

JOeSandbox Cloud BASIC



**ID:** 236664

**Cookbook:** browseurl.jbs

**Time:** 21:18:46

**Date:** 08/06/2020

**Version:** 29.0.0 Ocean Jasper

## Table of Contents

Table of Contents	2
Analysis Report <a href="http://url7220.caapvisio.com/ls/click?upn=U5wBbtTMlgqzyFeoDeLr9oYI88rjnJDkdB-2FOqe4mjsPWQeP8r8RzDIgeUom6oe-2FaiU7o_DC4y3DdDCeEScwRgaDHqvVGy56gjIVzN-2FR6WAJbPzoldJWWMS5Nkfg9TStdNBwzzNXg19pf8z0ZDZc9DdeYbjXBEzOUQDtj5Y6qNaHhwy8a1GmmWUfNIKQdV5jNi2FPYjImpPgGMNcOKDnCFRzE-2BtIPuEuW9HL8vR8Wt5eD4RcdD-2FKL22gop-2FvXlzeVJxcDVXnSCieFHQtGOL7OWAFTFIEIOVBANnwHDrwyLzxVtqL2xBsu9e2Yuuq6z29wQB7-2FyidJCIZLUne1Rn4dgtxj2S9qSfe47d18pWh0akhpla0oEiNBwjG-2FEerbIB3yotE-2B0rDgEyV1dN7xqp6IWS4wNe2SjpCq-2Bd3KysdMWKgtf9-2Fyx-2Foz6kqZij-2FhoFvYJVLNIXpuCIS14ETkrvFVaSdzrl-2FAFD4CJ0lpN8haTyAlyfzLLUDNIBK2-2FKRqq0VKbmPlaVSI5idyFxaDOg-2FDb8pZJZJ6FP17mdPcFXzud7tUBE0fW1sqj-2BDKXgTJ-2FOP2an5z6KllwnX6tNwnVLzn5RuoJAJMdlmua1AtTqdjip0hnCSda-2FxsdlNP0qciBTe99zuZZYqSuju2N0uix-2BiYqvDE7-2B0Kk0wlbHMZ38a-2BFoXgFH9dWpjZqmaF3RH2OQ-2FgS9WsoMHejqz88SBj0zdDjKSE2ve6qo0veAzLH3FJZZ2OTtnVmvXVTWOnTxVMCuDNo0gTLg9c45S1XgyV4CrH8AZF7E 2BTHkpNEnAQFWWIFbiMXHPUwOXqBoNH9gEhqsF-2FNHoPURLLGoeaBgxQhPYPf7ALCwTbW96GnOGSqZnKLcZo-2FIt2D-2B1qWVvm1I392O1TAT2xXs7f173Pd6IPoXclYuMXEjSwascmy5p6x6Aa7iw3NUDri7YF0">http://url7220.caapvisio.com/ls/click?upn=U5wBbtTMlgqzyFeoDeLr9oYI88rjnJDkdB-2FOqe4mjsPWQeP8r8RzDIgeUom6oe-2FaiU7o_DC4y3DdDCeEScwRgaDHqvVGy56gjIVzN-2FR6WAJbPzoldJWWMS5Nkfg9TStdNBwzzNXg19pf8z0ZDZc9DdeYbjXBEzOUQDtj5Y6qNaHhwy8a1GmmWUfNIKQdV5jNi2FPYjImpPgGMNcOKDnCFRzE-2BtIPuEuW9HL8vR8Wt5eD4RcdD-2FKL22gop-2FvXlzeVJxcDVXnSCieFHQtGOL7OWAFTFIEIOVBANnwHDrwyLzxVtqL2xBsu9e2Yuuq6z29wQB7-2FyidJCIZLUne1Rn4dgtxj2S9qSfe47d18pWh0akhpla0oEiNBwjG-2FEerbIB3yotE-2B0rDgEyV1dN7xqp6IWS4wNe2SjpCq-2Bd3KysdMWKgtf9-2Fyx-2Foz6kqZij-2FhoFvYJVLNIXpuCIS14ETkrvFVaSdzrl-2FAFD4CJ0lpN8haTyAlyfzLLUDNIBK2-2FKRqq0VKbmPlaVSI5idyFxaDOg-2FDb8pZJZJ6FP17mdPcFXzud7tUBE0fW1sqj-2BDKXgTJ-2FOP2an5z6KllwnX6tNwnVLzn5RuoJAJMdlmua1AtTqdjip0hnCSda-2FxsdlNP0qciBTe99zuZZYqSuju2N0uix-2BiYqvDE7-2B0Kk0wlbHMZ38a-2BFoXgFH9dWpjZqmaF3RH2OQ-2FgS9WsoMHejqz88SBj0zdDjKSE2ve6qo0veAzLH3FJZZ2OTtnVmvXVTWOnTxVMCuDNo0gTLg9c45S1XgyV4CrH8AZF7E 2BTHkpNEnAQFWWIFbiMXHPUwOXqBoNH9gEhqsF-2FNHoPURLLGoeaBgxQhPYPf7ALCwTbW96GnOGSqZnKLcZo-2FIt2D-2B1qWVvm1I392O1TAT2xXs7f173Pd6IPoXclYuMXEjSwascmy5p6x6Aa7iw3NUDri7YF0</a>	3
Overview	3
General Information	3
Detection	3
Signatures	3
Classification	3
Startup	3
Malware Configuration	3
Yara Overview	3
Sigma Overview	3
Signature Overview	3
AV Detection:	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	7
URLs	7
Domains and IPs	9
Contacted Domains	9
URLs from Memory and Binaries	9
Contacted IPs	11
Public	12
General Information	12
Simulations	14
Behavior and APIs	14
Joe Sandbox View / Context	14
IPs	14
Domains	14
ASN	14
JA3 Fingerprints	14
Dropped Files	14
Created / dropped Files	14
Static File Info	45
No static file info	45
Network Behavior	45
Network Port Distribution	45
TCP Packets	45
UDP Packets	47
DNS Queries	47
DNS Answers	48
HTTP Request Dependency Graph	48
HTTP Packets	48
HTTPS Packets	48
Code Manipulations	49
Statistics	49
Behavior	49
System Behavior	49
Analysis Process: iexplore.exe PID: 5436 Parent PID: 700	50
General	50
File Activities	50
Registry Activities	50
Analysis Process: iexplore.exe PID: 5580 Parent PID: 5436	50
General	50
File Activities	50
Registry Activities	51
Disassembly	51

# Analysis Report <http://url7220.caapvisio.com/ls/click?up...>

## Overview

### General Information

Sample URL:

<http://url7220.caapvisio.com/ls/click>

Most interesting Screenshot:

### Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

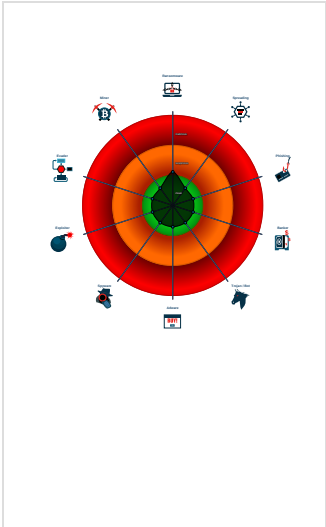
Score:	56
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

### Signatures

Antivirus detection for URL or domain

Multi AV Scanner detection for doma...

### Classification



## Startup

- System is w10x64
- iexplore.exe (PID: 5436 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5580 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5436 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- cleanup

## Malware Configuration

No configs have been found

## Yara Overview

No yara matches

## Sigma Overview

No Sigma rule has matched

## Signature Overview

- AV Detection
- Networking
- System Summary



Click to jump to signature section

AV Detection:



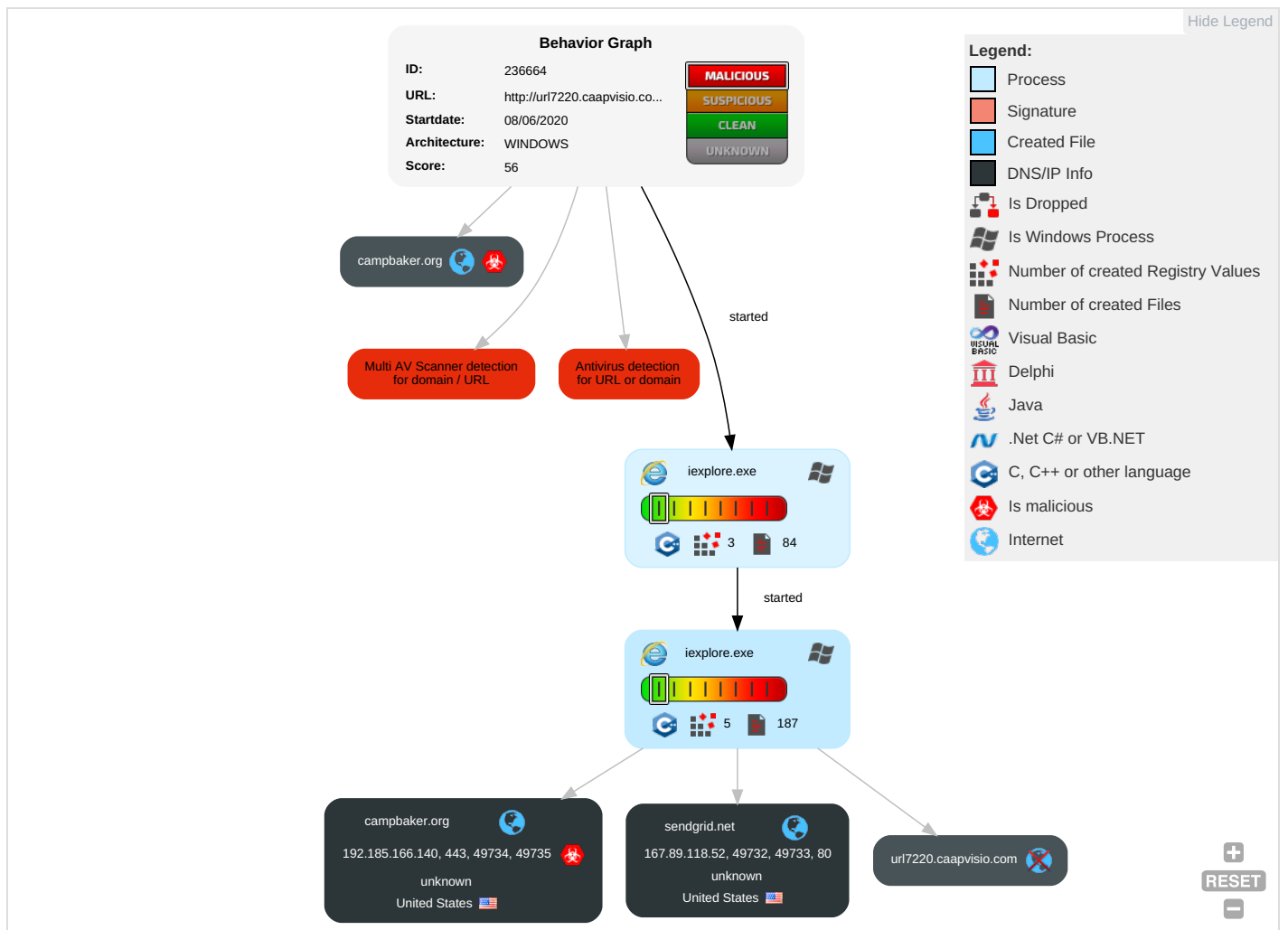
Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

