CB06F5F1F9B1F8F2CC13119F5E2ACDA2F3BB8D987DE94A
SHA-512:	3FAF2FE9C98144F41A3AB614E23E1D488AAEB2C944A3C736C196C69175C96E4D78D2FD69C0B05A5DDCAAB819C0FCA2BE40DC2C178257E2D0AFA2523072CDA85
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://offi4hf.weebly.com/files/theme/jquery.pxuMenu.js?1574700255
Preview:	/*==========.= Weebly Horizontal Site Menu =.==========*/..(function($) {.. /**. *. * Generate a flexible responsive menu from the default navigation templates. *. * Groups overflowing nav items into a "more" menu item. *. */.. var Menu = function(menu, settings) {. this.$menu = $(menu);. this.settings = settings;. this.$more = $('\. <li class="menu-more has-submenu ' + settings.parentClass + '"> \. ' + settings.moreLinkHtml + ' \. \. <ul class="' + settings.listClass + '" data-menu-more /> \. \. ');.. this.init();. };.. /**. *. * Initialize the menu on load and on resize. *. */.. Menu.prototype.init = function() {. var self = this;.. $('body').addClass("mor

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\main_style[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	assembler source, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	45877
Entropy (8bit):	4.957624688727777
Encrypted:	false
SSDEEP:	768:lCBrzt/swgxyG5abmDm13JK657agZ1JezZXCQgAGCiTPFE/D:lCBrzt/sjhEmDqJV7agZ1JQCQgAGCiTa
MD5:	BFD333770DC1CE5D99E8C6119477A1F9
SHA1:	D4A215779900C8B58A21EA627596F8CCD1BD6822
SHA-256:	9E18DD92F5BB8097C1DD380866C737B737AF6904977D585C36C29B92B9666A20
SHA-512:	777AC15D8592FB30B17BF8A74793D7250B02C0C87D8A537BEDBD9B822C6FB6D8E8488BD63B0C660121240AA45385332C0B75AA55CE52E79B5A1CFC655216192
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://offi4hf.weebly.com/files/main_style.css?1623367237
Preview:	ul, ol, li, h1, h2, h3, h4, h5, h6, pre, form, body, html, div.paragraph, blockquote, fieldset, input { margin: 0; padding: 0; }.ul, ol, li, h1, h2, h3, h4, h5, h6, pre, form, body, html, p, blockquote, fieldset, input { margin: 0; padding: 0; }. input[type="text"], input[type="email"], textarea { -webkit-box-shadow: none; -moz-box-shadow: none; box-shadow: none; -webkit-appearance: none; -moz-appearance: none; appearance: none; text-shadow: none; }. input[type="text"]:focus, input[type="email"]:focus, textarea:focus { border: 1px solid #777777; }. textarea { resize: none; }. select { -webkit-appearance: none; -moz-appearance: none; appearance: none; text-indent: 0.01px; text-overflow: ''; }. .wsite-form-field input[type="radio"], .wsite-form-field input[type="checkbox"], .wsite-form-field #wsite-search-sidebar .wsite-search-facet-availability input[type=checkbox], .wsite-form-field #wsite-search-sidebar .wsite-search-facet-checkbox input[type=checkbox], .wsite-com-product-option-group

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\plugins[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	67465
Entropy (8bit):	4.809594108927749
Encrypted:	false
SSDEEP:	1536:59rPpU1wHKYTpQ73CHJHDuYL/OHHeZF+YwLMC0ht/uJFO0815wZDk5/2M:59rPpl1NQ73CHJHDuYL/OHHeZF+pLM75
MD5:	2B8D85F1EA01D2C3E8B962EAC8D76A5C
SHA1:	936987A7E08DAA4A916C77D86937EDEE42D657DA
SHA-256:	B6353CA52760ABA4E7547AE9861DB68158DC2AF0F4FEBECE55E5C775EE4449F5
SHA-512:	F64D0E9FC7ED02F4C7B3CF7FD680DF3A6F8F4CEFADEEA63553D0F0A4BB5472ABF5EE754C0E056CD91272F0108910347BA6F3CF23C825FD89260CF0545DD070A
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\plugins[1].js	
IE Cache URL:	http://https://offi4hf.weebly.com/files/theme/plugins.js?1574700255
Preview:	./*! Hammer.JS - v2.0.4 - 2014-09-28. * http://hammerjs.github.io/. *. * Copyright (c) 2014 Jorik Tangelder;. * Licensed under the MIT license */.(function(window, document, exportName, undefined) {. 'use strict';..var VENDOR_PREFIXES = ['', 'webkit', 'moz', 'MS', 'ms', 'o'];..var TEST_ELEMENT = document.createElement('div');..var TYPE_FUNCTION = 'function';..var round = Math.round;.var abs = Math.abs;.var now = Date.now;../**. * set a timeout with a given scope. * @param {Function} fn. * @param {Number} timeout. * @param {Object} context. * @returns {number}. */.function setTimeoutContext(fn, timeout, context) {. return setTimeout(bindFn(fn, context), timeout);.}../**. * if the argument is an array, we want to execute the fn on each entry. * if it aint an array we don't want to do a thing.. * this is used by all the methods that accept a single and array argument.. * @param {*|Array} arg. * @param {String} fn. * @param {Object} [context]. * @returns {Boolean}. */.function invokeArr

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\qkBIXvYC6trAT55ZBi1ueQVIjQTD-JqaE0lM[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 14260, version 1.1
Category:	downloaded
Size (bytes):	14260
Entropy (8bit):	7.966217847401131
Encrypted:	false
SSDEEP:	384:H3P28k2W4TMcRXu2kE5+6mihFraeQMGS+JCVgyS:XP2Mzu2F+6mihFunZSrvS
MD5:	6EE84F63EF54DC2F82EAC18A81E18503
SHA1:	D2FE4F772BE85D76D50A4B6308FB2660879EC215
SHA-256:	1803E8587D79FB3755BE85803B10D2A642B67E7F547E75654B919F598AEC9461
SHA-512:	2F5BB2E91A8C0C61300BFD77CAD2ED6EC812CA524ED332CB8B8FC0E892D73DE37F1554B10FD63166F7982BA097B87E2548CFE48CE8154BB4B986AAE3C1B0D82
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/karla/v15/qkBIXvYC6trAT55ZBi1ueQVIjQTD-JqaE0lM.woff
Preview:	wOFF.....7.....U.....GDEF...l.....GPOS.....d....N.'.GSUB...\.....J.2 OS/2.....Y...`tE%xSTAT...\...=...L....cmap.....r.....gasp.....glyf.....)5..@. .7..head..1P...6...6.=.zhhea..1.... ...$....hmtx..1.....X4.v.loca..4P.....maxp..6l..... .(..name..6....."3[U.post..7..... ...2prep..7.....h...x.-.....!.....FWH.A.....T.Q.B ..P. .`.{...=D..'.IP.:....v..N.....dm7l.=p.g'.N\..q..'J.T.x.F\|..:..ok'%JlO9.K.S ....A.j... .C.....x.}...\Q.E.}..3...Om..j..m....j{..v.",...+.....9.\.I.....f-ZuR...F(Y...n...3B.x6.....D..F.tDa..{} .W.T.c...id.^f..e..m.9g.....qF93.y..g..6.(.KD79.Id.....P.2.,....\|Y*...\|9....U-.V...PS.m...).s/...A.d....^.h..(.'.MtH.J...^W:..I.[....0.\|..G.....g...trA.C.....#<.h.;.(...ak..N..v.. .Ag.$..y....yP.D. .....g.~.:..}D.m.....H2..Mc7.A./.=..s.N.n..C..~2Aj0e5.....x..?.\.6..es.6.....q.....zh.....t.....:D..E....p.S..U....h....J.zx./.,.. ..\l..|..m."b.....l.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\qkBIXvYC6trAT55ZBi1ueQVIjQTDH52aE0lM[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 14336, version 1.1
Category:	downloaded
Size (bytes):	14336
Entropy (8bit):	7.967095491114002
Encrypted:	false
SSDEEP:	384:E9L+8kuMz0xjYCayC+lJdjaOSMfdSiypqnABNIfTHG:4aAMcayllJFaNcZKqnABN8G
MD5:	B2CD4A140A2B39890DC726B9F96E4DE1
SHA1:	D0C6ACC7E507FDA049AE4A4FA7EF1E65C36AB94D
SHA-256:	78A5EB7E60B53AE1A8D9627BA251E8A8E281CC2ED955153A59A87CF7AC181C48
SHA-512:	8788A7C54F43B877864F5F7364FECA041807A76A007F2DC0555795FFDA7A6491EAC87ECCDAE801A4B6EB0E55B9EE9E6F8523C849F640CFA8D483EEC49E5E738
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/karla/v15/qkBIXvYC6trAT55ZBi1ueQVIjQTDH52aE0lM.woff
Preview:	wOFF.....8.....U.....GDEF...l.....GPOS.....o....N ".GSUB...h.....J.2 OS/2.....X...`uq%XSTAT...d...>...L.Q. cmap.....r.....gasp.....glyf... ..)...@. .chead..1....6...6.>.zhhea..1.... ...$....hmtx..1.....Xl.j.loca..4.....maxp..6..... .(..name..6.....0]R.post..7..... ...2prep..7.....h...x.-.!....D.w?..c...G.W{/.&F..{...*X..f va...mbgu...C..p.....};`hG...1...v..n....{r....+7{w.tA..o....?..vR....#..9."(.....R<.....x.}....a...?....g..m.m...7..M..A..A._.....sq.dd$.([e..k.."...7B..K^.....ID..!2.....5.c..^...xL..6.L-.. .2S.,...2...s.<6..N.g.3..,qV9/....._.(Jy..X.P.r...<.*...<.*..JR%UV.....QS..PU.K._5...!s..."...!..G.D.....V>.\1.T.Z...J.....ly.*..+#/l..o...l,.}.{.....U4..GPt.L....w.o.....T.I.1..do...L~..*? 3.P;C...w.....G.G..~.. .Iy...\r.A.@.....d.....$/^..3..*3....%...S.|..H.....Dl2H'.Am&.Y.. .\.7T...Q...6....m%.a."6n.j.....9....2.E...H1h....hi".....H>...Rl..Z....;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\qkBKXvYC6trAT7RQNNK2EG7SIwPWMNlCV3lGb7U[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 17380, version 1.1
Category:	downloaded
Size (bytes):	17380
Entropy (8bit):	7.967431465079427
Encrypted:	false
SSDEEP:	384:ULlgsw6kfhCXlGWcTFao44zXaDwnDhKcQ0svQi/alWPCWa+M06MJh:Spsw6IYlmTFaNc6uDhK8svQuaX6boJh
MD5:	47242894FDCE6238F8C9A86F1253BF8E
SHA1:	EB47032AF64B6735C115B6CEC9D296EA650BBFE9
SHA-256:	2B0C28A0FA7CD0B83ACEB02E12D8607BF045C4B06D734C06BC0D4F5F1B215540
SHA-512:	B0D662E820E04772644D44230F8A6BCFCD0313EA2C60CD00ACEA93FD700FB2909A9FC76A743ECF70AD7F146D568A0CF347942C05981645726F1D246C31551FB
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\qkBKXvYC6trAT7RQNNK2EG7SIwPWMNlCV3lGb7U[1].woff	
IE Cache URL:	http://https://fonts.gstatic.com/s/karla/v15/qkBKXvYC6trAT7RQNNK2EG7SIwPWMNlCV3lGb7U.woff
Preview:	wOFF.....C.....hX.....GDEF...l.....#.&6GPOS...$...q.....h.QGSUB.....-OS/2.....]...`tPE?STAT.....=...H....cmap...T...}.....gasp.....glyf.....2...N.. .E^head..;....6...6....hhea..<$...#...$.+.jhmtx..<H...g...8...ploca..?.....[.lmaxp..B..... ....name..B...../3Ospost..C..... ...2prep..C.....h...x...1.A.....y.ldT."..dOY....d6.-.. (.>.nP2l.....~.. .R.....#A..o...]..k6v...9.#g{.joN.y.'/.v...O E..I%..*..e.....-.I+..j...m.e...zv...hbgZ .... .o.....J...>..c....!....x.}....A....}....}....5..m.EP...v..oXn.l.5..?s...Y.I1..z*.M.nJ.? u.....;a.R.&I.Sf..q..%..5.f.....Vh...n.B.j<.d.L..1.L...L23."...0..M..c>{..A..o.7.[.=/.V.].....IIJV..*M..PP.*...|....Z..l6..<5T.....jb7...s.R.K.V...k..}..E(.....U*1.5H.....2G..!N....>f..3.h. "U{I.r.!.9Gs.....,s.Md..~+`3`.`~.V..P.....F...7e.....R..xE].....D9.rCM....;>R.....P.|....%@.>.....+.J.,..D.sg.1....rc.....P...qC.)!5...8y..=l....aC.5rn.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\rowsconcept[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	49158
Entropy (8bit):	4.8202186427726375
Encrypted:	false
SSDEEP:	1536:y+5581lgrD8zvK508nfWgLqQHMtbv/cC8nINcuyE1J8vRY:Z8r8d808YJ8u
MD5:	745B54070C7A541F8D0B4DB8E266B663
SHA1:	70796DA230AD216BDDFE472F9CBBE721DB0C241C
SHA-256:	3CE414BDADD954365590DDBE52057E0B465B89FB5E0ECAF6E7C7B12997480308
SHA-512:	BAC3CBED2C6C18580C7A1E99DD0F53335F6825FA02F655AB8198477DD20D55EAE38A1575F75ED64A58CF45F6D48508F86BE47DF15ADD98377B4C2EF32FE6829
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://stgdjas.simplesite.com/d/designs/base/rowsconcept.css
Preview:	@media screen and (max-width: 724px) {. body.stefan-asafti .content-wrapper .layout5-row .span4 .first .section,. body.stefan-asafti .content-wrapper .layout5-row .span6 .first .section,. body.stefan-asafti .content-wrapper .layout5-row .span12 .first .section {. padding-top: 10px;. padding-left: 10px;. }. body.stefan-asafti .content-wrapper .layout5-row .span4 .last .section,. body.stefan-asafti .content-wrapper .layout5-row .span6 .last .section,. body.stefan-asafti .content-wrapper .layout5-row .span12 .last .section {. padding-bottom: 10px;. }. body.stefan-asafti .content-wrapper .layout5-row .span4 .section,. body.stefan-asafti .content-wrapper .layout5-row .span6 .section,. body.stefan-asafti .content-wrapper .layout5-row .span12 .section {. padding: unset;. padding-left: 10px;. padding-right: 10px;. padding-top: 10px;. padding-bottom: 10px;. }. body.stefan-asafti .content-wrapper .layout5-row.signature-image {. overflow: hidden;. width:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\somelinks[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	5712
Entropy (8bit):	4.840227092465098
Encrypted:	false
SSDEEP:	96:t9eNCYm70zC4CCzdCOq5Ic65Nbkem6TN26keylyBv:t9eQRQuPtvqc65OLaKpav
MD5:	4DDDA98C50B7F5652B1C4E743C01F343
SHA1:	703BB5309B261ECF0D9BD0AB8789B1597F41C9D7
SHA-256:	A84CD15387E15DF55B5B1FA3B6361DEFE0DA90629C3283852D27D4C8D0F576CA
SHA-512:	61EF511BEF03D040EF129739A2DA3A94F40F9C0BE33F89A298060987176995EE7A86F991124950DFF4FCA55D85D6A1A492A6D0892C41D89D63A282A065C417F0
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://stgdjas.simplesite.com/d/designs/base/somelinks.css
Preview:	.social-media-links {. display: flex;.}..social-media-links.display-contact-information .phone-email {. width: 50%;. padding: 7px 0px;. padding-left: 2em;.}..social-media-links.display-contact-information .header-icons {. width: 50%;.}..social-media-links .header-icons {. display: flex;. align-items: center;. justify-content: flex-end;. padding: 7px 0px;. width: 100%;.}..social-media-links .header-icons:not(:last-child) {. padding-right: 20px;.}..social-media-links .social-media-decoration {. text-decoration: none !important;.}.@media screen and (min-width: 724px) {. .social-media-links .social-media-links-container {. justify-content: left !important;. }.}..social-media-links .social-media-links-container {. display: flex;. align-items: center;. justify-content: center;.}..social-media-links .social-media-icon-header {. display: flex;. align-items: center;. justify-content: center;. width: 14px;. height: 14px;. font-size: 14px;. border-radius: 60px;. paddin

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\soundmanager2_flash9[1].swf	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Macromedia Flash data (compressed), version 14
Category:	downloaded
Size (bytes):	8678
Entropy (8bit):	7.976931613613915
Encrypted:	false
SSDEEP:	192:ZOV8hcu5qfh75a4zhNUUyCYYmDmbeXZliR0DKBCt4SbJ9J7:w8hcuwps4QUyvYm+ejiR0+B09bD5
MD5:	D90C2E7B025FEB999EFD3A72BB837361
SHA1:	538C3038A8C697E7B1C8CB20775BDDCE52F4FE1A
SHA-256:	6CC64D582CEEB1087AA0E1295003DA6D26447328369935D136A7921937360C26
SHA-512:	4949599B52C8E6121BCB02C60271B41C9590F08AE0B6105F7C4655595ED85686A8DC967E8C3D19EF89E8384F7B8CD13F748759F00BE7C7B84D249C104D48C542
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\soundmanager2_flash9[1].swf	
IE Cache URL:	http://https://stgdjas.simplesite.com/Images/sm297/soundmanager2_flash9.swf
Preview:	CWS..>..x.{yx\G.xW...fF3..-.R...E...$.l.c[.....'Q.73.i.C.!.....\..p.B.(qH.$$@ ....v.F...,.....B`/...Cr...??}.~}TWWUWWU.$'..S...2..X..J.....4.....fr.-..3U*Mn..>~.x..M]..D. ..7w..v..n@.....~bC.xy.VI..(&...R:..P[....;...D..d...$..n#cd.\...k#.J&...BV/m."3.N.Ol(..c..)c.....4...e...'.D..f..... .d...C.\...K.B..IH.L$#.6N ...x&]L...#y.t\/...r.Y_..H.....Z.....>....>al. .+.jm.^2...OF6.F#.=.7.Q.....ne.._..g}|~~....w\EP....._....h.....G....#...K_u=c8...56...bn..H.K.)S.tR.)....#...zN.[..._.Q.1E.....G..6....G.D)<b$.t..@../.9.].z...2...p..k.FJz.\....h.. ..&..d.8..O.#...!..B.u.<...Z..T.s..^..?...".A...n.....H.z:7.(.Ewz`}(....|.T.g2..b..~{..V.#E..BA?i...E..l.....^8....F.}...$R..rz<c$.l#^.6.....5..F...[@e..h..n..t.....".W.J..`..$.6....T;..H.d...> y.....K..'..d|..<.*..%=....+....R~...8m..o.CZF!.gv..k...Q,5..f.....X..n.c_!?Q...G.A..IvU[.|....v.....(.Q.....Q2.....z...O..s....j..Id..?)[.b)?.b..J..^..BR.s

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\L0xuDF4xlVMF-BfR8bXMlhJHg45mwgGEFl0_Of2_ROW-[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 15236, version 1.1
Category:	downloaded
Size (bytes):	15236
Entropy (8bit):	7.969203300169163
Encrypted:	false
SSDEEP:	384:LRpyXzNKZkpfrUcPlG9rmucpNaYVSzKQKwb:VADNnpfrtkpuQKwb
MD5:	9D793A8D492EE02DF891E473D9267325
SHA1:	90F7C3665DAD15564CBB01EF5B31BB909EE517CA
SHA-256:	8545FDDD567039B81C7224949B5D930212762BF7B93124EB86905D6F8B5299A2
SHA-512:	58EBE21FEE685D6A580AA2F233776D2A92CE726595DD76E575ACC1A327EE30CB493A2CCEEB307F0CA4B2C18AD0F66C203CE527376BD44D58FA0898B2D68D8 28
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/robotomono/v13/L0xuDF4xlVMF-BfR8bXMlhJHg45mwgGEFl0_Of2_ROW-.woff
Preview:	wOFF.....;.....V.....GSUB...D...5...6....OS/2...|...S...`u.QTSTAT.....9...D...,cmap.....y...68.<.gasp.....glyf.....3K..L..$..head..6....6...6.6..hhea..7.....$ ...*hmtx..74...0....LCF.loca..8d.....4maxp..:..... ...:name..:8...,...l;.\8post..;d..... .m.eprep..:|.....h...x.c`d``.b0b0a`qq..a.J.,.aPl/J.fP.I,.cPa`a.....:...x.c`a9.....u..1...< .f.....A.Hy.....d.....*..G.....|.F...+..`u..{....x.....@...y...FG.b...K..p.`DL.....;..5..z1.....x....XY.E..9.}...m.m.m....N..3...p#.q.0uc.?>.;.M.xo.....H..=.d..=.gb...Zx#| .>._...O..!....o.....>JUN~..... ....hZ*..#.....t....'Pv!...$o..YI...OJxp....Tt$:....D....Q.(c..~.X.B...b.(.9P...L./....6@1=.TK.M..Fy.U.UE.t.Qge..L7..U.~-...0.Q\....`G....]\..a...]...4D..d ..)y.W9..7..#...X..3...L6.T.L7..3.5K{s,4.|.,RXQ.,...K-..Jk.....l..f[.U.....U..f6.....x.Z.x.W...I.1.F3..4b4.-...l..9M.&e.fSn.)37ef.6....r...]...X.wFv.9i.n:.*.p.....\.0.Q .}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\TK3_WkUHHAIjg75cFRf3bXL8LICs1xZosUZiYw[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 20140, version 1.1
Category:	downloaded
Size (bytes):	20140
Entropy (8bit):	7.968457390339718
Encrypted:	false
SSDEEP:	384:lT1BUIZSm/F1njJCyS32+PJt/HxrT/1O1eSe7RRJXmL5dBPjSoYaG7dv:lT1+IZDjJCBPr/HVdO1gRRM9FYaov
MD5:	C8EE6FE62C4BA1B3F6CB790030A7A04A
SHA1:	FD714B4271D326C46076FAF4D2D6EDB9423A5CCD
SHA-256:	84E0AF767E6764A06CE933086F62A8A2C6CE7BBC994868720E46E6570D6F71D1
SHA-512:	8A8811EEE65C7A81B411BA27E9CFC9422CA6E9E4CC201D528CF36B7D61C6C7662E7DD98B7CAE2717580F81FF145E2720C2E95CD95365DDE7117B4259F198C8 2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/oswald/v36/TK3_WkUHHAIjg75cFRf3bXL8LICs1xZosUZiYw.woff
Preview:	wOFF.....N.....@.....GDEF.....E...^...nGPOS.....5.....b..GSUB.....rOS/2.....O...`._>.STAT...h...&...*y.kIcmap.....n..@.cvt ...4...E.....Yfpgm...|..... 6..gasp...@.....glyf...H..8...c*...head..HX...6...6....hhea..H.....$....hmtx..H....%.....loca..J.....maxp..L.... ... .<.;name..L.....*1OO@post..M..... ...2prep..N.....<l .x.....@P..._...k@....z0.U.$8...h0|...I..R...I_..K.....N...r.,..k...x....l9...$.{<.m[c.m.Q^.....]x~c.d.J...9.}..In..=....+..Wr...:.s..H4..9....Q.x.D.J..h.....R3.MC....G....Y....;.^x.n.5....._T. Qn.[mkl.c.mr.MvE.....$w.{.}.>w.....5D..Q\V.d.")MY..._.....9F..GS.`M.L..|-..-U..*_....t2.S.J....J.....u(G7.V...T..P.b.'....<.g..z...`.l...._....&.....6.....W9M.Yq.....E.....N.x./ ..."..ea.^.9XN.....,8. .qH.t_.....$...1<..q0.&.D...a...MZ.....X..`5..ud.....P.EP...9..h8.....x8.N.S.4...u...j.f....t...0...8..`"L..0.f..pF.g4..0.^.w...>.4..)G.*....q.....y

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\api[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	852
Entropy (8bit):	5.5030292156198515
Encrypted:	false
SSDEEP:	24:2jkm94/zKPccAjZy+KVCetg1AnDsLqo40RWUnYN:VKEcixKoee1AnILrwUnG
MD5:	463E88C8F565526A5AB7826B0714B197
SHA1:	632317C20898D7FF1F5C2BA95C684617E0A293AC
SHA-256:	FF3ED906D85A8C901B27C9D6EDE2E00DE6CEC8C395FE4EB9B3B2E3D56C7D8755
SHA-512:	4AC53AA72F4807596C37E2D82CC5A648CE2CAEC9E3BE8BED5E2E991DC4B0F3120A44A5465677A7EF8CCE7F2E56CF032373103F1C3F815068583B620B061FB91 7
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\api[1].js	
IE Cache URL:	http://https://www.google.com/recaptcha/api.js?render=explicit&hl=en
Preview:	/* PLEASE DO NOT COPY AND PASTE THIS CODE. */(function(){var w=window,C='___grecaptcha_cfg',cfg=w[C]=w[C]||{},N='grecaptcha';var gr=w[N]=w[N]||{};gr.ready=gr.ready||function(f){(cfg['fns']=cfg['fns']||[]).push(f);};w['__recaptcha_api']='https://www.google.com/recaptcha/api2/';(cfg['render']=cfg['render']||[]).push('explicit');w['__google_recaptcha_client']=true;var d=document,po=d.createElement('script');po.type='text/javascript';po.async=true;po.src='https://www.gstatic.com/recaptcha/releases/6OAif-f8nYV0qSFmq-D6Qssr/recaptcha__en.js';po.crossOrigin='anonymous';po.integrity='sha384-f1gfYQgq4OmhARgCSe1q7WV7tIcPpqu0qD+jYdSEMczD1YXPg0ibdIzvD/fZzwKc';var e=d.querySelector('script[nonce]'),n=e&&(e['nonce']||e.getAttribute('nonce'));if(n){po.setAttribute('nonce',n);}var s=d.getElementsByTagName('script')[0];s.parentNode.insertBefore(po, s);})();

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\api[2].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	850
Entropy (8bit):	5.5017545950531765
Encrypted:	false
SSDEEP:	24:2jkm94/zKPccAv+KVCetg1AnDsLqo40RWUnYN:VKEctKoee1AnILrwUnG
MD5:	65B6FEB732C65BEE99FD396A3E99F27F
SHA1:	8F719875F058EEE21257BC1CBCA2A6BA1A7B9A21
SHA-256:	9B7EA780F5FF5CD8A0AD4A2700143F3661284DC98D571CB38B188C2C060FE55A
SHA-512:	433CF4B099A6CFD3D98F128F86EA8C2EAACA852A38777683C7AD14953B3A4782C54985A87F5A2FCCA67CF3C2C83159EE2BBE71713338A11274D0516E4C5B8E(
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.google.com/recaptcha/api.js?_=1623417226032
Preview:	/* PLEASE DO NOT COPY AND PASTE THIS CODE. */(function(){var w=window,C='___grecaptcha_cfg',cfg=w[C]=w[C]||{},N='grecaptcha';var gr=w[N]=w[N]||{};gr.ready=gr.ready||function(f){(cfg['fns']=cfg['fns']||[]).push(f);};w['__recaptcha_api']='https://www.google.com/recaptcha/api2/';(cfg['render']=cfg['render']||[]).push('onload');w['__google_recaptcha_client']=true;var d=document,po=d.createElement('script');po.type='text/javascript';po.async=true;po.src='https://www.gstatic.com/recaptcha/releases/6OAif-f8nYV0qSFmq-D6Qssr/recaptcha__en.js';po.crossOrigin='anonymous';po.integrity='sha384-f1gfYQgq4OmhARgCSe1q7WV7tIcPpqu0qD+jYdSEMczD1YXPg0ibdIzvD/fZzwKc';var e=d.querySelector('script[nonce]'),n=e&&(e['nonce']||e.getAttribute('nonce'));if(n){po.setAttribute('nonce',n);}var s=d.getElementsByTagName('script')[0];s.parentNode.insertBefore(po, s);})();