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
Valid Accounts	Graphical User Interface 1	Winlogon Helper DLL	Process Injection 1	Masquerading 1	Credential Dumping	File and Directory Discovery 1	Remote File Copy 1	Data from Local System	Data Compressed	Standard Cryptographic Protocol 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization
Replication Through Removable Media	Service Execution	Port Monitors	Accessibility Features	Process Injection 1	Network Sniffing	Application Window Discovery	Remote Services	Data from Removable Media	Exfiltration Over Other Network Medium	Standard Non-Application Layer Protocol 2	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization
External Remote Services	Windows Management Instrumentation	Accessibility Features	Path Interception	Rootkit	Input Capture	Query Registry	Windows Remote Management	Data from Network Shared Drive	Automated Exfiltration	Standard Application Layer Protocol 3	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups
Drive-by Compromise	Scheduled Task	System Firmware	DLL Search Order Hijacking	Obfuscated Files or Information	Credentials in Files	System Network Configuration Discovery	Logon Scripts	Input Capture	Data Encrypted	Remote File Copy 1	SIM Card Swap	

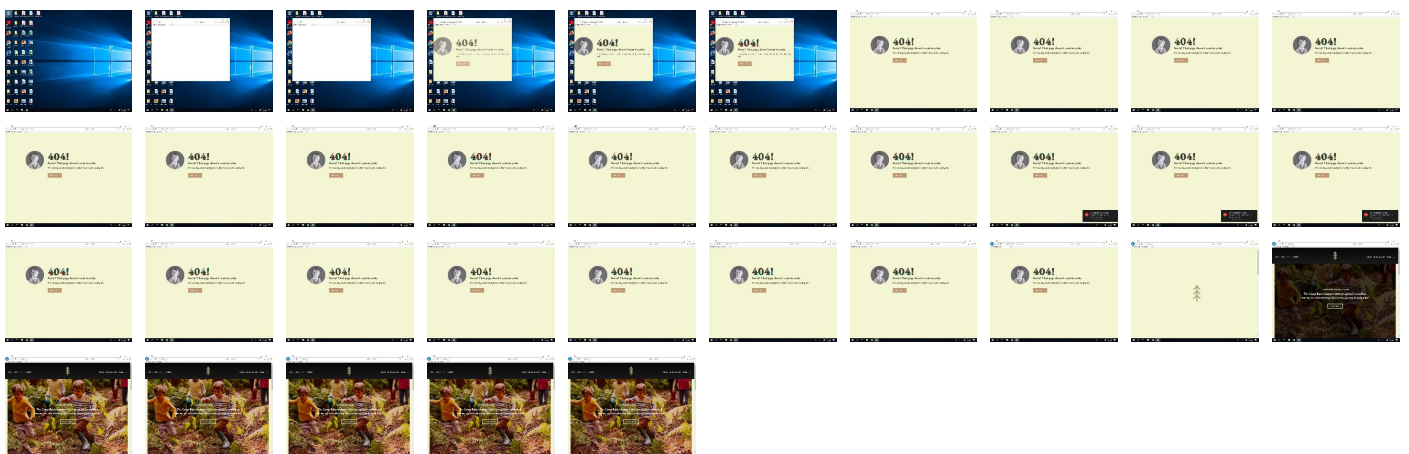
Behavior Graph

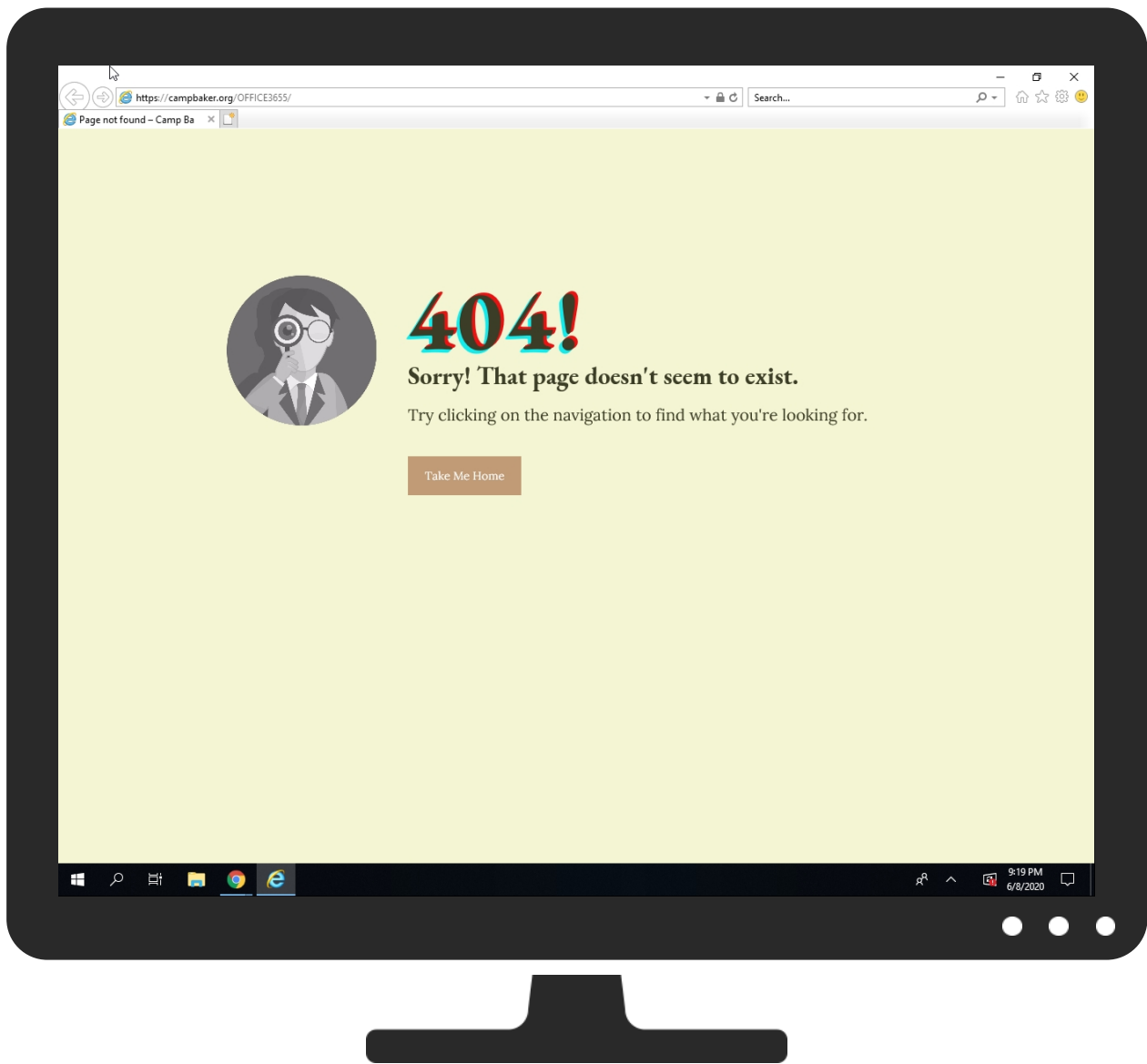


## Screenshots

### 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
<a href="http://url7220.caapvisio.com/ls/click?upn=U5wBbtTMIgqzyFeoDeLr9oYI88rjnJDKdB-2FOqe4mjsPWQeP8r8RzDIgeUom6oe-2FaiU7o_DC4y3DdDCeEScwRgaDHqvVGy56gjlVzN-2FR6WAJbPzolndJWWMS5Nkfg9TStdNBwzzNXg19pf8z0ZDzc9DdeYbjXBEzOUQDjt5Y6qNaHhwy8a1GmmWUfNIKQdV5jNijS-2FPYjImpGgMNCOKDnCFRzE-2BtlPuEuW9HL8vR8Wt5eD4RcdD-2FKL22gop-2FvXlzeVJxcDVXnSCieFHQtG0L7OWAFTFIEIOVBANnwHDwylLzxVtqL2xBSu9e2Yuuq6z29wQB7-2FyidJCIZLUne1Rn4dgbxj2S9qSfe47d18pWh0akhpla0oEinBwjG-2FEerblB3yotE-2B0rDgEyV1dN7xqp6lWS4wNe2SjpCq-2Bd3KysdMWKgtf9-2Fyx-2Foz6kqZij-2FhoFvYJVLNIXpuCIS14ETkrvFVaSdzrl-2FAFD4CJ0lpN8haTyAlyfzLLUDNibK2-2FKRqQ0VKbmPlaVSI5idyFxaDOg-2FDb8pZjZJ6FP17mdPcFXzud7tUBE0fw1sqj-2BDKXgTJ-2Fop2an5z6KIwnX6tNwnVLzn5RuoAJjMdlmua1AtTqdjip0hnCSda-2FxsdlNP0qciBTe99zuZZYqSuju2N0uix-2BiYqvDE7-2B0Kk0wlbHMZ38a-2BFoXgFH9dWpjZqmaF3RH2OQ-2FgS9WsoMHejqz88SBj0zdDjKSE2ve6qo0veAzLH3FJZZ2OTnVmvXVTWOnTxVMCuDNo0gTLg9c45S1XgyV4CrH8AZF7EpWJOXWtZ9Cg9pggyJJg5JsPeixq93R4KOGlRsu6RLWPepjvN4KUBwpagxkw003fyVu9GcSgjiCUnNq9-2BTHkpNEnAQFWWIFbIMXHPUwOXqBoNH9gEhqsF-2FNHoPURLLGoeaBgxQhPYYPf7ALCwTbW96GnOGSqZnKLcZo-2FIt2D-2B1qWVvm1i392O1TAT2xXs7f173Pd6IPoXclYuMXEjSwascmy5p6x6Aa7iw3NUDri7YF0">http://url7220.caapvisio.com/ls/click?upn=U5wBbtTMIgqzyFeoDeLr9oYI88rjnJDKdB-2FOqe4mjsPWQeP8r8RzDIgeUom6oe-2FaiU7o_DC4y3DdDCeEScwRgaDHqvVGy56gjlVzN-2FR6WAJbPzolndJWWMS5Nkfg9TStdNBwzzNXg19pf8z0ZDzc9DdeYbjXBEzOUQDjt5Y6qNaHhwy8a1GmmWUfNIKQdV5jNijS-2FPYjImpGgMNCOKDnCFRzE-2BtlPuEuW9HL8vR8Wt5eD4RcdD-2FKL22gop-2FvXlzeVJxcDVXnSCieFHQtG0L7OWAFTFIEIOVBANnwHDwylLzxVtqL2xBSu9e2Yuuq6z29wQB7-2FyidJCIZLUne1Rn4dgbxj2S9qSfe47d18pWh0akhpla0oEinBwjG-2FEerblB3yotE-2B0rDgEyV1dN7xqp6lWS4wNe2SjpCq-2Bd3KysdMWKgtf9-2Fyx-2Foz6kqZij-2FhoFvYJVLNIXpuCIS14ETkrvFVaSdzrl-2FAFD4CJ0lpN8haTyAlyfzLLUDNibK2-2FKRqQ0VKbmPlaVSI5idyFxaDOg-2FDb8pZjZJ6FP17mdPcFXzud7tUBE0fw1sqj-2BDKXgTJ-2Fop2an5z6KIwnX6tNwnVLzn5RuoAJjMdlmua1AtTqdjip0hnCSda-2FxsdlNP0qciBTe99zuZZYqSuju2N0uix-2BiYqvDE7-2B0Kk0wlbHMZ38a-2BFoXgFH9dWpjZqmaF3RH2OQ-2FgS9WsoMHejqz88SBj0zdDjKSE2ve6qo0veAzLH3FJZZ2OTnVmvXVTWOnTxVMCuDNo0gTLg9c45S1XgyV4CrH8AZF7EpWJOXWtZ9Cg9pggyJJg5JsPeixq93R4KOGlRsu6RLWPepjvN4KUBwpagxkw003fyVu9GcSgjiCUnNq9-2BTHkpNEnAQFWWIFbIMXHPUwOXqBoNH9gEhqsF-2FNHoPURLLGoeaBgxQhPYYPf7ALCwTbW96GnOGSqZnKLcZo-2FIt2D-2B1qWVvm1i392O1TAT2xXs7f173Pd6IPoXclYuMXEjSwascmy5p6x6Aa7iw3NUDri7YF0</a>	0%	Avira URL Cloud	safe	

### Dropped Files

No Antivirus matches

### Unpacked PE Files

No Antivirus matches

## Domains

Source	Detection	Scanner	Label	Link
campbaker.org	6%	Virustotal		<a href="#">Browse</a>
campbaker.org	100%	Google Safe Browsing	phishing	
url7220.caapvisio.com	2%	Virustotal		<a href="#">Browse</a>

## URLs

Source	Detection	Scanner	Label	Link
<a href="https://campbaker.org/wp-content/uploads/2019/04/hale-partner-logo.png">https://campbaker.org/wp-content/uploads/2019/04/hale-partner-logo.png</a>	100%	Google Safe Browsing	phishing	
<a href="https://campbaker.org/wp-includes/js/jquery/jquery-migrate.min.js?ver=1.4.1">https://campbaker.org/wp-includes/js/jquery/jquery-migrate.min.js?ver=1.4.1</a>	100%	Google Safe Browsing	phishing	
<a href="http://www.jacobward.co.uk">http://www.jacobward.co.uk</a>	0%	Avira URL Cloud	safe	
<a href="https://campbaker.org/job/graduate-counselor/">https://campbaker.org/job/graduate-counselor/</a>	100%	Google Safe Browsing	phishing	
<a href="https://campbaker.org/wp-includes/css/dist/block-library/style.min.css?ver=5.4.1">https://campbaker.org/wp-includes/css/dist/block-library/style.min.css?ver=5.4.1</a>	100%	Google Safe Browsing	phishing	
<a href="https://campbaker.org/wp-content/plugins/woocommerce/assets/js/frontend/woocommerce.min.js?ver=4.1.1">https://campbaker.org/wp-content/plugins/woocommerce/assets/js/frontend/woocommerce.min.js?ver=4.1.1</a>	100%	Google Safe Browsing	phishing	
<a href="http://adomas.org/javascript-mouse-wheel/">http://adomas.org/javascript-mouse-wheel/</a>	5%	Virustotal		<a href="#">Browse</a>
<a href="http://adomas.org/javascript-mouse-wheel/">http://adomas.org/javascript-mouse-wheel/</a>	0%	Avira URL Cloud	safe	
<a href="https://campbaker.org/job/undergraduate-counselor/">https://campbaker.org/job/undergraduate-counselor/</a>	100%	Google Safe Browsing	phishing	
<a href="https://campbaker.org/wp-content/themes/diwine/images/up-arrow-2.svg">https://campbaker.org/wp-content/themes/diwine/images/up-arrow-2.svg</a>	100%	Google Safe Browsing	phishing	
<a href="https://campbaker.org/wp-content/plugins/booking/js/datepick/jquery.datepick.js?ver=1.1">https://campbaker.org/wp-content/plugins/booking/js/datepick/jquery.datepick.js?ver=1.1</a>	100%	Google Safe Browsing	phishing	
<a href="https://campbaker.org/wp-content/plugins/booking/assets/libs/bootstrap/css/bootstrap-theme.css?ver=3">https://campbaker.org/wp-content/plugins/booking/assets/libs/bootstrap/css/bootstrap-theme.css?ver=3</a>	100%	Google Safe Browsing	phishing	
<a href="https://campbaker.org/wp-content/plugins/wp-job-manager-applications/assets/css/frontend.css?ver=5.4">https://campbaker.org/wp-content/plugins/wp-job-manager-applications/assets/css/frontend.css?ver=5.4</a>	100%	Google Safe Browsing	phishing	
<a href="https://campbaker.org/wp-content/uploads/2019/05/camp-baker-hero-slide2.jpg">https://campbaker.org/wp-content/uploads/2019/05/camp-baker-hero-slide2.jpg</a>	100%	Google Safe Browsing	phishing	
<a href="https://campbaker.org/wp-content/plugins/mp-timetable/media/css/style.css?ver=2.3.11">https://campbaker.org/wp-content/plugins/mp-timetable/media/css/style.css?ver=2.3.11</a>	100%	Google Safe Browsing	phishing	
<a href="https://campbaker.org/wp-content/themes/diwine/scripts/vendor/date-time/date-time-picker.js">https://campbaker.org/wp-content/themes/diwine/scripts/vendor/date-time/date-time-picker.js</a>	100%	Google Safe Browsing	phishing	
<a href="https://campbaker.org/wp-content/themes/diwine/scripts/vendor/fancybox/jquery.fancybox.css?ver=5.4.1">https://campbaker.org/wp-content/themes/diwine/scripts/vendor/fancybox/jquery.fancybox.css?ver=5.4.1</a>	100%	Google Safe Browsing	phishing	
<a href="https://campbaker.org/wp-content/plugins/revslider/public/assets/css/settings.css?ver=5.4.8.2">https://campbaker.org/wp-content/plugins/revslider/public/assets/css/settings.css?ver=5.4.8.2</a>	100%	Google Safe Browsing	phishing	
<a href="https://wpbakery.com">https://wpbakery.com</a>	0%	Avira URL Cloud	safe	
<a href="https://campbaker.org/team/">https://campbaker.org/team/</a>	100%	Google Safe Browsing	phishing	
<a href="http://getbootstrap.com">http://getbootstrap.com</a>	0%	Avira URL Cloud	safe	
<a href="https://campbaker.org/wp-content/themes/diwine/css/style-classic-menu.css?ver=5.4.1">https://campbaker.org/wp-content/themes/diwine/css/style-classic-menu.css?ver=5.4.1</a>	100%	Google Safe Browsing	phishing	
<a href="https://campbaker.org/wp-content/uploads/2019/03/cropped-camp-baker-icon-270x270.png">https://campbaker.org/wp-content/uploads/2019/03/cropped-camp-baker-icon-270x270.png</a>	100%	Google Safe Browsing	phishing	
<a href="https://campbaker.org/wp-includes/js/jquery/ui/datepicker.min.js?ver=1.11.4">https://campbaker.org/wp-includes/js/jquery/ui/datepicker.min.js?ver=1.11.4</a>	100%	Google Safe Browsing	phishing	
<a href="https://campbaker.org/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fcampbaker.org%2F">https://campbaker.org/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fcampbaker.org%2F</a>	100%	Google Safe Browsing	phishing	
<a href="https://campbaker.org/parent-nights/">https://campbaker.org/parent-nights/</a>	100%	Google Safe Browsing	phishing	
<a href="https://campbaker.org/wp-content/themes/diwine/style.css?ver=5.4.1">https://campbaker.org/wp-content/themes/diwine/style.css?ver=5.4.1</a>	100%	Google Safe Browsing	phishing	
<a href="https://campbaker.org/wp-content/uploads/2019/04/donate-today-384x186.jpg">https://campbaker.org/wp-content/uploads/2019/04/donate-today-384x186.jpg</a>	100%	Google Safe Browsing	phishing	
<a href="https://campbaker.org/wp-content/uploads/2019/03/cropped-camp-baker-icon-180x180.png">https://campbaker.org/wp-content/uploads/2019/03/cropped-camp-baker-icon-180x180.png</a>	100%	Google Safe Browsing	phishing	
<a href="http://labs.skinkers.com/touchSwipe/">http://labs.skinkers.com/touchSwipe/</a>	0%	Virustotal		<a href="#">Browse</a>
<a href="http://labs.skinkers.com/touchSwipe/">http://labs.skinkers.com/touchSwipe/</a>	0%	Avira URL Cloud	safe	
<a href="https://campbaker.org/OFFICE3655/6Page">https://campbaker.org/OFFICE3655/6Page</a>	100%	Google Safe Browsing	phishing	
<a href="https://campbaker.org/wp-content/plugins/woocommerce/assets/js/jquery-blockui/jquery.blockUI.min.js?">https://campbaker.org/wp-content/plugins/woocommerce/assets/js/jquery-blockui/jquery.blockUI.min.js?</a>	100%	Google Safe Browsing	phishing	