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\base[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	downloaded
Size (bytes):	40551
Entropy (8bit):	4.781087741748243
Encrypted:	false
SSDEEP:	384:O4aRl9iytUhtqYNqDm0F2xpJKUIZ3xRBiTj77QNIvvVN9:Oj9NMTMNcv
MD5:	446645161AB81E489803EF51902BC6C8
SHA1:	7FB2BCE14ACF3D5CEFB28B88E8BCE0A2C6B634A1
SHA-256:	72801F0FD32E26C39B05AB19A4C3C7A19FC0380702BD8B4DBCE6987C4E6FBB7B
SHA-512:	A3E86FD95F29FA82CE95DB741A9AA60FD0F622080569043F1BB99686E7BBCFD0BF80793E9E0B6631F427C9B2C182130C1A8971B80FD9B6E632F39FD34F6B5AF4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://css.simplesite.com/d/1622630893/designs/base/base.css
Preview:	./* Hero Section Start */...hero-section {. height: auto;. margin: 0 auto;.}...hero-section .hero-content {. min-height: 440px;. width: 100%;. display: flex;. position: relative;. justify-content: center;. flex-direction: column;. text-shadow: 1px 2px 8px rgb(0 0 0 / 40%); /* Same shadow as in EditorV5 */.}..@media (max-width: 600px) { /* XS as in editor V5 */. .hero-section .hero-content {. padding: 15px 15px 15px 15px;. }.}...hero-section .hero-content-inner {. z-index: 3;. padding-top: 70px;. padding-bottom: 70px;. padding-left: 45px;. padding-right: 45px;.}...@media (max-width: 600px) { /* XS as in editor V5 */. .hero-section .hero-content-inner {. padding: 0;. }.}...hero-section .hero-content-inner h2 {. font-size: 36px;. line-height: 42px;. letter-spacing: 0.5px;. padding-top: 28px;. padding-bottom: 4px;. color: white;. text-shadow: 1px 2px 8px rgb(0 0 0 / 40%); /* Same shadow as in EditorV

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\css[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	368
Entropy (8bit):	5.131961962605393
Encrypted:	false
SSDEEP:	6:0IFFN+56ZN7izlpdgmJk2SpJNijFFBPLQ+56ZRWHTizlpdTczfr1nNin:jF3O6ZN76paKeqF70O6ZRoT6p2zRY
MD5:	95821BA6370D527B91BB2DCFAD42C0D0
SHA1:	AF76A7EAFC5077992D3177012F51EE270DEA7E34
SHA-256:	E45B4BC394D249BC29B0F06334CBDE3B4885C29302E1E37395215569937E580D
SHA-512:	1D6D9C7DF45C94A950BE470C0A443D25F8809BDED3092998193EA73C758A1108732F0680C335C24DEC9F20162B2A7E2D98DD9B89326DD884421DAA2B089C2A1
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\css[1].css	
Preview:	@font-face {. font-family: 'Lato';. font-style: normal;. font-weight: 700;. src: url(https://fonts.gstatic.com/s/lato/v17/S6u9w4BMUTPHh6UVSwaPHw.woff) format('woff'); .}.@font-face {. font-family: 'Merriweather';. font-style: normal;. font-weight: 400;. src: url(https://fonts.gstatic.com/s/merriweather/v22/u-440qyriQwlOrhSvowK_l5-c iZK.woff) format('woff');.}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\custom-1[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	15720
Entropy (8bit):	4.667585237746499
Encrypted:	false
SSDEEP:	384:W+1SbYbddF3bbO0ELZZRZpqOhPvF6b1yX:W+1SbYbddFLilTZpqOVF6b1M
MD5:	BEB222C03C3FDD6AF710530B7DF1C408
SHA1:	890E1225290F49994B8EDC37FF7B4676DDC7B75C
SHA-256:	6FCEDA9DF3549C1857609BCA8BB9BD132AAEF3EC76ADEB82B0A62C698CAE0011
SHA-512:	23B5EF01E5AF2E30F36ACA9D4251FBBF9E9EE3B02A57429569817D586666BF13CDD536CDA1B8F2F113FA80477B2D09009C01DCF41A693D163096A8328F02455D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://offi4hf.weebly.com/files/theme/custom-1.js?1574700255
Preview:	jQuery(function($) {.. // Mobile sidebars. $.fn.expandableSidebar = function(expandedClass) {. var $me = this;.. $me.on('click', function() {. if(!$me.hasCla ss(expandedClass)) {. $me.addClass(expandedClass);. } else {. $me.removeClass(expandedClass);. }. });.. }.. // Interval loop. $.fn.intervalLoop = funct ion(condition, action, duration, limit) {. var counter = 0;. var looper = setInterval(function(){. if (counter >= limit || $.fn.checkIfElementExists(condition)) {. clearInt erval(looper);. } else {. action();. counter++;. }. }, duration);.. if (!condition) action();.. }.. // Check if element exists. $.fn.checkIfElementExists = fu nction(selector) {. return $(selector).length;.. }.. $.fn.hideDropdowns = function(dropdownClass) {. this. .removeClass(dropdownClass). .find('.wsite-menu-wrap'). .revealer('hide'). .find('.' + dropdownClass). .removeClass(dropdownClass);

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\fa-regular-400[1].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), Font Awesome 5 Free Regular family
Category:	downloaded
Size (bytes):	34388
Entropy (8bit):	6.3192978450446855
Encrypted:	false
SSDEEP:	384:b/ILltPRwpXUazLuDULbN1TH/uOlrk4jx3l+89AyI6WcRwk9cQUm:bALDPXy6DO7/uOtx29uc59cQUm
MD5:	859001F6AE8EB0BB3878AAA971B50FC6
SHA1:	BFE858743BEA5FD2C7AFCE109CDB02B48B39928E
SHA-256:	939CA0E66E9E1C2966AFAA7CCFA5EA2D8294043CD32424ED84A3BFB22D3B0071
SHA-512:	A73B8D47959C1782BB2E7AD49AB1543D70B77F850B0059B9EC588348AA523FA4604D5D261A4E7059CA4E2BA30D6A1313060AF50D80448DB29E69D156C3C8C81
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://stgdjas.simplesite.com/webfonts/fa-regular-400.eot?
Preview:	T...,.....LP.....xR6.....6.F.o.n.t. .A.w.e.s.o.m.e. .5. .F.r.e.e. .R.e.g.u.l.a.r.....R.e.g.u.l.a.r...J.3.2.9...7.3.0. .(.F.o.n.t. .A.w.e.s.o.m.e. .v.e.r. s.i.o.n.:. .5...8...2.)...6.F.o.n.t. .A.w.e.s.o.m.e. .5. .F.r.e.e. .R.e.g.u.l.a.r.....PFFTM.N.6.....GDEF.*.....OS/2A.....X...`cmap.....gasp.....glyfl..... ..n.head... ).....6hhea.5.....$hmtx...t.....Tloca.E.....6maxp.....8... name,41...w....Upost.OA...}<.....I..6Rx._.<.....c.....c..... .@.....L.f...G.L.f.....PfEd.....T.....:.... .....@.....@.....@.....@.....@...@.....@...@..... .....`.....@.....@.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\fa-solid-900[1].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), Font Awesome 5 Free Solid family
Category:	downloaded
Size (bytes):	186708
Entropy (8bit):	6.356083890637828
Encrypted:	false
SSDEEP:	3072:hCNGM3n0ubr9ejZ5hLL1CdvPXiazQYY0UhWVNaKL/gjrLhFlxwP+SiehAMedj:ENGM3n04BGh9CxXiMQP0UhW3ejfhFHwK
MD5:	E2675A616B68F446FA6284C111554C7F
SHA1:	E256DFF855F792E365F35B3A37877BF9E8FDC98E
SHA-256:	E055D9C84DCB6AB8684F27E7AC6B48082B626B7C53639502FD05BF45CD43AFE3
SHA-512:	B4D670498384CF9D000B3D7840E005025280D0A373C4F0E01A1029B4779B0EE7DE8F01A3D423CE5093D7AFF8CD1F42A4E901EA22D5A6DCDF0DC3A112128CCB 2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://stgdjas.simplesite.com/webfonts/fa-solid-900.eot?

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\fa-solid-900[1].eot	
Preview:	T...8.....LP.....d.....2.F.o.n.t. .A.w.e.s.o.m.e. .5. .F.r.e.e. .S.o.l.i.d.....S.o.l.i.d...J.3.2.9...7.3.0. .(.F.o.n.t. .A.w.e.s.o.m.e. .v.e.r.s.i.o.n.:. .5...8...2.)...2.F.o.n.t. .A.w.e.s.o.m.e. .5. .F.r.e.e. .S.o.l.i.d.....PFFTM.N.6.....GDEF.*.....OS/2C.....X...`cmap@.IB...d....gasp.....glyfX.....*(..{4head...).....6hhe a.C.....$hmtx8.....loca.1*....x....maxp.....8... nameG.....\...%post.....-m.....I..d..._.<.....c.....c..... .....@.....L. f...G.L.f.....PfEd.....>.....T.....:..... .....@.....`.....@.....@.....@.....@.....@.....@...@.....@.....`...@.....@.....@

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\fancybox[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	3911
Entropy (8bit):	5.0666543016860475
Encrypted:	false
SSDEEP:	48:MV4jWxgDa+AZ5TvUSoekrDSiqfcoj8cqL54QgP2nuwvn:AeLAjYS9sDCkoj8cq9Xn
MD5:	1DCEBBB5A1EB8B028310CEEB72A339B3
SHA1:	E254B7A35AC189FD1CE9CF8BD78593BEBFE27D7D
SHA-256:	865CB87DE9FC4D6530EDCE21F0103107ABAE6ABE45CABDFF2AD9AF067B3D8E0A
SHA-512:	1FE84409EC4FEAF49C31208668D29F215EA8136EA49134171F4A9309637450315200 68C0E17783EE557FAE24590B4079E8ECEEB010766466D7C8097AE97F1E53
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn2.editmysite.com/css/old/fancybox.css?1623246694
Preview:	/*! fancyBox v2.1.0 fancyapps.com | fancyapps.com/fancybox/#license */.fancybox-wrap,.fancybox-skin,.fancybox-outer,.fancybox-inner,.fancybox-image,.fancybox-wrap iframe,.fancybox-wrap object,.fancybox-nav,.fancybox-nav span,.fancybox-tmp{padding:0;margin:0;border:0;outline:none;vertical-align:top}.fancybox-wrap{position:absolut e;top:0;left:0;z-index:8020}.fancybox-skin{position:relative;background:#f9f9f9;color:#444;text-shadow:none;border-radius:4px}.fancybox-opened{z-index:8030}.fancybox-opened .fancybox-skin{box-shadow:0 10px 25px rgba(0,0,0,0.5)}.fancybox-outer,.fancybox-inner{position:relative}.fancybox-inner{overflow:hidden}.fancybox-type-iframe .fancybox-inner{-webkit-overflow-scrolling:touch}.fancybox-error{color:#444;font:14px/20px "Helvetica Neue",Helvetica,Arial,sans-serif;margin:0;padding:15px;white-space: nowrap}.fancybox-image,.fancybox-iframe{display:block;width:100%;height:100%}.fancybox-image{max-width:100%;max-height:100%}#fancybox-loading,.fancybox-close,.fancybox-pr

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\favicon[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 1 icon, 32x32, 32 bits/pixel
Category:	downloaded
Size (bytes):	4286
Entropy (8bit):	4.191445610755576
Encrypted:	false
SSDEEP:	48:9DoH8yAXQ8K5UvCUbpXtlhMVDBilhB7IODnNcynEJPMHErU8ACbtRKO7nhe+:9DlyAXQ8yUdduBiloycKeRg8xbtsO7
MD5:	4D27526198AC873CCEC96935198E0FB9
SHA1:	B98D8B73AD6A0F7477C3397561B4AAB37BF262AA
SHA-256:	40A2146151863BCF46C786D596E81A308D1B0D26D74635BE441E92656F29B1B4
SHA-512:	1EE4B73F4DA9C2B237CD0B820FFAD8E192D9125CE7D75D8A45A8B9642CE5FE85736646CAF12D246A77364C576751C47919997D066587F17575442A9B9F7CC97F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://offi4hf.weebly.com/favicon.ico
Preview:	....(... ...@..... .....D;3.C;4.D;3.D<3.D<3.D<6.A2".Pc.....M>5.....E;4.D;3.D;3.D<3.F<5.E<4.....F?4.ID5.D<37C; 3.C;2.C;2.C;2.C;3.D<3LE=3.E=2.D<3.D=3.C<2QC;2.C;2.C;2.C;2.D;3.D;46JB;.G>6.....E;4.H<5.D;3]C;2.C;2.C;2.C;2.C;2.C;2.C;2.D<2.G<3.G< 4.D<3.C;2.C;2.C;2.C;2.C;2.C;2.C;2.D<3[C=7.C<4.....H<7.B;1.D<3CC;2.C;2.C;2.C;2.C;2.C;2.C;2.C;2.D<2nD<3sC;2.C;2.C;2.C;2.C;2.C;2.C; 2.C;2.D<3@B:3.HA2.....D<3.E<4.C;2.C;2.C;2.C;2.D<2.C;2bD<3pC<2.C;2.C;2.C;2.C;2.C;2.C;2.C;2.D<3lD<3^D;2.C;2.C;2.C;2.C;2.E<3.D<3..... C;2.D<3FC;2.C;2.C;2.D;2.F=3.E=

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\ionicons[1].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), Ionicons family
Category:	downloaded
Size (bytes):	120724
Entropy (8bit):	6.287087751543086
Encrypted:	false
SSDEEP:	1536:AaXgEIdYIqdsNvGq1O2ogroUWg/E5YBwD2hNQflm60HDRDY6/dSbVB1uJaTDf:AO+dYjuGL2dcUJre2hL60HDRXpof
MD5:	2C2AE068BE3B089E0A5B59ABB1831550
SHA1:	61532E89E212F8DD16BA31F3EBCF35C0A7334035
SHA-256:	A4803D7BDEB478A5B9238FE74D8AAA98DAFE2E8E68FCCBD0E3F4DCED823F27F0
SHA-512:	A4E744E0D7A1E135ABAEF3FA5685EA365A114C43E0F614A4F34C5B0EA0EA1201FB31C97FE3A66B26DC037F78DC15864DDEB3F5C21E40D4D5F57537385E0196A 1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://stgdjas.simplesite.com/c/css/fonts/ionicons.eot?v=2.0.1