Source	Detection	Scanner	Label	Link
<a href="http://https://campbaker.org/wp-content/plugins/booking/assets/libs/bootstrap/css/bootstrap.css?ver=3.3.5.1">http://https://campbaker.org/wp-content/plugins/booking/assets/libs/bootstrap/css/bootstrap.css?ver=3.3.5.1</a>	100%	Google Safe Browsing	phishing	
<a href="http://https://campbaker.org/wp-includes/js/imagesloaded.min.js?ver=3.2.0">http://https://campbaker.org/wp-includes/js/imagesloaded.min.js?ver=3.2.0</a>	100%	Google Safe Browsing	phishing	
<a href="http://https://campbaker.org/wp-content/plugins/booking/core/timeline/v2/css/timeline_v2.css?ver=8.7.6">http://https://campbaker.org/wp-content/plugins/booking/core/timeline/v2/css/timeline_v2.css?ver=8.7.6</a>	100%	Google Safe Browsing	phishing	
<a href="http://https://campbaker.org/wp-content/themes/diwine/scripts/vendor/fancybox/jquery.fancybox.pack.js">http://https://campbaker.org/wp-content/themes/diwine/scripts/vendor/fancybox/jquery.fancybox.pack.js</a>	100%	Google Safe Browsing	phishing	
<a href="http://https://campbaker.org/faq/">http://https://campbaker.org/faq/</a>	0%	Virustotal		<a href="#">Browse</a>
<a href="http://https://campbaker.org/faq/">http://https://campbaker.org/faq/</a>	100%	Google Safe Browsing	phishing	
<a href="http://https://campbaker.org/wp-content/themes/diwine/css/flickity.min.css?ver=5.4.1">http://https://campbaker.org/wp-content/themes/diwine/css/flickity.min.css?ver=5.4.1</a>	100%	Google Safe Browsing	phishing	
<a href="http://https://campbaker.org/wp-content/plugins/booked/assets/js/toolipster/css/themes/toolipster-light.c">http://https://campbaker.org/wp-content/plugins/booked/assets/js/toolipster/css/themes/toolipster-light.c</a>	100%	Google Safe Browsing	phishing	
<a href="http://https://campbaker.org/wp-content/uploads/2019/05/camp-baker-footer-logo.png">http://https://campbaker.org/wp-content/uploads/2019/05/camp-baker-footer-logo.png</a>	100%	Google Safe Browsing	phishing	
<a href="http://https://campbaker.org/wp-content/themes/diwine/scripts/vendor/snap.svg-min.js">http://https://campbaker.org/wp-content/themes/diwine/scripts/vendor/snap.svg-min.js</a>	100%	Google Safe Browsing	phishing	
<a href="http://https://campbaker.org/comments/feed/">http://https://campbaker.org/comments/feed/</a>	100%	Google Safe Browsing	phishing	
<a href="http://https://campbaker.org/resources/">http://https://campbaker.org/resources/</a>	100%	Google Safe Browsing	phishing	
<a href="http://https://campbaker.org/wp-content/plugins/woocommerce/assets/css/woocommerce.css?ver=4.1.1">http://https://campbaker.org/wp-content/plugins/woocommerce/assets/css/woocommerce.css?ver=4.1.1</a>	100%	Google Safe Browsing	phishing	
<a href="http://https://campbaker.org/wp-content/plugins/booked-frontend-agents/css/styles.css?ver=2.2.6">http://https://campbaker.org/wp-content/plugins/booked-frontend-agents/css/styles.css?ver=2.2.6</a>	100%	Google Safe Browsing	phishing	
<a href="http://https://campbaker.org/wp-content/plugins/woocommerce/assets/js/frontend/cart-fragments.min.js?ver=4.">http://https://campbaker.org/wp-content/plugins/woocommerce/assets/js/frontend/cart-fragments.min.js?ver=4.</a>	100%	Google Safe Browsing	phishing	
<a href="http://https://campbaker.org/wp-content/plugins/booking/core/timeline/v2/css/timeline_skin_v2.css?ver=8.7.6">http://https://campbaker.org/wp-content/plugins/booking/core/timeline/v2/css/timeline_skin_v2.css?ver=8.7.6</a>	100%	Google Safe Browsing	phishing	
<a href="http://https://campbaker.org/wp-content/plugins/woocommerce/packages/woocommerce-blocks/build/style.css?ver">http://https://campbaker.org/wp-content/plugins/woocommerce/packages/woocommerce-blocks/build/style.css?ver</a>	100%	Google Safe Browsing	phishing	
<a href="http://https://campbaker.org/wp-content/plugins/rsvp/rsvp_plugin.css?ver=5.4.1">http://https://campbaker.org/wp-content/plugins/rsvp/rsvp_plugin.css?ver=5.4.1</a>	100%	Google Safe Browsing	phishing	
<a href="http://https://campbaker.org/wp-content/plugins/booking/assets/libs/bootstrap/js/bootstrap.js?ver=3.3.5.1">http://https://campbaker.org/wp-content/plugins/booking/assets/libs/bootstrap/js/bootstrap.js?ver=3.3.5.1</a>	100%	Google Safe Browsing	phishing	
<a href="http://https://campbaker.org/">http://https://campbaker.org/</a>	0%	Virustotal		<a href="#">Browse</a>
<a href="http://https://campbaker.org/">http://https://campbaker.org/</a>	100%	Google Safe Browsing	phishing	
<a href="http://https://campbaker.org/wp-content/plugins/booked/assets/js/toolipster/js/jquery.toolipster.min.js?v">http://https://campbaker.org/wp-content/plugins/booked/assets/js/toolipster/js/jquery.toolipster.min.js?v</a>	100%	Google Safe Browsing	phishing	
<a href="http://https://www.campbaker.org">http://https://www.campbaker.org</a>	100%	Google Safe Browsing	phishing	
<a href="http://https://campbaker.org/wp-content/plugins/booking/css/calendar.css?ver=8.7.6">http://https://campbaker.org/wp-content/plugins/booking/css/calendar.css?ver=8.7.6</a>	100%	Google Safe Browsing	phishing	
<a href="http://https://campbaker.org/wp-content/plugins/woocommerce/assets/css/woocommerce-layout.css?ver=4.1.1">http://https://campbaker.org/wp-content/plugins/woocommerce/assets/css/woocommerce-layout.css?ver=4.1.1</a>	100%	Google Safe Browsing	phishing	
<a href="http://https://campbaker.org/FICE3655/#contentF">http://https://campbaker.org/FICE3655/#contentF</a>	100%	Google Safe Browsing	phishing	
<a href="http://https://campbaker.org/wp-content/uploads/2019/05/jbcc-logo-white.png">http://https://campbaker.org/wp-content/uploads/2019/05/jbcc-logo-white.png</a>	100%	Google Safe Browsing	phishing	
<a href="http://https://campbaker.org/wp-content/plugins/booked/assets/css/icons.css?ver=2.2.6">http://https://campbaker.org/wp-content/plugins/booked/assets/css/icons.css?ver=2.2.6</a>	100%	Google Safe Browsing	phishing	
<a href="http://https://campbaker.org/wp-includes/js/jquery/jquery.js?ver=1.12.4-wp">http://https://campbaker.org/wp-includes/js/jquery/jquery.js?ver=1.12.4-wp</a>	100%	Google Safe Browsing	phishing	
<a href="http://https://campbaker.org/wp-content/uploads/2019/03/camp-baker-logo-retina.png">http://https://campbaker.org/wp-content/uploads/2019/03/camp-baker-logo-retina.png</a>	100%	Google Safe Browsing	phishing	
<a href="http://https://campbaker.org/wp-content/plugins/booked/assets/js/spin.jquery.js?ver=2.0.1">http://https://campbaker.org/wp-content/plugins/booked/assets/js/spin.jquery.js?ver=2.0.1</a>	100%	Google Safe Browsing	phishing	
<a href="http://https://campbaker.org/wp-content/themes/diwine/scripts/vendor/plugins/nicescroll.js">http://https://campbaker.org/wp-content/themes/diwine/scripts/vendor/plugins/nicescroll.js</a>	100%	Google Safe Browsing	phishing	
<a href="http://https://campbaker.org/wp-content/plugins/booked/assets/css/styles.css?ver=2.2.6">http://https://campbaker.org/wp-content/plugins/booked/assets/css/styles.css?ver=2.2.6</a>	100%	Google Safe Browsing	phishing	
<a href="http://https://campbaker.org/training-opportunities/">http://https://campbaker.org/training-opportunities/</a>	100%	Google Safe Browsing	phishing	
<a href="http://https://campbaker.org/wp-content/plugins/revslider/public/assets/js/jquery.themepunch.revolution.min">http://https://campbaker.org/wp-content/plugins/revslider/public/assets/js/jquery.themepunch.revolution.min</a>	100%	Google Safe Browsing	phishing	
<a href="http://https://campbaker.org/for-campers/">http://https://campbaker.org/for-campers/</a>	100%	Google Safe Browsing	phishing	
<a href="http://https://campbaker.org/wp-content/plugins/js_composer/assets/js/vendors/woocommerce-add-to-cart.js?ve">http://https://campbaker.org/wp-content/plugins/js_composer/assets/js/vendors/woocommerce-add-to-cart.js?ve</a>	100%	Google Safe Browsing	phishing	
<a href="http://https://campbaker.org/wp-content/themes/diwine-child/style.css?ver=5.4.1">http://https://campbaker.org/wp-content/themes/diwine-child/style.css?ver=5.4.1</a>	100%	Google Safe Browsing	phishing	