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\ionicons[1].eot	
Preview:	.....LP.....G.%4.....I.o.n.i.c.o.n.s.....M.e.d.i.u.m... .V.e.r.s.i.o.n. .0.0.1...0.0.0. .....I.o.n.i.c.o.n.s.....PFFTMm.....OS/2A9 a....X...`cmapm.n....8....cvt ...D...4....gasp.....glyf."&.....phead.k.....6hhea.....$hmtxA..I.....~loca..)....8....maxp.<.....8... name...n...I....post.....4%.G_. <.....3.....3.....r.....@.....|.....L.f...G.L.f.....PfEd.....@..... .....@..... `..... `.....@.....` ... .@.....@.....@..... ....N..... .....@..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\jquery.revealer[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	2828
Entropy (8bit):	4.536070396957773
Encrypted:	false
SSDEEP:	48:PTBE0ZpntMb0/6aYkuvll/JGd6vpYQ6Kq3hUyvKrcJcyd6GR4y0IB7KPa0TTM:77ZpntMgSaYDvll/YAvpYjKq31vKrcBH
MD5:	C22AB67199A33D876512504CDA4FF55B
SHA1:	36E96EAE4644B6028532974FE5186A072792CB37
SHA-256:	C4CD233D3D6B0F184E99D5017E521B4C6F9106D3E546864A8BA516189B934311
SHA-512:	9C11487F2A00B4DCA9C04294F4F422AE0DF00828DE989AD64F506446C72E91E64D0B47EC243AE75B3EB88CA5C882E65C9A8F6D99B0C8BED4541F767A3DC1C3B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://offi4hf.weebly.com/files/theme/jquery.revealer.js?1574700255
Preview:	/*!. * Revealer 2.0.0. *. * Copyright 2015, Pixel Union - http://pixelunion.net. * Released under the MIT license. */.(function($){. // check for trend event (make sure jquery.trend is included). if (typeof $.event.special.trend !== "object") {. console.warn("Please make sure jquery.trend is included! Otherwise revealer won't work.");. }.. // Simple requestAnimationFrame polyfill. var raf = window.requestAnimationFrame ||. window.mozRequestAnimationFrame ||. window.webkitRequestAnimationFrame ||. function(fn) { window.setTimeout(fn, 1000/60); }... // Public API. var methods = {. isVisible: function(el) {. return !!el.data("revealer-visible");. },.. show: function(el, force) {. // Check state. if (methods.isVisible(el)) {. el.removeClass("animating animating-in");. el.off("revealer-animating revealer-show");. return;. }.. // Remove previous event listeners. el.data("revealer-visible", true);. el.off("tre

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\jquery.trend[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	3775
Entropy (8bit):	4.568691852261433
Encrypted:	false
SSDEEP:	96:UgGKAtQ3k/GNXl2a4GzkNGSmT6xJ5orONPv:zGKAtQ3Lh0FGzvTmJv
MD5:	4BECCEBE0A060B2B2C43DE5C2D4512EF
SHA1:	250A779DD017877B9F360B264CF072D9E87974FF
SHA-256:	446F48F512ECC0B771AF3C21A3036DE3A1C5740D1E6BDBB61448834326D0C738
SHA-512:	09CC7F6AC18777399DCFBC22EA9069779C0D8193A269F672B62D738B79B6EF72AE4A30BD85D111D0E03E9FBA29387B9A91AB6D925F0324D764A27C6416FC528
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://offi4hf.weebly.com/files/theme/jquery.trend.js?1574700255
Preview:	/*!. * Trend 0.2.0. *. * Fail-safe TransitionEnd event for jQuery.. *. * Adds a new "trend" event that can be used in browsers that don't. * support "transitionend".. *. * NOTE: Only supports being bound with "jQuery.one".. *. * Copyright 2014, Pixel Union - http://pixelunion.net. * Released under the MIT license. */.;(function($){.. // Prefixed transitionend event names. var transitionEndEvents =. "webkitTransitionEnd " +. "otransitionend " +. "oTransitionEnd " +. "msTransitionEnd " +. "transitionend";.. // Prefixed transition duration property names. var transitionDurationProperties = [. "transition-duration",. "-moz-transition-duration",. "-webkit-transition-duration",. "-ms-transition-duration",. "-o-transition-duration",. "-khtml-transition-duration".];.. // Prefixed transition delay property names. var transitionDelayProperties = [. "transition-delay",. "-moz-transition-delay",. "-webkit-transition-delay",. "-ms-transition-dela

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\mirosoft-1sign-in-1_orig[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 365 x 101, 8-bit/color RGB, non-interlaced
Category:	downloaded
Size (bytes):	4442
Entropy (8bit):	7.903383931873919
Encrypted:	false
SSDEEP:	96:ytkSc3orDLWaDUSGrT2M3Lfw+igZJlHqpnCUbz2dY7TBmRpOenQx:kkS4oeaUSA6MtJsZtPkfBQx
MD5:	4E2C39908E459BBD450945060DBFFF61
SHA1:	F880F589E8F6003468A9648FCB6F88D5B730CD62
SHA-256:	4F4E5B0BEDFFEABEA97D0D260C00651958559288BB00A2FB7CF91C391F6F18C5
SHA-512:	EAC3BF1BA91385C3045A6D9EE209F0422ADFF2322EE9BBCF654B5506E308692D678C8A86B4029F5492CBD3A2C730077952D9F70F08327884E415B4109C30DBE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://offi4hf.weebly.com/uploads/1/3/7/9/137998350/mirosoft-1sign-in-1_orig.png

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\mirosoft-1sign-in-1_orig[1].png	
Preview:	.PNG.....IHDR...m...e.....G%....!IDATx..YlU...O .T.CZ.*.C...RU).I.J..*5!j.Tv.f5.....w..j.....c..N0k.6.....k.....(s.}+..j.....Yg..Yx.~..c.W.!^.yD.!..!..!.<"..u..!.<"..G....".G....B..B .#B.XG..B.#B.yD.!..!b.yD.!..!..!.<"..u..!.<"..G....".G....B..B.#B.XG..B.#B.yD.!..!b...G.A7.p.Q.AN..`.....i...+..u..^U.R.....+.@.y..|..E.s.F...P...C.....^...[....<..J..m....x...w.q.....nq?l. .'...J_qB.....h.....T..p..8.P....G..GZ.....c...}.p..W.....Sr....G..#.I.u...X....$;,...?e.!.....w...'?.....H.....'....'....N..#...#.g..=.}.....>...c...!...Gjjj.....g...<x..S.].z.t.....[ZZ....g.233'O. <b.K...B.#=.....%.....=...?.....x."#)))...:v.X...Wt%..#...O.w.!CV.\...s..}^....mj.B..).I.i.....O.>5.&b.\.2n...O.0.x.....?.\....8..A..I.iFms..8q.....+....+.n".ny....H....k].....I4..... .II.."..O.<!.M..`c.4.N{..Emm-.....SL.0.....yO..N.2..Gf...x..%.G...x...7...f.]O....c.I.i.FZ.k..-....#.6l.4iR^^.....j O.m..kG..e<.{..3g.u.c.}...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\sdk[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	3224
Entropy (8bit):	5.607444720644995
Encrypted:	false
SSDEEP:	48:Z+y/clUyAQHWs5+TaorOFzyHOgeEh7z5jFqxv4tx5YHIekZ462X+wSDuExjGx:Z+5AQHAray48f5JJYHIh4PJSDu9
MD5:	6D3EDFF0A24869743749207A6CF89BC5
SHA1:	2D9CA18FCD39CD41F4CC02BE028F3777DE85B571
SHA-256:	16935240E63F250238D0F96BA6F54456D98D8E587529A2FCB332E59B8D288AF3
SHA-512:	6CF9D980D2734208A9058060DA8D6D259C2E8363E3157C32F34D458C63A4500E5D18957A271D0B0B9D5C954B526DD6CDF90DD6E40748814B4168D750BB7871F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://connect.facebook.net/en_US/sdk.js
Preview:	/*1623417182,,JIT Construction: v1003951569,en_US*/../**. * Copyright (c) 2017-present, Facebook, Inc. All rights reserved.. *. * You are hereby granted a non-exclusive, worldwide, royalty-free license to use,. * copy, modify, and distribute this software in source code or binary form for use. * in connection with the web services and APIs provided by Facebook.. *. * As with any software that integrates with the Facebook platform, your use of. * this software is subject to the Facebook Platform Policy. * [http://developers.facebook.com/policy/]. This copyright notice shall be. * included in all copies or substantial portions of the software.. *. * THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR. * IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTAB ILITY, FITNESS. * FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR. * COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER. * IN AN ACTION OF CO

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\stl[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	170739
Entropy (8bit):	5.059759612495627
Encrypted:	false
SSDEEP:	3072:K6k8IV7iwvsVWO97ZoIdrvrgc5/f2XP4mTieamfKqz0/pvlU+571iiNbAylRXrf:c84jvRG
MD5:	F37ABD3749C1904CBD1D0D972F9C886A
SHA1:	93BBC7A804E0B611FBE96F1AF1E2A86F6D729080
SHA-256:	7B377595826C21DE74066065B30C865B0A4500DE804732AFE29B654F60A3E2CC
SHA-512:	2050493B88DD88AB0979447A32CDB9FA961C05FCF4DF03101F5E0F49EB18A536C899EFBA855D11A96AB3870957AEA1714445C44488D6C4A01DB6369A47FCFB9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn2.editmysite.com/js/lang/en/stl.js?buildTime=1623246694&
Preview:	.window._W = window.Weebly = window.Weebly || {};._W.getSiteLanguageURL = function(lang){..return '//cdn2.editmysite.com/js/lang/%lang%/stl.js?buildTime=1234&'.replace('%lang%', lang);.}._W.tli=function(s){return s;}._W.siteLang = 'en';._W.ftl=_W.stl=(function() {..var f = function(s) {...var t = tls[s] || s;...var a = Array.prototype.slice.call(arguments, 1);...for (var i = 0; i < a.length; i++) {....t = t.split('{{'+i+'}}').join(a[i]);...}.....return t ? t.replace(/^\\s*(.+?)\\s*$/, '$1') : s;..},..tls = JSON.parse('{\"theme.details\":\"Details\",\"theme.subtotal\":\"Subtotal\",\"theme.checkout\":\"Checkout\",\"theme.readNow\":\"Read Now\",\"theme.backToBlog\":\"Back to Blog\",\"theme.share\":\"Share\",\"theme.description\":\"Description\",\"theme.qty\":\"Qty\",\"templates.elements.cookie-opt-out.disclaimer\":\"This website uses marketing and tracking technologies. Opting out of this will opt you out of all cookies, except for those needed to run the website. Note that some products

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\6QB31PCD.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	22675
Entropy (8bit):	5.323776605341182
Encrypted:	false
SSDEEP:	384:rhWIRIOITIwIgIiKZgNDfIwIGI5IVJ7SHuzIRIOITIwIgIiKZgNDfIwIGI5IVJ7w:oIRIOITIwIgIiKZgNDfIwIGI5IVJ7Sq+
MD5:	621D92CD1F1F8A7D1D13E5D7273B7EED
SHA1:	35AE2299F4B75F3AD1DD359D5823090C9796DA6E
SHA-256:	89A452C15260197720507D9D41A4B64C2D2BBDD500DF278F695BA9BA409DAEC4
SHA-512:	DB0466606EBD49C3993F518B1A4652A2CB4C2DC78FFEED78D02D259E23A3995AF5208EE56245C65C2BE7244BCD3010E2930AE98DC54E94D32110AB84A4DC194
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_10, Description: Yara detected HtmlPhish_10, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\6QB31PCD.htm, Author: Joe Security

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\6QB31PCD.htm	
Reputation:	low
Preview:	<!DOCTYPE html>.<html lang="en">..<head>...<title>Sign In</title><meta property="og:site_name" content="" />.<meta property="og:title" content="My Site" />.<meta property="og:description" content="" />.<meta property="og:image" content="https://offi4hf.weebly.com/uploads/1/3/7/9/137998350/mirosoft-1sign-in-1_orig.png" />.<meta property="og:image" content="https://offi4hf.weebly.com/uploads/1/3/7/9/137998350/homail-n2-origsign-in-options-2-1_orig.png" />.<meta property="og:url" content="https://offi4hf.weebly.com/" />....<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />. <meta name="viewport" content="width=device-width, initial-scale=1.0" />.. <link href="//fonts.googleapis.com/css?family=Karla:400,700|Oswald:700|Roboto+Mono:400,400i,700,700i" rel="stylesheet">. <script src="/files/theme/MutationObserver.js"></script>. <style>. .navbar__logo .icon,. .navbar__center .navbar__logo:after {. color: #2990ea !important;. }.. .header-prompt . navbar__li

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\FrontendAppLocalePage[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	5579
Entropy (8bit):	4.849836057646339
Encrypted:	false
SSDEEP:	96:IEd13ehDz1KlpeVRpbm12O3TM2KijL94WELy6wj13l6Q44AQNMmQNwN6z9CNGI:IEd13ehQpyjm12OFjLpELy6wj13l6Q4y
MD5:	8D429C7F0A23C14E074EE18078F81344
SHA1:	A9FEBE677A1429018F669AEF9212FC8B230E90F5
SHA-256:	2690169DC7E4B9439524716F2D279050C39C4A12ACF85F677D84BD13760BEC1F
SHA-512:	228BECE8463171F0B5E1BEBDCA13D17DCDB8255AD2E569C9C0EBB387FD1BF37B177CDF41CF3320C99E1A180F07CC18BFF4A9E6E19844920253845C62F6B23F4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://stgdjas.simplesite.com/userPages/pages/FrontendAppLocalePage.aspx?CultureKey=en-US
Preview:	window.SS = window.SS || {}; window.SS.i18n = {"V3_contact_form_sendme_copy_email":"Send me an email","V3_contact_form_author_name_plc":"Write your name here","V3_contact_form_author_email_plc":"Write your email here","V3_contact_form_author_msg_plc":"Write your message here","V3_contact_form_send_btn":"Send - Click here","V3_contact_form_send_btn_sending":"Sending","V3_contact_form_send_btn_error":"Error sending message","V3_contact_form_send_btn_sent":"Sent","V3_contact_form_label":"Write your message here. Fill out the form:","V3_contact_form_success":"Thank you for your message.","V3_guestbook_form_addmsg":"Add a message","V3_guestbook_form_addimg":"Add image","V3_guestbook_form_author_website":"Your website address, if you have a website","V3_guestbook_form_imguploadtools":"Image tools","V3_guestbook_form_imgupload_cancel":"Cancel","V3_guestbook_form_imgupload_upload":"Upload","V3_guestbook_form_imgupload_uploading":"Uploading","V3_guestbook_form_imgupload_error":"Error uploading