Source	Detection	Scanner	Label	Link
<a href="http://https://campbaker.org/wp-content/plugins/contact-form-7/includes/js/scripts.js?ver=5.1.9">http://https://campbaker.org/wp-content/plugins/contact-form-7/includes/js/scripts.js?ver=5.1.9</a>	100%	Google Safe Browsing	phishing	
<a href="http://https://campbaker.org/wp-content/plugins/woocommerce/assets/css/woocommerce-smallscreen.css?ver=4.1.">http://https://campbaker.org/wp-content/plugins/woocommerce/assets/css/woocommerce-smallscreen.css?ver=4.1.</a>	100%	Google Safe Browsing	phishing	
<a href="http://https://campbaker.org/FICE3655/#contentN">http://https://campbaker.org/FICE3655/#contentN</a>	100%	Google Safe Browsing	phishing	

## Domains and IPs

### Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
sendgrid.net	167.89.118.52	true	false		high
campbaker.org	192.185.166.140	true	true	<ul style="list-style-type: none"> <li>6%, Virustotal, <a href="#">Browse</a></li> <li>100%, Google Safe Browsing</li> </ul>	unknown
url7220.caapvisio.com	unknown	unknown	false	<ul style="list-style-type: none"> <li>2%, Virustotal, <a href="#">Browse</a></li> </ul>	unknown

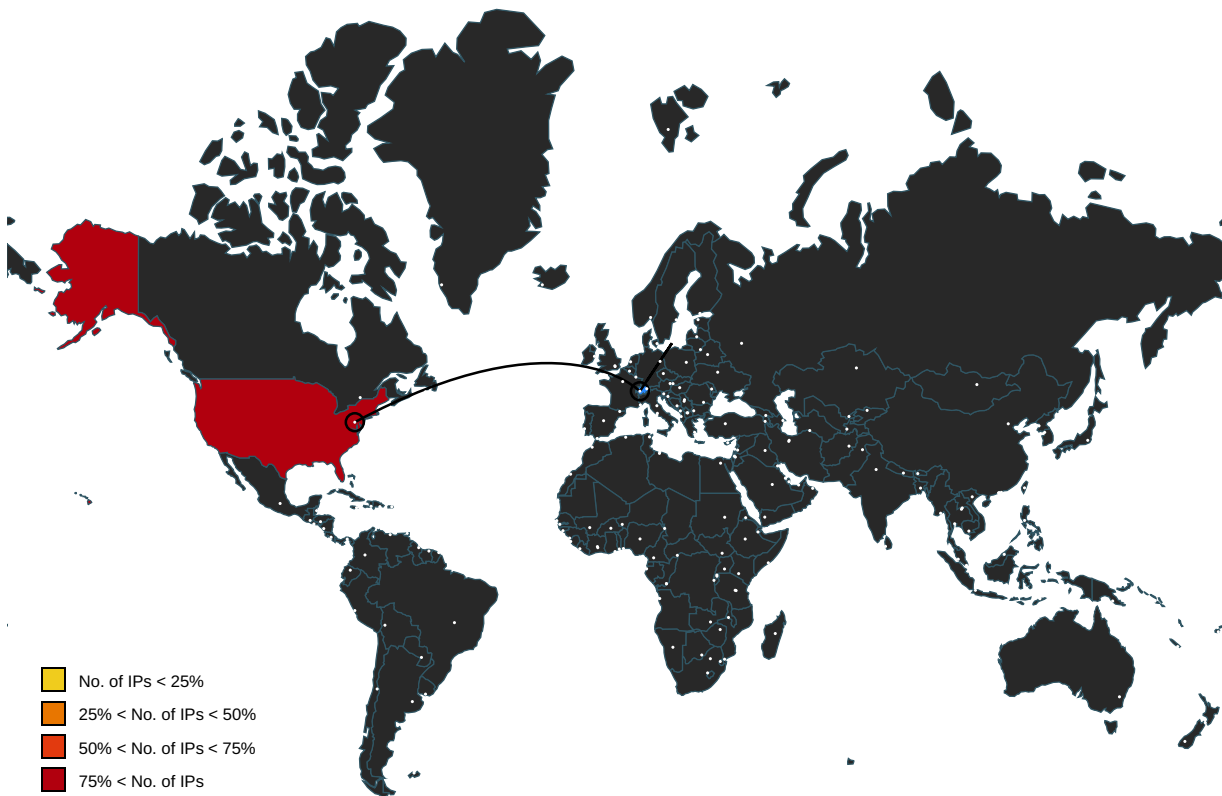
### URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
<a href="http://https://campbaker.org/OFFICE3655/#content">http://https://campbaker.org/OFFICE3655/#content</a>	{5E7EE38A-AA08-11EA-AADE-C25F135D3C65}.dat.1.dr, ~DFADE7453CFED17536.TMP.1.dr	true		unknown
<a href="http://https://campbaker.org/wp-content/uploads/2019/04/hale-partner-logo.png">http://https://campbaker.org/wp-content/uploads/2019/04/hale-partner-logo.png</a>	QELQMBMR.htm.2.dr	true	<ul style="list-style-type: none"> <li>Google Safe Browsing: phishing</li> </ul>	unknown
<a href="http://https://campbaker.org/wp-includes/js/jquery/jquery-migrate.min.js?ver=1.4.1">http://https://campbaker.org/wp-includes/js/jquery/jquery-migrate.min.js?ver=1.4.1</a>	QELQMBMR.htm.2.dr	true	<ul style="list-style-type: none"> <li>Google Safe Browsing: phishing</li> </ul>	unknown
<a href="http://greensock.com/club/">http://greensock.com/club/</a>	jquery.themepunch.tools.min[1].js.2.dr	false		high
<a href="http://www.jacobward.co.uk">http://www.jacobward.co.uk</a>	diwine-extended-scripts[1].js.2.dr	false	<ul style="list-style-type: none"> <li>Avira URL Cloud: safe</li> </ul>	low
<a href="http://https://campbaker.org/job/graduate-counselor/">http://https://campbaker.org/job/graduate-counselor/</a>	QELQMBMR.htm.2.dr	true	<ul style="list-style-type: none"> <li>Google Safe Browsing: phishing</li> </ul>	unknown
<a href="http://https://campbaker.org/wp-includes/css/dist/block-library/style.min.css?ver=5.4.1">http://https://campbaker.org/wp-includes/css/dist/block-library/style.min.css?ver=5.4.1</a>	QELQMBMR.htm.2.dr	true	<ul style="list-style-type: none"> <li>Google Safe Browsing: phishing</li> </ul>	unknown
<a href="http://https://campbaker.org/wp-content/plugins/woocommerce/assets/js/frontend/woocommerce.min.js?ver=4.1.1">http://https://campbaker.org/wp-content/plugins/woocommerce/assets/js/frontend/woocommerce.min.js?ver=4.1.1</a>	QELQMBMR.htm.2.dr	true	<ul style="list-style-type: none"> <li>Google Safe Browsing: phishing</li> </ul>	unknown
<a href="http://adomas.org/javascript-mouse-wheel/">http://adomas.org/javascript-mouse-wheel/</a>	date-time-picker[1].js.2.dr	false	<ul style="list-style-type: none"> <li>5%, Virustotal, <a href="#">Browse</a></li> <li>Avira URL Cloud: safe</li> </ul>	low
<a href="http://https://campbaker.org/job/undergraduate-counselor/">http://https://campbaker.org/job/undergraduate-counselor/</a>	QELQMBMR.htm.2.dr	true	<ul style="list-style-type: none"> <li>Google Safe Browsing: phishing</li> </ul>	unknown
<a href="http://https://campbaker.org/wp-content/themes/diwine/images/up-arrow-2.svg">http://https://campbaker.org/wp-content/themes/diwine/images/up-arrow-2.svg</a>	QELQMBMR.htm.2.dr	true	<ul style="list-style-type: none"> <li>Google Safe Browsing: phishing</li> </ul>	unknown
<a href="http://https://stats.g.doubleclick.net/r/collect?t=dc&amp;aip=1&amp;_r=3&amp;">http://https://stats.g.doubleclick.net/r/collect?t=dc&amp;aip=1&amp;_r=3&amp;</a>	analytics[1].js.2.dr	false		high
<a href="http://https://campbaker.org/wp-content/plugins/booking/js/datepick/jquery.datepick.js?ver=1.1">http://https://campbaker.org/wp-content/plugins/booking/js/datepick/jquery.datepick.js?ver=1.1</a>	QELQMBMR.htm.2.dr	true	<ul style="list-style-type: none"> <li>Google Safe Browsing: phishing</li> </ul>	unknown
<a href="http://https://campbaker.org/wp-content/plugins/booking/assets/libs/bootstrap/css/bootstrap-theme.css?ver=3">http://https://campbaker.org/wp-content/plugins/booking/assets/libs/bootstrap/css/bootstrap-theme.css?ver=3</a>	QELQMBMR.htm.2.dr	true	<ul style="list-style-type: none"> <li>Google Safe Browsing: phishing</li> </ul>	unknown
<a href="http://https://campbaker.org/wp-content/plugins/wp-job-manager-applications/assets/css/frontend.css?ver=5.4">http://https://campbaker.org/wp-content/plugins/wp-job-manager-applications/assets/css/frontend.css?ver=5.4</a>	QELQMBMR.htm.2.dr	true	<ul style="list-style-type: none"> <li>Google Safe Browsing: phishing</li> </ul>	unknown
<a href="http://https://campbaker.org/wp-content/uploads/2019/05/camp-baker-hero-slide2.jpg">http://https://campbaker.org/wp-content/uploads/2019/05/camp-baker-hero-slide2.jpg</a>	QELQMBMR.htm.2.dr	true	<ul style="list-style-type: none"> <li>Google Safe Browsing: phishing</li> </ul>	unknown
<a href="http://https://campbaker.org/wp-content/plugins/mp-timetable/media/css/style.css?ver=2.3.11">http://https://campbaker.org/wp-content/plugins/mp-timetable/media/css/style.css?ver=2.3.11</a>	QELQMBMR.htm.2.dr	true	<ul style="list-style-type: none"> <li>Google Safe Browsing: phishing</li> </ul>	unknown
<a href="http://https://github.com/MohammadYounes/jquery-scrollLock">http://https://github.com/MohammadYounes/jquery-scrollLock</a>	jquery-scrolllock[1].js.2.dr	false		high
<a href="http://www.opensource.org/licenses/mit-license.php">http://www.opensource.org/licenses/mit-license.php</a>	jquery.blockUI.min[1].js.2.dr	false		high
<a href="http://https://campbaker.org/wp-content/themes/diwine/scripts/vendor/date-time/date-time-picker.js">http://https://campbaker.org/wp-content/themes/diwine/scripts/vendor/date-time/date-time-picker.js</a>	QELQMBMR.htm.2.dr	true	<ul style="list-style-type: none"> <li>Google Safe Browsing: phishing</li> </ul>	unknown
<a href="http://https://campbaker.org/wp-content/themes/diwine/scripts/vendor/fancybox/jquery.fancybox.x.css?ver=5.4.1">http://https://campbaker.org/wp-content/themes/diwine/scripts/vendor/fancybox/jquery.fancybox.x.css?ver=5.4.1</a>	QELQMBMR.htm.2.dr	true	<ul style="list-style-type: none"> <li>Google Safe Browsing: phishing</li> </ul>	unknown
<a href="http://https://campbaker.org/wp-content/plugins/revslider/public/assets/css/settings.css?ver=5.4.8.2">http://https://campbaker.org/wp-content/plugins/revslider/public/assets/css/settings.css?ver=5.4.8.2</a>	QELQMBMR.htm.2.dr	true	<ul style="list-style-type: none"> <li>Google Safe Browsing: phishing</li> </ul>	unknown
<a href="http://getbootstrap.com/javascript/#tooltip">http://getbootstrap.com/javascript/#tooltip</a>	bootstrap[1].js.2.dr	false		high
<a href="http://https://wpbakery.com">http://https://wpbakery.com</a>	js_composer_front.min[1].js.2.dr	false	<ul style="list-style-type: none"> <li>Avira URL Cloud: safe</li> </ul>	low
<a href="http://https://campbaker.org/team/">http://https://campbaker.org/team/</a>	QELQMBMR.htm.2.dr	true	<ul style="list-style-type: none"> <li>Google Safe Browsing: phishing</li> </ul>	unknown
<a href="http://https://wpbookingcalendar.com/faq/customize-booking-form-for-having-several-steps-of-reservation/">http://https://wpbookingcalendar.com/faq/customize-booking-form-for-having-several-steps-of-reservation/</a>	client[1].js.2.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://getbootstrap.com)	bootstrap[1].js.2.dr	false	<ul style="list-style-type: none"> <li>Avira URL Cloud: safe</li> </ul>	low
http://https://campbaker.org/wp-content/themes/diwine/css/style-classic-menu.css?ver=5.4.1	QELQMBMR.htm.2.dr	true	<ul style="list-style-type: none"> <li>Google Safe Browsing: phishing</li> </ul>	unknown
http://https://stats.g.doubleclick.net/j/collect	analytics[1].js.2.dr	false		high
http://https://campbaker.org/wp-content/uploads/2019/03/cropped-camp-baker-icon-270x270.png	QELQMBMR.htm.2.dr	true	<ul style="list-style-type: none"> <li>Google Safe Browsing: phishing</li> </ul>	unknown
http://https://campbaker.org/wp-includes/js/jquery/ui/datepicker.min.js?ver=1.11.4	QELQMBMR.htm.2.dr	true	<ul style="list-style-type: none"> <li>Google Safe Browsing: phishing</li> </ul>	unknown
http://https://campbaker.org/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fcampbaker.org%2F	QELQMBMR.htm.2.dr	true	<ul style="list-style-type: none"> <li>Google Safe Browsing: phishing</li> </ul>	unknown
http://www.reddit.com/	msapplication.xml4.1.dr	false		high
http://https://campbaker.org/parent-nights/	QELQMBMR.htm.2.dr	true	<ul style="list-style-type: none"> <li>Google Safe Browsing: phishing</li> </ul>	unknown
http://https://campbaker.org/wp-content/themes/diwine/style.css?ver=5.4.1	QELQMBMR.htm.2.dr	true	<ul style="list-style-type: none"> <li>Google Safe Browsing: phishing</li> </ul>	unknown
http://https://campbaker.org/wp-content/uploads/2019/04/donate-today-384x186.jpg	QELQMBMR.htm.2.dr	true	<ul style="list-style-type: none"> <li>Google Safe Browsing: phishing</li> </ul>	unknown
http://https://campbaker.org/wp-content/uploads/2019/03/cropped-camp-baker-icon-180x180.png	QELQMBMR.htm.2.dr	true	<ul style="list-style-type: none"> <li>Google Safe Browsing: phishing</li> </ul>	unknown
http://https://campbaker.org/	QELQMBMR.htm.2.dr	true		unknown
http://labs.skinkers.com/touchSwipe/	jquery.themepunch.tools.min[1].js.2.dr	false	<ul style="list-style-type: none"> <li>0%, Virustotal, <a href="#">Browse</a></li> <li>Avira URL Cloud: safe</li> </ul>	unknown
http://www.modernizr.com/)	bootstrap[1].js.2.dr	false		high
http://api.jqueryui.com/category/ui-core/	core.min[1].js.2.dr	false		high
http://https://campbaker.org/OFFICE3655/6Page	{5E7EE38A-AA08-11EA-AADE-C25F135D3C65}.dat.1.dr	true	<ul style="list-style-type: none"> <li>Google Safe Browsing: phishing</li> </ul>	unknown
http://https://campbaker.org/wp-content/plugins/woocommerce/assets/js/jquery-blockui/jquery.blockUI.min.js?	QELQMBMR.htm.2.dr	true	<ul style="list-style-type: none"> <li>Google Safe Browsing: phishing</li> </ul>	unknown
http://https://campbaker.org/wp-content/plugins/booking/assets/libs/bootstrap/css/bootstrap.css?ver=3.3.5.1	QELQMBMR.htm.2.dr	true	<ul style="list-style-type: none"> <li>Google Safe Browsing: phishing</li> </ul>	unknown
http://https://campbaker.org/wp-includes/js/imagesloaded.min.js?ver=3.2.0	QELQMBMR.htm.2.dr	true	<ul style="list-style-type: none"> <li>Google Safe Browsing: phishing</li> </ul>	unknown
http://https://campbaker.org/wp-content/plugins/booking/core/timeline/v2/css/timeline_v2.css?ver=8.7.6	QELQMBMR.htm.2.dr	true	<ul style="list-style-type: none"> <li>Google Safe Browsing: phishing</li> </ul>	unknown
http://https://campbaker.org/wp-content/themes/diwine/scripts/vendor/fancybox/jquery.fancybox.pack.js	QELQMBMR.htm.2.dr	true	<ul style="list-style-type: none"> <li>Google Safe Browsing: phishing</li> </ul>	unknown
http://https://campbaker.org/faq/	QELQMBMR.htm.2.dr	true	<ul style="list-style-type: none"> <li>0%, Virustotal, <a href="#">Browse</a></li> <li>Google Safe Browsing: phishing</li> </ul>	unknown
http://https://campbaker.org/wp-content/themes/diwine/css/flickity.min.css?ver=5.4.1	QELQMBMR.htm.2.dr	true	<ul style="list-style-type: none"> <li>Google Safe Browsing: phishing</li> </ul>	unknown