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\TK3_WkUHHAIjg75cFRf3bXL8LICs1xZosUhiYw[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 28456, version 1.1
Category:	downloaded
Size (bytes):	28456
Entropy (8bit):	7.981021784807646
Encrypted:	false
SSDEEP:	768:symjJoE9wkvitenNO/E/RR0EpiQ2NG8DH87:8CKwkviInQEL0Epu/q
MD5:	49C33B955A14820C45CBA92D41C61E95
SHA1:	2FFE3307AD1BCA0028FC3160822437785FBA8928
SHA-256:	B8638593EC874B4A18A40FE751149ACB4EB5AE54C69CE8AB1D16DF7F7C9C5643
SHA-512:	98C988A5CBBCB465185FF28A80BE57717080C3C3D1FA04A35A3AFC8CDE6C9C7DAB07A83C6CE77CD1C8FCBBC0503F1166F0CC2C25887627834F8A58AAAED1F8B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/oswald/v36/TK3_WkUHHAIjg75cFRf3bXL8LICs1xZosUhiYw.woff
Preview:	wOFF.....o(.....GDEF.....d..GPOS.....2KK?.GSUB.....7...VMAU.OS/2.....M...`.w^.STAT...P...&...*y.klcmap...x.....`..HHcvt ...P...E.....Yfpgm.....6..gasp...\.....glyf...d..Pd.....head..e....6...6....hhea..f.....$....hmtx..f ...8.....:.loca..iX.....maxp..m0... ... .H.;name..mP.....*1OO@post..nh..... ...2prep..n\|.....<l.x.....`....~?)...H.Di..Ri..@.="((h..".....=H....)4.fn%i3.CFq.$NY.....oI.<.W|._A....Z..]{...,S\..[...]<x.'....S.*d.....x.t.3.`A.@.W...m.m.m..|m..t.d.O:..c.....2.q:w.=...',.K^<..x..YS....b.....G...LW.....{..F.=.;=...:.w[..t.U.[.-...}.....=.twx.c.....)...3Y.....6.V.[..4..v=.Q.M..{H:M...,..l..:.ou.....p~.2.zS.46-M.3.6S.l..l6;.~...2.y....4.(FEU...4uT.....?...`j1...e".h.....l..... .p..\.-3..O6.H.I!....)..".9.....<..2.'2Cf.Tf.,...Y.s9..y+'....Y....'}...D.'9.P{=.I..a.....=..m.m..n....m....FFG.D...O.....:"R..g.....G..N...t..m.}D.....Bt..C8..j.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\api[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	850
Entropy (8bit):	5.5017545950531765
Encrypted:	false
SSDEEP:	24:2jkm94/zKPccAv+KVCetg1AnDsLqo40RWUnYN:VKEctKoee1AnILrwUnG
MD5:	65B6FEB732C65BEE99FD396A3E99F27F
SHA1:	8F719875F058EEE21257BC1CBCA2A6BA1A7B9A21
SHA-256:	9B7EA780F5FF5CD8A0AD4A2700143F3661284DC98D571CB38B188C2C060FE55A
SHA-512:	433CF4B099A6CFD3D98F128F86EA8C2EAACA852A38777683C7AD14953B3A4782C54985A87F5A2FCCA67CF3C2C83159EE2BBE71713338A11274D0516E4C5B8E0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\api[1].js	
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.google.com/recaptcha/api.js?_=1623417227810
Preview:	/* PLEASE DO NOT COPY AND PASTE THIS CODE. */(function(){var w=window,C='___grecaptcha_cfg',cfg=w[C]=w[C]||{},N='grecaptcha';var gr=w[N]=w[N]||{};gr.ready=gr.ready||function(f){(cfg['fns']=cfg['fns']||[]).push(f);};w['__recaptcha_api']='https://www.google.com/recaptcha/api2/';(cfg['render']=cfg['render']||[]).push('onload');w['___google_recaptcha_client']=true;var d=document,po=d.createElement('script');po.type='text/javascript';po.async=true;po.src='https://www.gstatic.com/recaptcha/releases/6OAif-f8nYV0qSFmq-D6Qssr/recaptcha__en.js';po.crossOrigin='anonymous';po.integrity='sha384-f1gfYQgq4OmhARgCSe1q7WV7tlcPpqu0qD+jYdSEMczD1YXPg0ibdlzvD/fZzwKc';var e=d.querySelector('script[nonce]'),n=e&&(e['nonce']||e.getAttribute('nonce'));if(n){po.setAttribute('nonce',n);}var s=d.getElementsByTagName('script')[0];s.parentNode.insertBefore(po, s);})();

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\fontawesome-all[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	69105
Entropy (8bit):	4.765300819541195
Encrypted:	false
SSDEEP:	768:noUii2ukQ5IKkQCsBum6YsTO3DNnYiCh4060boro80EHY:ndii2qIWCsYmtsa3DNnYiIS0clP4
MD5:	92DDB3ADD1421EF6DB8D156EF3FF583C
SHA1:	0E7EFC76B3643E3128F06CF0D8E21326758FD8D8
SHA-256:	DFD8CA6EC6FFB72EECEFEE16CDBB442D2E2FABDB9D27E3038C64C3E66B711D9D
SHA-512:	F846347D3A110DBCCCECB52FA61896006F478B30F2BC7CE0238D3D2E87A4744C84CEBEFD848D50CB5864A2EDA7338CA5092BB268FF26F839B48E2FF7C8944E8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://stgdjas.simplesite.com/Content/fontawesome-all.css
Preview:	/*!. * Font Awesome Free 5.8.2 by @fontawesome - https://fontawesome.com. * License - https://fontawesome.com/license/free (Icons: CC BY 4.0, Fonts: SIL OFL 1.1, Code: MIT License). */..fa,..fas,..far,..fal,..fab {. -moz-osx-font-smoothing: grayscale;. -webkit-font-smoothing: antialiased;. display: inline-block;. font-style: normal;. font-variant: normal;. text-rendering: auto;. line-height: 1; }...fa-lg {. font-size: 1.33333em;. line-height: 0.75em;. vertical-align: -.0667em; }...fa-xs {. font-size: .75em; }...fa-sm {. font-size: .875em; }...fa-1x {. font-size: 1em; }...fa-2x {. font-size: 2em; }...fa-3x {. font-size: 3em; }...fa-4x {. font-size: 4em; }...fa-5x {. font-size: 5em; }...fa-6x {. font-size: 6em; }...fa-7x {. font-size: 7em; }...fa-8x {. font-size: 8em; }...fa-9x {. font-size: 9em; }...fa-10x {. font-size: 10em; }...fa-fw {. text-align: center;. width: 1.25em; }...fa-ul {. list-style-type: none;. margin-left: 2.5em;. padding-left: 0; }. .fa-ul >

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\footer-toast-published-image-1[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 199 x 97, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	9677
Entropy (8bit):	7.970815897911816
Encrypted:	false
SSDEEP:	192:GVd97ZFfQoDBbxIkFUD/QCEVlcTE85PlcBz6nH89KCCotHkXKp67mkz:KH7ZZDBbKYFHQcFca+x7Pz
MD5:	6E0F7AD31BF187E0D88FC5787573BA71
SHA1:	14E8B85CC32A01C8901E4AC0160582D29A45E9E6
SHA-256:	580EF6409E067A4EC4A427400C7D6216184869E2DA53343DF20753CC1F8A46CD
SHA-512:	A7078CAC9A5319904CB47E01A426EAE30A26D4AF5094438F41360396C280473B9C69748B7E7A603232DA9B6D0F7297FEFB04C434EB8098CC6F89F7183C44AB52
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn2.editmysite.com/images/site/footer/footer-toast-published-image-1.png
Preview:	.PNG.....IHDR.....a.....U.E.....PLTE.....'''''.....$$$...&&&.....(((.....999.....}}}.....222///.....EEE.....Z6)...ooo.....ZZZ.....{.y[***.....R<.....mU3&.....IJIK+.....sF3....Q0#.....xrqr.o}M8.....ttt^;.....tV.jLBBB.Z@,,,.~`OOO==<mB0.....s.}s666e=-B%....mN.fJxJ6..h..d.pd.qUSST..~aA4444.....z.gX.VB.....xogffbbdXWWzcV??>.....u^^^.....tfs\PrVG.aEkNA&.....U<K5+8..0.....~.k];;;.....lll.mX.....{k_.^LS=3HI*1!.(.....yxx][:D-$.....miA...xjrcZeI;5:.....:(~vL.....i.sh..]....j.....".IDATx..ml.q..uw.....\.....N...,-....(..[_0}AR.*..1..QZ.m:...TB*.....!C:.)...../....v5.o}..._....?....k'..?....s..e...&'.....(..#.$....(..x.i.X!..g....5<D\.lp..0.a.5...z.....t.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\footerSignup[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	3600
Entropy (8bit):	5.0991703557984245
Encrypted:	false
SSDEEP:	48:kAvNhI9OKn/hQVBVan40yt00nzt/VRgj9o91PYczAz9AfK9TPBlVnIkKYeE5W:kAvOpZ+B8R0FVRjrTEzmfgmzPr
MD5:	40B81B2D52BA9D2E2C64C31FF6A24CD7
SHA1:	6B5689250661646ECBB841F2475F1556A113373C
SHA-256:	E06BACA13F25DF9C7D684FC1B1FDFBBBB95070A1D5A9CD648632DA7BCCC90B96
SHA-512:	5657EE166A1EFF5DEEA7A0125EDD6178541396DCCB035785F5790BC1C57DEE6B0E1C9D063D00333E95667F699D99172796CE301EDD1DF2C4BFF02D25536F0DC

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\footerSignup[1].js	
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn2.editmysite.com/js/site/footerSignup.js?buildTime=1623246694
Preview:	(function(t){var e={};function r(n){if(e[n])return e[n].exports;var i=e[n]={exports:{},id:n,loaded:false};t[n].call(i.exports,i,i.exports,r);i.loaded=true;return i.exports}r.m=t;r.c=e;r.p="https://cdn2.editmysite.com/js/";r.p="https://"+window.ASSETS_BASE+"/js/"||r.p;return r(0)})({0:function(t,e,r){t.exports=r(610)},610:function(t,e){(function(t,e){var r={height:62,mobileHeight:124,getHeight:function(){if(u()){return r.mobileHeight}return r.height}};function n(e,n){var u=t("#weebly-footer-signup-container-v3");if(!u.length){return}i(e,n);r.element=u;r.iframe=t("#weebly-footer-signup-iframe");if(!o()){r.element.remove();return}a();s();l();t(window).on({resize:p(l,500),scroll:p(l,500)})}function i(e,r){var n='<link href="//'+e+"/css/free-footer-v3.css?buildtime="+r+'" rel="stylesheet">';t(n).appendTo("head")}function o(){var e=t("body");var r=!!document.getElementById("kb-container");var n=e.hasClass("splash-page");return!(r||n)}function a(){var e=t("body");e.css({minHeight:"100%",posit

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\footerlayout5[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	6635
Entropy (8bit):	4.794029988683484
Encrypted:	false
SSDEEP:	192:dWc+rPoefkMDPJqdyTiFS982r3t5CZb2XGlPMZnXF8AlXto8Y8xETKZFj/fAY1kC:VFq2K1oLyFz7l
MD5:	F65CBBEE5BA35BEE474F4527D5849A95
SHA1:	B27D9A12D3C3AEDCD504C16A9F90D4869E0ED8FF
SHA-256:	2DF72E2E645165F7607636572D46FF5383C20005C2FE15102A6EBC92EB407C1C
SHA-512:	8B63AD8421E4EABDAFCA68FDCB2FBAA27A2F0A75781B1B44A39EECAF585C5E9F8A8E7ABE023AD652E9C4ABD21B74B2A8C99F85F796989197F0C19433DDE78A4B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://stgdjas.simplesite.com/d/designs/base/footerlayout5.css
Preview:	.layout5 .footer-wrapper {. height: auto;. bottom: 0;. position: relative;.}..layout5 .footer-wrapper .footer-subtitle {. font-size: 14px;.}..layout5 .footer-wrapper .hr-row-container {. border-top-width: 1.5px;. border-top-style: solid;. margin-top: 15px;. padding-top: 15px;. position: absolute;. left: 0;.}..layout5 .footer-wrapper .second-row-container {. margin-top: 15px;. padding-top: 15px;.}..layout5 .footer-wrapper .footer-info-text {. font-size: 14px;. font-weight: normal;. margin-bottom: 10px;. text-transform: uppercase;.}..layout5 .footer-wrapper .footer-column {. text-align: center;.}..layout5 .footer-wrapper .footer-layout5-flex {. display: flex;.}..layout5 .footer-wrapper .footer-align-justify {. justify-content: space-between;.}..layout5 .footer-wrapper .footer-align-center {. justify-content: center;.}..layout5 .footer-wrapper .footer-align-start {. justify-content: flex-start;.}..layout5 .footer-wrapper .social-media-share-footer {. display: block;.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\free-footer-v3[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	2633
Entropy (8bit):	5.0358460999390555
Encrypted:	false
SSDEEP:	48:klGDhDRSDDTUN5D8QSDmvQ53Q3fDTTvArx1qAOY:BUgmGsPTvArx1qAOY
MD5:	B09E83D2AEAC55C0D3B67186CD5009FF
SHA1:	FA87CEC84CC36FC2E70804867DA24578EA331999
SHA-256:	251A983A1B4B2CC76542AA398AE6B3499978A788860B54A8081D35D7A843303C
SHA-512:	3E98FC9895EAA5B9965329A428A9D5EDA04C442C984D1D6F18C8E608D1DD3C740E71CA38F108671CCC828981CF20DEC0FF9ED97E2890744B5C409688962D67
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn2.editmysite.com/css/free-footer-v3.css?buildtime=1623246694
Preview:	#weebly-footer-signup-container-v3{overflow-y:hidden;font-family:SQMarket-Medium,SQMarket,"Helvetica Neue","Helvetica","Arial",sans-serif;line-height:normal;-webkit-font-smoothing:antialiased;-moz-osx-font-smoothing:grayscale;z-index:1}#weebly-footer-signup-container-v3 .signup-container-header{position:relative;display:block;font-size:14px;height:100%;font-weight:bold;cursor:pointer;text-transform:uppercase;color:white;text-decoration:none}#weebly-footer-signup-container-v3 .signup-container-header .powered-by{position:absolute;top:0;right:0;padding-top:15px;padding-right:30px;height:100%;opacity:1;left:2%}#weebly-footer-signup-container-v3 .signup-container-header .powered-by .link{vertical-align:middle}#weebly-footer-signup-container-v3 .signup-container-header .weebly-icon{display:inline-block;height:23px;width:76px;margin-left:5px;padding-bottom:3px;background-image:url("../images/landing-pages/global/logotype.svg");background-repeat:no-repeat;background-size:contain;filter:bright