http://https://campbaker.org/wp-content/plugins/booked/assets/js/tooltipsster/css/themes/tooltipsster-light.c	QELQMBMR.htm.2.dr	true	<ul style="list-style-type: none"> <li>Google Safe Browsing: phishing</li> </ul>	unknown
http://https://campbaker.org/wp-content/uploads/2019/05/camp-baker-footer-logo.png	QELQMBMR.htm.2.dr	true	<ul style="list-style-type: none"> <li>Google Safe Browsing: phishing</li> </ul>	unknown
http://https://campbaker.org/wp-content/themes/diwine/scripts/vendor/snap.svg-min.js	QELQMBMR.htm.2.dr	true	<ul style="list-style-type: none"> <li>Google Safe Browsing: phishing</li> </ul>	unknown
http://malsup.com/jquery/block/	jquery.blockUI.min[1].js.2.dr	false		high
http://https://campbaker.org/comments/feed/	QELQMBMR.htm.2.dr	true	<ul style="list-style-type: none"> <li>Google Safe Browsing: phishing</li> </ul>	unknown
http://https://campbaker.org/resources/	QELQMBMR.htm.2.dr	true	<ul style="list-style-type: none"> <li>Google Safe Browsing: phishing</li> </ul>	unknown
http://https://campbaker.org/wp-content/plugins/woocommerce/assets/css/woocommerce.css?ver=4.1.1	QELQMBMR.htm.2.dr	true	<ul style="list-style-type: none"> <li>Google Safe Browsing: phishing</li> </ul>	unknown
http://https://github.com/briancray/tooltipsy	tooltipsy[1].js.2.dr	false		high
http://https://github.com/twbs/bootstrap/blob/master/LICENSE)	bootstrap[1].js.2.dr	false		high
http://https://campbaker.org/wp-content/plugins/booked-frontend-agents/css/styles.css?ver=2.2.6	QELQMBMR.htm.2.dr	true	<ul style="list-style-type: none"> <li>Google Safe Browsing: phishing</li> </ul>	unknown
http://https://campbaker.org/wp-content/plugins/woocommerce/assets/js/frontend/cart-fragments.min.js?ver=4.	QELQMBMR.htm.2.dr	true	<ul style="list-style-type: none"> <li>Google Safe Browsing: phishing</li> </ul>	unknown
http://https://github.com/js-cookie/js-cookie	js.cookie.min[1].js.2.dr	false		high
http://diwine.freevision.me/	style[2].css0.2.dr	false		high
http://validator.w3.org	diwine-extended-scripts[1].js.2.dr	false		high
http://https://campbaker.org/wp-content/plugins/booking/core/timeline/v2/css/timeline_skin_v2.css?ver=8.7.6	QELQMBMR.htm.2.dr	true	<ul style="list-style-type: none"> <li>Google Safe Browsing: phishing</li> </ul>	unknown
http://www.bitstorm.org/jquery/color-animation/	jquery-animate-colors[1].js.2.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
<a href="http://https://campbaker.org/wp-content/plugins/woocommerce/packages/woocommerce-blocks/build/style.css?ver">http://https://campbaker.org/wp-content/plugins/woocommerce/packages/woocommerce-blocks/build/style.css?ver</a>	QELQMBMR.htm.2.dr	true	<ul style="list-style-type: none"> <li>Google Safe Browsing: phishing</li> </ul>	unknown
<a href="http://https://campbaker.org/wp-content/plugins/rsvp/rsvp_plugin.css?ver=5.4.1">http://https://campbaker.org/wp-content/plugins/rsvp/rsvp_plugin.css?ver=5.4.1</a>	QELQMBMR.htm.2.dr	true	<ul style="list-style-type: none"> <li>Google Safe Browsing: phishing</li> </ul>	unknown
<a href="http://https://campbaker.org/wp-content/plugins/booking/assets/libs/bootstrap/js/bootstrap.js?ver=3.3.5.1">http://https://campbaker.org/wp-content/plugins/booking/assets/libs/bootstrap/js/bootstrap.js?ver=3.3.5.1</a>	QELQMBMR.htm.2.dr	true	<ul style="list-style-type: none"> <li>Google Safe Browsing: phishing</li> </ul>	unknown
<a href="http://flickity.metafizzy.co">http://flickity.metafizzy.co</a>	flickity[1].js.2.dr, flickity.min[1].css.2.dr	false		high
<a href="http://https://campbaker.org/">http://https://campbaker.org/</a>	QELQMBMR.htm.2.dr	true	<ul style="list-style-type: none"> <li>0%, Virustotal, <a href="#">Browse</a></li> <li>Google Safe Browsing: phishing</li> </ul>	unknown
<a href="http://https://campbaker.org/wp-content/plugins/booked/assets/js/tooltipster/jquery.tooltipster.min.js?v">http://https://campbaker.org/wp-content/plugins/booked/assets/js/tooltipster/jquery.tooltipster.min.js?v</a>	QELQMBMR.htm.2.dr	true	<ul style="list-style-type: none"> <li>Google Safe Browsing: phishing</li> </ul>	unknown
<a href="http://https://www.campbaker.org">http://https://www.campbaker.org</a>	QELQMBMR.htm.2.dr	true	<ul style="list-style-type: none"> <li>Google Safe Browsing: phishing</li> </ul>	unknown
<a href="http://https://campbaker.org/wp-content/plugins/booking/css/calendar.css?ver=8.7.6">http://https://campbaker.org/wp-content/plugins/booking/css/calendar.css?ver=8.7.6</a>	QELQMBMR.htm.2.dr	true	<ul style="list-style-type: none"> <li>Google Safe Browsing: phishing</li> </ul>	unknown
<a href="http://https://campbaker.org/wp-content/plugins/woocommerce/assets/css/woocommerce-layout.css?ver=4.1.1">http://https://campbaker.org/wp-content/plugins/woocommerce/assets/css/woocommerce-layout.css?ver=4.1.1</a>	QELQMBMR.htm.2.dr	true	<ul style="list-style-type: none"> <li>Google Safe Browsing: phishing</li> </ul>	unknown
<a href="http://www.youtube.com/watch?v=opj24KnzrWo">http://www.youtube.com/watch?v=opj24KnzrWo</a>	jquery.fancybox-media[1].js.2.dr	false		high
<a href="http://https://campbaker.org/FICE3655/#contentF">http://https://campbaker.org/FICE3655/#contentF</a>	~DFADE7453CFED17536.TMP.1.dr	true	<ul style="list-style-type: none"> <li>Google Safe Browsing: phishing</li> </ul>	unknown
<a href="http://getbootstrap.com/javascript/#collapse">http://getbootstrap.com/javascript/#collapse</a>	bootstrap[1].js.2.dr	false		high
<a href="http://https://campbaker.org/wp-content/uploads/2019/05/jbcc-logo-white.png">http://https://campbaker.org/wp-content/uploads/2019/05/jbcc-logo-white.png</a>	QELQMBMR.htm.2.dr	true	<ul style="list-style-type: none"> <li>Google Safe Browsing: phishing</li> </ul>	unknown
<a href="http://getbootstrap.com/javascript/#modals">http://getbootstrap.com/javascript/#modals</a>	bootstrap[1].js.2.dr	false		high
<a href="http://www.amazon.com/">http://www.amazon.com/</a>	msapplication.xml.1.dr	false		high
<a href="http://https://campbaker.org/wp-content/plugins/booked/assets/css/icons.css?ver=2.2.6">http://https://campbaker.org/wp-content/plugins/booked/assets/css/icons.css?ver=2.2.6</a>	QELQMBMR.htm.2.dr	true	<ul style="list-style-type: none"> <li>Google Safe Browsing: phishing</li> </ul>	unknown
<a href="http://https://campbaker.org/wp-includes/js/jquery/jquery.js?ver=1.12.4-wp">http://https://campbaker.org/wp-includes/js/jquery/jquery.js?ver=1.12.4-wp</a>	QELQMBMR.htm.2.dr	true	<ul style="list-style-type: none"> <li>Google Safe Browsing: phishing</li> </ul>	unknown
<a href="http://go.wpbakery.com/licensing">http://go.wpbakery.com/licensing</a>	js_composer_front.min[1].js.2.dr	false		high
<a href="http://www.twitter.com/">http://www.twitter.com/</a>	msapplication.xml5.1.dr	false		high
<a href="http://https://campbaker.org/wp-content/uploads/2019/03/camp-baker-logo-retina.png">http://https://campbaker.org/wp-content/uploads/2019/03/camp-baker-logo-retina.png</a>	QELQMBMR.htm.2.dr	true	<ul style="list-style-type: none"> <li>Google Safe Browsing: phishing</li> </ul>	unknown
<a href="http://https://campbaker.org/wp-content/plugins/booked/assets/js/spin.jquery.js?ver=2.0.1">http://https://campbaker.org/wp-content/plugins/booked/assets/js/spin.jquery.js?ver=2.0.1</a>	QELQMBMR.htm.2.dr	true	<ul style="list-style-type: none"> <li>Google Safe Browsing: phishing</li> </ul>	unknown
<a href="http://https://campbaker.org/wp-content/themes/diwine/scripts/vendor/plugins/nicescroll.js">http://https://campbaker.org/wp-content/themes/diwine/scripts/vendor/plugins/nicescroll.js</a>	QELQMBMR.htm.2.dr	true	<ul style="list-style-type: none"> <li>Google Safe Browsing: phishing</li> </ul>	unknown
<a href="http://https://campbaker.org/wp-content/plugins/booked/assets/css/styles.css?ver=2.2.6">http://https://campbaker.org/wp-content/plugins/booked/assets/css/styles.css?ver=2.2.6</a>	QELQMBMR.htm.2.dr	true	<ul style="list-style-type: none"> <li>Google Safe Browsing: phishing</li> </ul>	unknown
<a href="http://https://campbaker.org/training-opportunities/">http://https://campbaker.org/training-opportunities/</a>	QELQMBMR.htm.2.dr	true	<ul style="list-style-type: none"> <li>Google Safe Browsing: phishing</li> </ul>	unknown
<a href="http://api.jquery.com/jquery.browser">http://api.jquery.com/jquery.browser</a>	wpbc-migrate[1].js.2.dr	false		high
<a href="http://https://campbaker.org/wp-content/plugins/revslider/public/assets/js/jquery.themepunch.rvolution.min">http://https://campbaker.org/wp-content/plugins/revslider/public/assets/js/jquery.themepunch.rvolution.min</a>	QELQMBMR.htm.2.dr	true	<ul style="list-style-type: none"> <li>Google Safe Browsing: phishing</li> </ul>	unknown
<a href="http://https://campbaker.org/for-campers/">http://https://campbaker.org/for-campers/</a>	QELQMBMR.htm.2.dr	true	<ul style="list-style-type: none"> <li>Google Safe Browsing: phishing</li> </ul>	unknown
<a href="http://https://campbaker.org/wp-content/plugins/js_composer/assets/js/vendors/woocommerce-add-to-cart.js?ve">http://https://campbaker.org/wp-content/plugins/js_composer/assets/js/vendors/woocommerce-add-to-cart.js?ve</a>	QELQMBMR.htm.2.dr	true	<ul style="list-style-type: none"> <li>Google Safe Browsing: phishing</li> </ul>	unknown
<a href="http://https://campbaker.org/wp-content/themes/diwine-child/style.css?ver=5.4.1">http://https://campbaker.org/wp-content/themes/diwine-child/style.css?ver=5.4.1</a>	QELQMBMR.htm.2.dr	true	<ul style="list-style-type: none"> <li>Google Safe Browsing: phishing</li> </ul>	unknown
<a href="http://dev.jquery.com/browser/trunk/jquery/GPL-LICENSE.txt">http://dev.jquery.com/browser/trunk/jquery/GPL-LICENSE.txt</a>	jquery.datepick[1].js.2.dr	false		high
<a href="http://https://github.com/imakewebthings/jquery-waypoints/blob/master/licenses.txt">http://https://github.com/imakewebthings/jquery-waypoints/blob/master/licenses.txt</a>	waypoints[1].js.2.dr	false		high
<a href="http://https://campbaker.org/wp-content/plugins/contact-form-7/includes/js/scripts.js?ver=5.1.9">http://https://campbaker.org/wp-content/plugins/contact-form-7/includes/js/scripts.js?ver=5.1.9</a>	QELQMBMR.htm.2.dr	true	<ul style="list-style-type: none"> <li>Google Safe Browsing: phishing</li> </ul>	unknown
<a href="http://https://campbaker.org/wp-content/plugins/woocommerce/assets/css/woocommerce-smallscreen.css?ver=4.1">http://https://campbaker.org/wp-content/plugins/woocommerce/assets/css/woocommerce-smallscreen.css?ver=4.1</a>	QELQMBMR.htm.2.dr	true	<ul style="list-style-type: none"> <li>Google Safe Browsing: phishing</li> </ul>	unknown
<a href="http://xdsoft.net/jqplugins/datetimepicker/">http://xdsoft.net/jqplugins/datetimepicker/</a>	date-time-picker[1].js.2.dr	false		high
<a href="http://https://campbaker.org/FICE3655/#contentN">http://https://campbaker.org/FICE3655/#contentN</a>	~DFADE7453CFED17536.TMP.1.dr	true	<ul style="list-style-type: none"> <li>Google Safe Browsing: phishing</li> </ul>	unknown