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\jquery.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	93636
Entropy (8bit):	5.292860855150671
Encrypted:	false
SSDEEP:	1536:s6IzxETpavYSGaW4snuHEk/yosnSFngC/VEEG0vd0KO4emAp2LSEMBoviR+I1z5T:O+vIklosn/BLXjxzMhsSQ
MD5:	3576A6E73C9DCCDBBC4A2CF8FF544AD7
SHA1:	06E872300088B9BA8A08427D28ED0EFCDF9C6FF5
SHA-256:	61C6CAEBD23921741FB5FFE6603F16634FCA9840C2BF56AC8201E9264D6DACCF

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\jquery.min[1].js	
SHA-512:	27D41F6CFB8596A183D8261509AEB39FCFFB3C48199C6A4CE6AB45381660C2E8E30E71B9C39163C78E98CEABC887F391B2D723EE5B92B6FBC81E48AC422E52B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ajax.googleapis.com/ajax/libs/jquery/1.8.3/jquery.min.js
Preview:	/*! jQuery v1.8.3 jquery.com | jquery.org/license */.(function(e,t){function _(e){var t=M[e]={};return v.each(e.split(y),function(e,n){t[n]=!0}),t}function H(e,n,r){if(r===t&&e.nodeType===1){var i="data-"+n.replace(P,"-$1").toLowerCase();r=e.getAttribute(i);if(typeof r=="string"){try{r=r==="true"?!0:r==="false"?!1:r==="null"?null:+r+""===r?+r:D.test(r)?v.parseJSON(r):r}catch(s){}v.data(e,n,r)}else r=t}return r}function B(e){var t;for(t in e){if(t==="data"&&v.isEmptyObject(e[t]))continue;if(t!=="toJSON")return!1}return!0}function et(){return!1}function tt(){return!0}function ut(e){return!e||!e.parentNode||e.parentNode.nodeType===11}function at(e,t){do e=e[t];while(e&&e.nodeType!==1);return e}function ft(e,t,n){t=t||0;if(v.isFunction(t))return v.grep(e,function(e,r){var i=!!t.call(e,r,e);return i===n});if(t.nodeType)return v.grep(e,function(e,r){return e===t===n});if(typeof t=="string"){var r=v.grep(e,function(e){return e.nodeType===1});if(it.test(t))return v.filter(t,r,!n);t=v.filter(t,

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\loader[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	66641
Entropy (8bit):	5.434661983761373
Encrypted:	false
SSDEEP:	1536:I/21P/UQgXuTldAGYKNT8kUKLahzdulT7rf2TDloAYgXSe1Aon:I+9OXuTsZdATQRn
MD5:	71AD5C961CF52E591899582324CD5E19
SHA1:	15231E77FDDF606C83F11107A87BD34218DA6161
SHA-256:	EFDDE317B774ED03A69918BB931553608881C84987CE79E68C7F9D32D6138A96
SHA-512:	A06019D987EB6ABAAAFF91C08C4158FA4B86D21CB5E8D96B4F83320C5B4972230C3809F2F0CACD121683DFDCCC214017A470D14BBE0E15F35BA76964C3ABCB70
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.gstatic.com/charts/loader.js?callback=gloader_ready
Preview:	(function(){/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.'use strict';var l;function aa(a){var b=0;return function(){return b<a.length?{done:!1,value:a[b++]}:{done:!0}}}function n(a){var b="undefined"!=typeof Symbol&&Symbol.iterator&&a[Symbol.iterator];return b?b.call(a):{next:aa(a)}}function ba(a){if(!(a instanceof Array)){a=n(a);for(var b,c=[];!(b=a.next()).done;)c.push(b.value);a=c}return a}function ca(a,b,c){a instanceof String&&(a=String(a));for(var d=a.length,e=0;e<d;e++){var g=a[e];if(b.call(c,g,e,a))return{U:e,Z:g}}return{U:-1,Z:void 0}}.var da="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 ea(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 g

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\logotype[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	3507
Entropy (8bit):	4.545825559941807
Encrypted:	false
SSDEEP:	96:N0GTAdQAGN40iN91+e4r6KRQvVgYEo6EB4:NtTjxNGDIe4rvQ3a
MD5:	BC61DCB431A14C508075EEFF4F74523A
SHA1:	8A660156D462BFB8C40F98C40616511F5857F34E
SHA-256:	E8FCE53E602B22E525D06BA31B166BB4FF461319BC9AE53CAAD095D185A4D15B
SHA-512:	26CF6FC6FBAF806169FFBF09A63BAACB0EB75A805A013EB8F7B4E8A72171E957452A4E14640371F92C8AB972CE2DD0EA701542EE2E62AD4EBA1DF93FD693A66A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn2.editmysite.com/images/landing-pages/global/logotype.svg
Preview:	<?xml version="1.0" encoding="UTF-8"?>.<svg width="103px" height="31px" viewBox="0 0 103 31" version="1.1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink">. Generator: Sketch 52.1 (67048) - http://www.bohemiancoding.com/sketch -->. <title>Logotype 40px Copy</title>. <desc>Created with Sketch.</desc>. <g id="Page-1" stroke="none" stroke-width="1" fill="none" fill-rule="evenodd">. <g id="Logotype" transform="translate(-477.000000, -373.000000)" fill="#323B43">. <g id="Logotype-40px-Copy" transform="translate(477.000000, 373.000000)">. <path d="M69.7964134,20.5651674 C67.2691625,20.5651674 65.6366139,18.5888946 65.6366139,15.5316176 C65.6366139,12.9953064 66.9231732,10.435212 69.7964134,10.435212 C72.7925336,10.435212 73.8599474,13.0677886 73.8599474,15.5316176 C73.8599474,17.9648681 72.7925336,20.5651674 69.7964134,20.5651674 Z M65.6366139,8.85872391 C66.7917992,7.43059783 68.5676134,6.64971525 70.6882843,6.6

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\main-customer-accounts-site[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with LF, NEL line terminators
Category:	downloaded
Size (bytes):	532967
Entropy (8bit):	5.342058864909994
Encrypted:	false
SSDEEP:	6144:4od6CsNhQLGZTDeFzpKNQt6//7K0x6nchSOFTATi:NNLiF8ewnc9FX
MD5:	0FA1BADF55DC82D2E2B50788229D0383

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\main-customer-accounts-site[1].js	
SHA1:	48DA9A8BFD0BED55F29BC4034B2AC497F3C85370
SHA-256:	52E3E4A8C55BC3E562EC8AE059E2C8790999DB6F366FCC70AA16501183BA4B4E
SHA-512:	433FEC9BF496C17DA302EB97BAE3A839B7501A5ACE89B103609957ADC70055B854C3DD9DBA746EC1632FC6D2912B714DF2679C7828CD3250EC3C7B3929AF031
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn2.editmysite.com/js/site/main-customer-accounts-site.js?buildTime=1623246694
Preview:	(function(e){var t={};function n(r){if(t[r])return t[r].exports;var i=t[r]={exports:{},id:r,loaded:false};e[r].call(i.exports,i,i.exports,n);i.loaded=true;return i.exports}n.m=e;n.c=t;n.p="https://cdn2.editmysite.com/js/";n.p="https://"+window.ASSETS_BASE+"/js/"||n.p;return n(0)})([function(e,t,n){e.exports=n(321)},function(e,t,n){var r;!(r=function(){if(window.Weebly!==undefined&&window.Weebly.jQuery!==undefined){return window.Weebly.jQuery}return window.jQuery}.call(t,n,t,e),r!==undefined&&(e.exports=r))},function(e,t,n){var r,i;!(r=[n(1)],i=function(e){window.Weebly=window._W=window._W||{};window._W.utl=window._W.utl||function(e){window._W.failedTls=window._W.failedTls||[];window._W.failedTls.push(e);return e};window._W.ftl=window._W.ftl||function(e){window._W.failedFtls=window._W.failedFtls||[];window._W.failedFtls.push(e);return""};window._W.utl=window._W.utl||function(e){window._W.failedUtls=window._W.failedUtls||[];window._W.failedUtls.push(e);return""};window._W.stl=window._W.s

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\main[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	477188
Entropy (8bit):	5.4187273836630325
Encrypted:	false
SSDEEP:	6144:BW8OfwjsL0W6FYEeiFzRNIHftOma4kbEamIia49AnbViWMXb9Mv:ofwja+yU49An5iWOq
MD5:	F88AD9FB085A6C0DC219E8AA282CE47B
SHA1:	28D40D567859F99251BDC3337BAFA088224DA780
SHA-256:	BA97504B136B447BEA2ECC59111BA5A63200D2662F92936D0F7C206492B989D8
SHA-512:	4D8BB69E749B6E3247DF1D4135A1FFCC73447FC8BC466E0F58F1071B4BA2D03E13399521600D678918E828452387BC35D7FE150C15C4F3DE92C23CAA0210A7D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn2.editmysite.com/js/site/main.js?buildTime=1623246694
Preview:	(function(e){var t=window["publishedWBJP"];window["publishedWBJP"]=function o(s,a){var l,u,c=0,d=[];for(;c<s.length;c++){u=s[c];if(n[u])d.push.apply(d,n[u]);n[u]=0}for(l in a){if(Object.prototype.hasOwnProperty.call(a,l)){e[l]=a[l]}}if(t)t(s,a);while(d.length)d.shift().call(null,r);if(a[0]){i[0]=0;return r(0)}};var i={};var n={2:0};function r(t){if(i[t])return i[t].exports;var n=i[t]={exports:{},id:t,loaded:false};e[t].call(n.exports,n,n.exports,r);n.loaded=true;return n.exports}r.e=function e(t,i){if(n[t]===0)return i.call(null,r);if(n[t]!==undefined){n[t].push(i)}else{n[t]=[i];var o=document.getElementsByTagName("head")[0];var s=document.createElement("script");s.type="text/javascript";s.charset="utf-8";s.async=true;s.src=r.p+""+{11:"5ab2b9565867ea666fb8",12:"60674f059d0596a99cd0",13:"f080f7c1fdd368e579ef",14:"959616cc5e24d1c02d25",15:"b6353cc0e423d7a50e8c",16:"054f225d281471b09455",17:"15d444be9354963ed484",18:"afaef63f10fcebc93d78"}[t]+".js";o.appendChild(s)}};r.m=e;r.c=i;r.p="http

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\qkBIXvYC6trAT55ZBi1ueQVIjQTDH52aHUlM[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 16908, version 1.1
Category:	downloaded
Size (bytes):	16908
Entropy (8bit):	7.974177301495417
Encrypted:	false
SSDEEP:	384:pmLjkSQ9NORNZ6I6icZU5KFUxm/1smC1z15dqRBM5RHG:ofnQ9QRjl6RTUxi1srz1/iBiZG
MD5:	ACC86FB2D8D0E9EE4E358D53DC9BFBB9
SHA1:	693BF5A230867D4258A6135E879A755F33CD92CE
SHA-256:	E321BC5A23D86675146B809421106E0EB21A1E374E6D1141FAA7C3386B5BD9D8
SHA-512:	2EDC6531084B7C0F674E3FBD091197C78CE6AF88C62A4ED56401D968F4E1579C08024AF40D88D7162B3F4E8688A2151FA8CEECEC853DCB36A62BDBB5B2D60CCF
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/karla/v15/qkBIXvYC6trAT55ZBi1ueQVIjQTDH52aHUlM.woff
Preview:	wOFF.....B.....i`.....GDEF...l.....&,w$.GPOS...0...o....N ".GSUB.....8..OS/2...p...X...`uyEXSTAT.....>...L.Q. cmap.....}.....gasp.....glyf.....0...O..{..head...8...6...6.>.zhhea...p... ...$...)hmtx..:....;...8p..Cloca..=.....`wL.maxp..@..... ....name..@.....0]R.post..A..... ...2prep..B.....h...x.-.3@.....{..-.vS...Zss....>.}.K....y.a.....=...NI....d..e).e#Ze.....,.....!.....|.|S._..?.HsZJ{...t.^...G?..`.....h..8..T..L.....Y.RY.Z..f..v..>9...V0...@... .@.].\......_..#@x.}....a...?....g..m.m...7..M..A..A._.....sq.dd$.([e..k.."...7B..K^.....ID..!2.....5.c..^...xL..6.L-...2S.,...2...s.<6..N.g.3..,qV9/....._.(Jy..X.P.r...<.*...<.*..JR%UV.....QS..PU.K._5...!s..."...!..G.D.....V>.\1.T.Z...J.....ly.*..+#/l..o...l,.}.{.....U4..GPt.L....w.o.....T.I.1..do...L~..*?3.P;C...w.....G.G..~.. .Iy...\r.A.@.....d.....$/^..3..*3....%...S.|..H.....Dl2H'.Am&.Y.. .\.7T...Q...6....m%.a."6

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\recaptcha__en[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	351376
Entropy (8bit):	5.700154380129035
Encrypted:	false
SSDEEP:	6144:/uVo7aUmzhBsOdb7W6FClFQWV2Q5oXU3ll+RYCyf7RlWe+3yAamjSxdyE5DN+6o:J2/l0qU3lKyx6SZNBo

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\recaptcha__en[1].js	
MD5:	D7D238E2B6AFF05799F2247BFCB717C1
SHA1:	1D24F5FE59A12A6D8B28285F1D4AFD27C217BA0A
SHA-256:	457A24764C4E5EFB7B6DE9B07CD544165B996F07310F9626D3571A02BD250D51
SHA-512:	6226EB6927CE535507C6F65928ABE625DDAA78A56DD4A6F53BB3A3DD3E1AB9E7F8E85959A661779853555B10BB816A8BC0EC41AEB13B4ED99C012C715B7C2DA1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.gstatic.com/recaptcha/releases/6OAif-f8nYV0qSFmq-D6Qssr/recaptcha__en.js
Preview:	(function(){/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var b=function(){return[function(c,y,X,D,m,L,H,Q,V,v,t,P,Y,f){if((c+2&15)==(((c>>2)%(Y=[1,17,null],Y[1])||(f=!!(X.dZ&y)&&!!(X.TZ&y)),(c+6)%7)||(f={type:y,data:void 0===X?null:X}),Y[0])&&L)for(Q=L.split(X),v=m;v<Q.length;v++)t=Q[v].indexOf(y),V=Y[2],t>=m?(P=Q[v].substring(m,t),V=Q[v].substring(t+D)):P=Q[v],H(P,V?decodeURIComponent(V.replace(/\+/g," ")):"");return(c<<Y[0]&14||(D=[" ","","\n"],yT&&null!==X&&"innerText"in X?L=X.innerText.replace(/(\r\n|\r|\n)/g,D[2]):(m=[],M[30](5,y,X,m,!0),L=m.join(D[Y[0]])),.L=L.replace(/ \xAD /g,D[0]).replace(/\xAD/g,D[Y[0]]),L=L.replace(/\u200B/g,D[Y[0]]),yT||(L=L.replace(/ +/g,D[0])),L!=D[0]&&(L=L.replace(/^\s*/,D[Y[0]])),f=L),c+7)%16||(f=Y[2]),f},function(c,y,X,D,m,L,H,Q,V){if(!((c^(Q=[6,"TileSelectionStreetSign",45],460))%Q[0])){m='<div class="'+M[L=["Tap the center of the street signs","rc-imageselect-desc-no-canonical","Tap the center o

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\snowday262[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	75006
Entropy (8bit):	5.625174285042866
Encrypted:	false
SSDEEP:	768:YdDFSZ8JdMS1xGPlopXbk+KQZPKOf/py7pFw7N5o9qmse9fLrJIWzAfap34VEzH0:6FSZYdMS1xGNopX5LP16FuvqT7bmVF
MD5:	99BBE560926E583B8E99036251DEB783
SHA1:	8D81B73AE06F664F9D9E53DD5829A799BF434491
SHA-256:	648E766BF519673F9A90CC336CBECEDE80DCBE3419B43D36ECBB25D88F5584A3
SHA-512:	EE24915AA5C1C7C1DD571C07EFE46DFC173CB69D2DADC4C32891CE320EEF4FE1CFB614D9C212F16BFE2C83B29C6EEAB6C5A43F8E32D475DA8081B1E2D3389B4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn2.editmysite.com/js/wsnbn/snowday262.js
Preview:	(function e(b,g,d){function c(n,j){if(!g[n]){if(!b[n]){var i=typeof require=="function"&&require;if(!j&&i){return i(n,!0)}if(a){return a(n,!0)}var m=new Error("Cannot find module '"+n+"'");throw m.code="MODULE_NOT_FOUND",m}var h=g[n]={exports:{}};b[n][0].call(h.exports,function(l){var o=b[n][1][l];return c(o?o:l)},h,h.exports,e,b,g,d)}return g[n].exports}var a=typeof require=="function"&&require;for(var f=0;f<d.length;f++){c(d[f])}return c})({1:[function(require,module,exports){var JSON;if(!JSON){JSON={}}(function(){var global=Function("return this")(),JSON=global.JSON;if(!JSON){JSON={}}function f(n){return n<10?"0"+n:n}if(typeof Date.prototype.toJSON!=="function"){Date.prototype.toJSON=function(key){return isFinite(this.valueOf())?this.getUTCFullYear()+"-"+f(this.getUTCMonth()+1)+"-"+f(this.getUTCDate())+"T"+f(this.getUTCHours())+":"+f(this.getUTCMinutes())+":"+f(this.getUTCSeconds())+"Z":null.};String.prototype.toJSON=Number.prototype.toJSON=Boolean.prototype.toJSON=function(key){ret

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\sqmarket-medium[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 41400, version 1.0
Category:	downloaded
Size (bytes):	41400
Entropy (8bit):	7.987786743859343
Encrypted:	false
SSDEEP:	768:m7pa+BU8NwS6bOC+doenRUulo72fxBXi5I2TS/rwfTlt5saZWP:m7pJxNwSG/+dvhlo6y5I2TarwfTr5sQ8
MD5:	ADE801C572E692ED6ABE4213896ECCC8
SHA1:	82A61609A657857D3A2B2A4E12D7DB9546221F22
SHA-256:	F321DF4AF5EA5D9AD9D0840C3F6B332567584620EFEDD1FADE186123ABC7479E
SHA-512:	C909842FB4005EC6374563C0F96E39ED77DC4FA20D50A8BBAE08106DFE7B8DA9E9E50D28899A16E7F01F01B924B4E6B3B5139A6013908BC35D1D075E73BC3FDC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn2.editmysite.com/fonts/SQ_Market/sqmarket-medium.woff
Preview:	wOFF.....I.....FFTM.....n.a]GDEF.....K...Z...yGPOS.....$...HL.4..GSUB..&.....OS/2..+I...Y...`.~+Scmap..+.....6...Jcvt .....7..fpgm.....s.Y.7gasp../.....glyf../...`=...t~} .head... ...1...6..p.hhea...T...!...$. .'hmtx...x.....P.F.loca...\.....g.maxp...4... ... ...5name...T.....\...post.....2.....w..prep...H...h....'...webf.....T.....0.....9x...A..0.D.....y.[.s).D.hq.(.....I.M.h.....l/Z.Y.H.dv...'.}S.....p.x...tT.y..]..hA..d....1..c0`..1..P.1.../.O...q...)....%..p..v.1..c.....2.F...a...3..FW.(...}.j.LOS...33.]...,.E.....@..._mz.E..$...}.PLzd...~..U.^....~z.J~.aYB....[/..".N$.8d.pe>w_.....wB./...@m|n.d.'.....?..H...P.2.....^M8.P.89...&..:..H.+_%-Mz=.,Y$OK~:....).).'e[jB..S...I.:..s..;J..yU.0.e...3iO.=..-.....\....'...N..;=.y.....?v.].j.....-./.3{..:...WQ.J/...t=...O..q>...u.Dz.k\.....V....)q.c..|.Q:....m....G..'.3i..H....Ic]..^.IK...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\u-440qyriQwlOrhSvowK_l5-ciZK[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 35696, version 1.1
Category:	downloaded
Size (bytes):	35696
Entropy (8bit):	7.986011105874064

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\u-440qyriQwlOrhSvowK_l5-ciZK[1].woff	
Encrypted:	false
SSDEEP:	768:2WjhRIJYG9geaIgC8Ur9qS24F3f9NhwRZ6PoxET1PqfEYZ4Zn+u/0:2yeJ33vgoDF3frh+k0EYZ4Znv0
MD5:	757EFB349637CD90764BE5A359ACFB05
SHA1:	704672DBC2EF0040E47402312F88D4022B965A2C
SHA-256:	29787613DF0C91A5319324070310E4376B956CEB10EACCA23694EAE398902325
SHA-512:	808A171CD37B35FDD2F53FAC7DDDE3C8C9B7C9DC51E9C17529A34C5D67D73DAC42A4EBE32E3C00CEB430C28AAB1813221E7412AEBF83589CE7F34076056D(4B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/merriweather/v22/u-440qyriQwlOrhSvowK_l5-ciZK.woff
Preview:	wOFF.....p.....d.....GDEF.....GPOS..... ... DvLuGSUB...4.....dW.O.OS/2... ...Q...`U..Kcmap...t.....|"$.$cvt ...L...8.....~.lfpgm.....F...mA..|gasp..... ....glyf.....lt...t.ZT.head..{H...6...6.).7hhea..{.... ...$...}hmtx..{....G.....?2loca..~.....*...maxp..... ... .c.pname.....r:.Q.post.....Xprep.....Z.,.x...CV...E..3..v.l..0l 7... ^L\F.e....\.D...d.D$".$.b".b_J.....A..(c~.i?gb.%.._g....M.s...W..;.....~.P..P..W.OV..S./P./R..U.oV'.....DFLT.....x.....a.D..m.6..m..X.Y.nl..b....>..]....$. sn.N.9.9.....O..-..2.....i..4.+....L/.S..d.).+Y:mi.....E.+..t.J..._.j..y...FpH...K>...QEk.=2(...(.dRB..Q...Z:..@6e....Dr(...('.K..tG9.<*i.....p<.yt.6M.....q....o\j\m.h.n.k<l<y...:....dL 6.....kt.2zF.H..l....K..Q...FpH...\..(..T.....B..../D.<..x\.....-.}...H@./.ze.h..j.....0...m.&m...k.vj.v#...6.....03Y.n<...j.....:e.lgL..h'.:....u:jqv\.s...Q.G...:n%..>

C:\Users\user\AppData\Local\Temp\~DF298FB71CE0182D5F.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.27918767598683664
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laA:kBqoxxJhHWSVSEab
MD5:	AB889A32AB9ACD33E816C2422337C69A
SHA1:	1190C6B34DED2D295827C2A88310D10A8B90B59B
SHA-256:	4D6EC54B8D244E63B0F04FBE2B97402A3DF722560AD12F218665BA440F4CEFDA
SHA-512:	BD250855747BB4CEC61814D0E44F810156D390E3E9F120A12935EFDF80ACA33C4777AD66257CCA4E4003FEF0741692894980B9298F01C4CDD2D8A9C7BB522FB
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFDA317FA3CDAE8B78.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.47550222343239845
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lo+9lou9lWud+GXk:kBqoIZvud+GXk
MD5:	3E3AB2C466E0884CC6A55A63E3FA8264
SHA1:	A6104C16A8F0EAE6171A54C2015A95FCA7F6CADC
SHA-256:	58C7B2010042B6509D9C65B6C4513B0FF760D6967C3C4EB50F423A9ED54695B4
SHA-512:	525F364D0074A97722E3631016D3DFDF7D761F9AF181A67F20EBD39AC1AECA628F4407A30F6DC0809F67DEF733372A3A34C2D5827B595008392F49856EB129BB
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFF7C87180A599BF81.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	56205
Entropy (8bit):	1.4537535460983102
Encrypted:	false
SSDEEP:	384:kBqoxKAuqR+CkuH04zux3d3kRFI5mltFI5mRMBI5m5:
MD5:	F6BA6F826895F704A1E2E4CF589C57BB
SHA1:	817935C7F22BC4FD88B722AB0664C1D057D149EB
SHA-256:	FF2E2F2B088C4B72A5071C2512EBD82B53E2E922612A5B4C4D7290E17139681E

C:\Users\user\AppData\Local\Temp\~DFF7C87180A599BF81.TMP

SHA-512:	D165F24F23FE1F1FB1E11B1AEA756EC05BE80137A02C1B2EFD441DBD98B77AE4EB7D4C491230275021317B44D4D4DF570B88D75A18132A8E66C38C68EAD998 B
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Roaming\Macromedia\Flash Player\macromedia.com\support\flashplayer\sys\settings.sxx

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25475
Entropy (8bit):	5.101526115397042
Encrypted:	false
SSDEEP:	384:yrCEF/h+hag5f1SFhUdgEDeIszIjiKlsHV:GQ8h
MD5:	FA9681B9C76FE5BB7D892533E246017D
SHA1:	DCDA75110395193974DDA13268A0446ED5DEE699
SHA-256:	6663DD08486E9E70CFF294C00C756991CE045DD499F44C2FD596FF38B0486063
SHA-512:	F128D5F5AAA4A0CA77755A4706EC750BA5761499F067E6E28345524694D4C76611EF500771C16DCEDA891D5423A390B28A97C5708D41FA6356FEAB89421A873D
Malicious:	false
Reputation:	low
Preview:	.....(TCSO........settings......gain.@I............<TCSO........settings......gain.@I.........echosuppression........STCSO........settings......gain.@I.........echosuppression.....defaultmicrophone.........fTCSO........settings......gain.@I.........echosuppression.....defaultmicrophone......defaultcamera.........xTCSO........settings......gain.@I.........echosuppression.....defaultmicrophone......defaultcamera......defaultaudio..........TCSO........settings......gain.@I.........echosuppression.....defaultmicrophone......defaultcamera......defaultaudio......defaultklimit.@Y............TCSO........settings......gain.@I.........echosuppression.....defaultmicrophone......defaultcamera......defaultaudio......defaultklimit.@Y ....defaultalways.........TCSO........settings......gain.@I.........echosuppression.....defaultmicrophone......defaultcamera......defaultaudio......defaultklimit.@Y.........defaultalways.....windowlessDisable.........TCSO........settings......gain.@I.........echosu

C:\Users\user\AppData\Roaming\Macromedia\Flash Player\openssl\cache\RevocationCacheFile.dat

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	0F343B0931126A20F133D67C2B018A3B
SHA1:	60CACBF3D72E1E7834203DA608037B1BF83B40E8
SHA-256:	5F70BF18A086007016E948B04AED3B82103A36BEA41755B6CDDFAF10ACE3C6EF
SHA-512:	8EFB4F73C5655351C444EB109230C556D39E2C7624E9C11ABC9E3FB4B9B9254218CC5085B454A9698D085CFA92198491F07A723BE4574ADC70617B73EB0B6461
Malicious:	false
Reputation:	low
Preview:	....

Static File Info

No static file info

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 11, 2021 15:13:16.495152950 CEST	192.168.2.4	8.8.8.8	0xbc08	Standard query (0)	stgdjas.simplesite.com	A (IP address)	IN (0x0001)
Jun 11, 2021 15:13:16.956363916 CEST	192.168.2.4	8.8.8.8	0x219c	Standard query (0)	css.simplesite.com	A (IP address)	IN (0x0001)
Jun 11, 2021 15:13:16.977057934 CEST	192.168.2.4	8.8.8.8	0xd974	Standard query (0)	www.simplesite.com	A (IP address)	IN (0x0001)
Jun 11, 2021 15:13:20.486696959 CEST	192.168.2.4	8.8.8.8	0x93b7	Standard query (0)	connect.facebook.net	A (IP address)	IN (0x0001)
Jun 11, 2021 15:13:23.578854084 CEST	192.168.2.4	8.8.8.8	0x40f0	Standard query (0)	fpdownload.macromedia.com	A (IP address)	IN (0x0001)
Jun 11, 2021 15:13:42.831161976 CEST	192.168.2.4	8.8.8.8	0xee2c	Standard query (0)	stgdjas.simplesite.com	A (IP address)	IN (0x0001)
Jun 11, 2021 15:13:45.019718885 CEST	192.168.2.4	8.8.8.8	0x7a15	Standard query (0)	offi4hf.weebly.com	A (IP address)	IN (0x0001)
Jun 11, 2021 15:13:45.800853968 CEST	192.168.2.4	8.8.8.8	0xead9	Standard query (0)	cdn2.editmysite.com	A (IP address)	IN (0x0001)
Jun 11, 2021 15:13:46.745978117 CEST	192.168.2.4	8.8.8.8	0xbb28	Standard query (0)	ec.editmysite.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 11, 2021 15:13:16.557013035 CEST	8.8.8.8	192.168.2.4	0xbc08	No error (0)	stgdjas.simplesite.com		52.222.158.113	A (IP address)	IN (0x0001)
Jun 11, 2021 15:13:16.557013035 CEST	8.8.8.8	192.168.2.4	0xbc08	No error (0)	stgdjas.simplesite.com		52.222.158.124	A (IP address)	IN (0x0001)
Jun 11, 2021 15:13:16.557013035 CEST	8.8.8.8	192.168.2.4	0xbc08	No error (0)	stgdjas.simplesite.com		52.222.158.46	A (IP address)	IN (0x0001)
Jun 11, 2021 15:13:16.557013035 CEST	8.8.8.8	192.168.2.4	0xbc08	No error (0)	stgdjas.simplesite.com		52.222.158.69	A (IP address)	IN (0x0001)
Jun 11, 2021 15:13:17.018676043 CEST	8.8.8.8	192.168.2.4	0x219c	No error (0)	css.simplesite.com		52.222.158.15	A (IP address)	IN (0x0001)
Jun 11, 2021 15:13:17.018676043 CEST	8.8.8.8	192.168.2.4	0x219c	No error (0)	css.simplesite.com		52.222.158.40	A (IP address)	IN (0x0001)
Jun 11, 2021 15:13:17.018676043 CEST	8.8.8.8	192.168.2.4	0x219c	No error (0)	css.simplesite.com		52.222.158.30	A (IP address)	IN (0x0001)
Jun 11, 2021 15:13:17.018676043 CEST	8.8.8.8	192.168.2.4	0x219c	No error (0)	css.simplesite.com		52.222.158.16	A (IP address)	IN (0x0001)
Jun 11, 2021 15:13:17.038773060 CEST	8.8.8.8	192.168.2.4	0xd974	No error (0)	www.simplesite.com		52.222.158.77	A (IP address)	IN (0x0001)
Jun 11, 2021 15:13:17.038773060 CEST	8.8.8.8	192.168.2.4	0xd974	No error (0)	www.simplesite.com		52.222.158.119	A (IP address)	IN (0x0001)
Jun 11, 2021 15:13:17.038773060 CEST	8.8.8.8	192.168.2.4	0xd974	No error (0)	www.simplesite.com		52.222.158.73	A (IP address)	IN (0x0001)
Jun 11, 2021 15:13:17.038773060 CEST	8.8.8.8	192.168.2.4	0xd974	No error (0)	www.simplesite.com		52.222.158.84	A (IP address)	IN (0x0001)
Jun 11, 2021 15:13:20.550034046 CEST	8.8.8.8	192.168.2.4	0x93b7	No error (0)	connect.facebook.net	scontent.xx.fbcdn.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 15:13:20.550034046 CEST	8.8.8.8	192.168.2.4	0x93b7	No error (0)	scontent.xx.fbcdn.net		31.13.92.14	A (IP address)	IN (0x0001)
Jun 11, 2021 15:13:23.644087076 CEST	8.8.8.8	192.168.2.4	0x40f0	No error (0)	fpdownload.macromedia.com	fpdownload.macromedia.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 11, 2021 15:13:42.894977093 CEST	8.8.8.8	192.168.2.4	0xee2c	No error (0)	stgdjas.simplesite.com		52.222.158.69	A (IP address)	IN (0x0001)
Jun 11, 2021 15:13:42.894977093 CEST	8.8.8.8	192.168.2.4	0xee2c	No error (0)	stgdjas.simplesite.com		52.222.158.113	A (IP address)	IN (0x0001)
Jun 11, 2021 15:13:42.894977093 CEST	8.8.8.8	192.168.2.4	0xee2c	No error (0)	stgdjas.simplesite.com		52.222.158.46	A (IP address)	IN (0x0001)
Jun 11, 2021 15:13:42.894977093 CEST	8.8.8.8	192.168.2.4	0xee2c	No error (0)	stgdjas.simplesite.com		52.222.158.124	A (IP address)	IN (0x0001)
Jun 11, 2021 15:13:45.085427046 CEST	8.8.8.8	192.168.2.4	0x7a15	No error (0)	offi4hf.weebly.com	pages-wildcard.weebly.com		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 15:13:45.085427046 CEST	8.8.8.8	192.168.2.4	0x7a15	No error (0)	pages-wildcard.weebly.com		199.34.228.53	A (IP address)	IN (0x0001)
Jun 11, 2021 15:13:45.085427046 CEST	8.8.8.8	192.168.2.4	0x7a15	No error (0)	pages-wildcard.weebly.com		199.34.228.54	A (IP address)	IN (0x0001)
Jun 11, 2021 15:13:45.864274979 CEST	8.8.8.8	192.168.2.4	0xead9	No error (0)	cdn2.editmysite.com	weebly.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 15:13:45.864274979 CEST	8.8.8.8	192.168.2.4	0xead9	No error (0)	weebly.map.fastly.net		151.101.1.46	A (IP address)	IN (0x0001)
Jun 11, 2021 15:13:45.864274979 CEST	8.8.8.8	192.168.2.4	0xead9	No error (0)	weebly.map.fastly.net		151.101.65.46	A (IP address)	IN (0x0001)
Jun 11, 2021 15:13:45.864274979 CEST	8.8.8.8	192.168.2.4	0xead9	No error (0)	weebly.map.fastly.net		151.101.129.46	A (IP address)	IN (0x0001)
Jun 11, 2021 15:13:45.864274979 CEST	8.8.8.8	192.168.2.4	0xead9	No error (0)	weebly.map.fastly.net		151.101.193.46	A (IP address)	IN (0x0001)
Jun 11, 2021 15:13:46.807612896 CEST	8.8.8.8	192.168.2.4	0xbb28	No error (0)	ec.editmysite.com	sp-2020021412301152490000000a-1069308460.us-west-2.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 15:13:46.807612896 CEST	8.8.8.8	192.168.2.4	0xbb28	No error (0)	sp-2020021412301152490000000a-1069308460.us-west-2.elb.amazonaws.com		52.43.249.183	A (IP address)	IN (0x0001)
Jun 11, 2021 15:13:46.807612896 CEST	8.8.8.8	192.168.2.4	0xbb28	No error (0)	sp-2020021412301152490000000a-1069308460.us-west-2.elb.amazonaws.com		44.241.96.221	A (IP address)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jun 11, 2021 15:13:16.688095093 CEST	52.222.158.113	443	192.168.2.4	49721	CN=*.simplesite.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Fri May 21 02:00:00 CEST 2021 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Mon Jun 20 01:59:59 CEST 2022 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	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=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Jun 11, 2021 15:13:16.688679934 CEST	52.222.158.113	443	192.168.2.4	49720	CN=*.simplesite.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Fri May 21 02:00:00 CEST 2021 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Mon Jun 20 01:59:59 CEST 2022 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	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=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Jun 11, 2021 15:13:17.132047892 CEST	52.222.158.15	443	192.168.2.4	49723	CN=*.simplesite.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Fri May 21 02:00:00 CEST 2021 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Mon Jun 20 01:59:59 CEST 2022 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	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=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Jun 11, 2021 15:13:17.133692026 CEST	52.222.158.15	443	192.168.2.4	49725	CN=*.simplesite.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Fri May 21 02:00:00 CEST 2021 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Mon Jun 20 01:59:59 CEST 2022 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	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=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Jun 11, 2021 15:13:17.134565115 CEST	52.222.158.15	443	192.168.2.4	49724	CN=*.simplesite.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Fri May 21 02:00:00 CEST 2021 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Mon Jun 20 01:59:59 CEST 2022 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	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=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Jun 11, 2021 15:13:17.148233891 CEST	52.222.158.77	443	192.168.2.4	49726	CN=*.simplesite.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Fri May 21 02:00:00 CEST 2021 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Mon Jun 20 01:59:59 CEST 2022 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	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=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Jun 11, 2021 15:13:17.148451090 CEST	52.222.158.77	443	192.168.2.4	49727	CN=*.simplesite.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Fri May 21 02:00:00 CEST 2021 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Mon Jun 20 01:59:59 CEST 2022 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	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=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jun 11, 2021 15:13:20.639504910 CEST	31.13.92.14	443	192.168.2.4	49738	CN=*.facebook.com, O="Facebook, Inc.", L=Menlo Park, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed May 26 02:00:00 CEST 2021 Tue Oct 22 14:00:00 CEST 2013	Wed Aug 25 01:59:59 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Jun 11, 2021 15:13:20.640028000 CEST	31.13.92.14	443	192.168.2.4	49737	CN=*.facebook.com, O="Facebook, Inc.", L=Menlo Park, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed May 26 02:00:00 CEST 2021 Tue Oct 22 14:00:00 CEST 2013	Wed Aug 25 01:59:59 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Jun 11, 2021 15:13:45.467613935 CEST	199.34.228.53	443	192.168.2.4	49755	CN=*.weebly.com CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Oct 04 02:00:00 CEST 2019 Mon Nov 06 13:23:33 CET 2017	Thu Dec 02 13:00:00 CET 2021 Sat Nov 06 13:23:33 CET 2027	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=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:33 CET 2017	Sat Nov 06 13:23:33 CET 2027		
Jun 11, 2021 15:13:45.467792034 CEST	199.34.228.53	443	192.168.2.4	49756	CN=*.weebly.com CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Oct 04 02:00:00 CEST 2019 Mon Nov 06 13:23:33 CET 2017	Thu Dec 02 13:00:00 CET 2021 Sat Nov 06 13:23:33 CET 2027	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=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:33 CET 2017	Sat Nov 06 13:23:33 CET 2027		
Jun 11, 2021 15:13:45.960951090 CEST	151.101.1.46	443	192.168.2.4	49761	CN=*.editmysite.com CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue May 11 01:04:12 CEST 2021 Tue Jul 28 02:00:00 CEST 2020	Sun Jun 12 01:04:11 CEST 2022 Sun Mar 18 01:00:00 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Jul 28 02:00:00 CEST 2020	Sun Mar 18 01:00:00 CET 2029		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jun 11, 2021 15:13:45.979357958 CEST	151.101.1.46	443	192.168.2.4	49765	CN=*.editmysite.com CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue May 11 01:04:12 CEST 2021	Sun Jun 12 01:04:11 CEST 2022	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Jul 28 02:00:00 CEST 2020	Sun Mar 18 01:00:00 CET 2029		
Jun 11, 2021 15:13:45.979705095 CEST	151.101.1.46	443	192.168.2.4	49762	CN=*.editmysite.com CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue May 11 01:04:12 CEST 2021	Sun Jun 12 01:04:11 CEST 2022	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Jul 28 02:00:00 CEST 2020	Sun Mar 18 01:00:00 CET 2029		
Jun 11, 2021 15:13:45.979904890 CEST	151.101.1.46	443	192.168.2.4	49764	CN=*.editmysite.com CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue May 11 01:04:12 CEST 2021	Sun Jun 12 01:04:11 CEST 2022	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Jul 28 02:00:00 CEST 2020	Sun Mar 18 01:00:00 CET 2029		
Jun 11, 2021 15:13:45.981703043 CEST	151.101.1.46	443	192.168.2.4	49766	CN=*.editmysite.com CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue May 11 01:04:12 CEST 2021	Sun Jun 12 01:04:11 CEST 2022	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Jul 28 02:00:00 CEST 2020	Sun Mar 18 01:00:00 CET 2029		
Jun 11, 2021 15:13:45.981750965 CEST	151.101.1.46	443	192.168.2.4	49763	CN=*.editmysite.com CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue May 11 01:04:12 CEST 2021	Sun Jun 12 01:04:11 CEST 2022	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Jul 28 02:00:00 CEST 2020	Sun Mar 18 01:00:00 CET 2029		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jun 11, 2021 15:13:46.238533974 CEST	199.34.228.53	443	192.168.2.4	49757	CN=*.weebly.com CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Oct 04 02:00:00 CEST 2019 Mon Nov 06 13:23:33 CET 2017	Thu Dec 02 13:00:00 CET 2021 Sat Nov 06 13:23:33 CET 2027	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=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:33 CET 2017	Sat Nov 06 13:23:33 CET 2027		
Jun 11, 2021 15:13:46.239187956 CEST	199.34.228.53	443	192.168.2.4	49758	CN=*.weebly.com CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Oct 04 02:00:00 CEST 2019 Mon Nov 06 13:23:33 CET 2017	Thu Dec 02 13:00:00 CET 2021 Sat Nov 06 13:23:33 CET 2027	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=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:33 CET 2017	Sat Nov 06 13:23:33 CET 2027		
Jun 11, 2021 15:13:46.239367008 CEST	199.34.228.53	443	192.168.2.4	49759	CN=*.weebly.com CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Oct 04 02:00:00 CEST 2019 Mon Nov 06 13:23:33 CET 2017	Thu Dec 02 13:00:00 CET 2021 Sat Nov 06 13:23:33 CET 2027	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=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:33 CET 2017	Sat Nov 06 13:23:33 CET 2027		
Jun 11, 2021 15:13:46.242366076 CEST	199.34.228.53	443	192.168.2.4	49760	CN=*.weebly.com CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Oct 04 02:00:00 CEST 2019 Mon Nov 06 13:23:33 CET 2017	Thu Dec 02 13:00:00 CET 2021 Sat Nov 06 13:23:33 CET 2027	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=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:33 CET 2017	Sat Nov 06 13:23:33 CET 2027		
Jun 11, 2021 15:13:47.219300032 CEST	52.43.249.183	443	192.168.2.4	49771	CN=ec.editmysite.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 09 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Sat Oct 09 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	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=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Jun 11, 2021 15:13:47.219492912 CEST	52.43.249.183	443	192.168.2.4	49772	CN=ec.editmysite.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 09 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Sat Oct 09 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	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=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 5856 Parent PID: 800

General

Start time:	15:13:14
Start date:	11/06/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff75b020000
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

Show Windows behavior

Registry Activities

Show Windows behavior

Analysis Process: iexplore.exe PID: 5828 Parent PID: 5856

General

Start time:	15:13:15
Start date:	11/06/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5856 CREDAT:17410 /prefetch:2
Imagebase:	0x1e0000
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

Show Windows behavior

Registry Activities

Show Windows behavior

Disassembly