## Contacted IPs



Public					
IP	Country	Flag	ASN	ASN Name	Malicious
167.89.118.52	United States		11377	unknown	false
192.185.166.140	United States		46606	unknown	true

General Information	
Joe Sandbox Version:	29.0.0 Ocean Jasper
Analysis ID:	236664
Start date:	08.06.2020
Start time:	21:18:46
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 52s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs

Sample URL:	<a href="http://url7220.caapvisio.com/ls/click?upn=U5wBbtTMlgqzyFeoDeLr9oYI88rjnJDKdB-2FOqe4mjsPWQeP8r8RzDIgeUom6oe-2FaiU7o_DC4y3DdDCeEScwRgaDHqvVGy56gjlVzN-2FR6WAJbPzoIndJWWMS5Nkfg9TStdNBwzzNXg19pf8z0ZDZc9DdeYbjXBEzOUQDij5Y6qNaHhwy8a1GmmWUfNIKQdV5jNijS-2FPYjImppGgMNCOKDnCFRzE-2BtlPuEuW9HL8vR8Wt5eD4RcdD-2FKL22gop-2FvXlzeVJxcDVXnSCieFHQtG0L7OWAFTFIEIOVBANnwHDrwyLzxVtqL2xBsu9e2Yuuq6z29wQB7-2FyidJCIZLUne1Rn4dgtxj2S9qSfe47d18pWh0akhpla00EiNBwjG-2FEerblB3yotE-2B0rDgEyV1dN7xqp6IWS4wNe2SjpCq-2Bd3KysdMWKgtf9-2Fyx-2Foz6kqZij-2FhoFvYJVLNIXpuCIS14ETkrvFVaSdzrl-2FAFD4CJ0lpN8haTyAlyfzLLUDNibK2-2FKRqq0VKbmPlaVSI5idyFxaDOg-2FD8pZjZJ6FP17mdPcFXzud7tUBE0fW1sqj-2BDKXgTJ-2FOp2an5z6KIwnX6tNwnVLzn5RuoJAjMdlmua1AtTqdjip0hnCSda-2FxsdINP0qciBTe99zuZZYqSuju2N0uix-2BiYqvDE7-2B0Kk0wlbHmZ38a-2BFoXgFH9dWpjZqmaF3RH2OQ-2FgS9WsoMHejqz88SBj0zdDjKSE2ve6qo0veAzLH3FJZZ2OTnVmVmvXTWOnTxVMCuDNo0gTLg9c45S1XgyV4CrH8AZF7EpWJOXWIrZ9Cg9pggyJJg5JsPeixq93R4KOGIRsu6RLWPepjvN4KUBwpagxkwo03fyU9GcSgjCUnNq9-2BTHkpNEnAQFWWIFbiMXHPUwOXqBoNH9gEhqsF-2FNHoPURLLGoeaBgxQhPYPf7ALCwTbW96GnOGSgqZnKLCZo-2Fit2D-2B1qWVvm1I392O1TAT2xXs7f173Pd6IPoXclYUMXEJSwascmy5p6x6Aa7iw3NUDri7YF0">http://url7220.caapvisio.com/ls/click?upn=U5wBbtTMlgqzyFeoDeLr9oYI88rjnJDKdB-2FOqe4mjsPWQeP8r8RzDIgeUom6oe-2FaiU7o_DC4y3DdDCeEScwRgaDHqvVGy56gjlVzN-2FR6WAJbPzoIndJWWMS5Nkfg9TStdNBwzzNXg19pf8z0ZDZc9DdeYbjXBEzOUQDij5Y6qNaHhwy8a1GmmWUfNIKQdV5jNijS-2FPYjImppGgMNCOKDnCFRzE-2BtlPuEuW9HL8vR8Wt5eD4RcdD-2FKL22gop-2FvXlzeVJxcDVXnSCieFHQtG0L7OWAFTFIEIOVBANnwHDrwyLzxVtqL2xBsu9e2Yuuq6z29wQB7-2FyidJCIZLUne1Rn4dgtxj2S9qSfe47d18pWh0akhpla00EiNBwjG-2FEerblB3yotE-2B0rDgEyV1dN7xqp6IWS4wNe2SjpCq-2Bd3KysdMWKgtf9-2Fyx-2Foz6kqZij-2FhoFvYJVLNIXpuCIS14ETkrvFVaSdzrl-2FAFD4CJ0lpN8haTyAlyfzLLUDNibK2-2FKRqq0VKbmPlaVSI5idyFxaDOg-2FD8pZjZJ6FP17mdPcFXzud7tUBE0fW1sqj-2BDKXgTJ-2FOp2an5z6KIwnX6tNwnVLzn5RuoJAjMdlmua1AtTqdjip0hnCSda-2FxsdINP0qciBTe99zuZZYqSuju2N0uix-2BiYqvDE7-2B0Kk0wlbHmZ38a-2BFoXgFH9dWpjZqmaF3RH2OQ-2FgS9WsoMHejqz88SBj0zdDjKSE2ve6qo0veAzLH3FJZZ2OTnVmVmvXTWOnTxVMCuDNo0gTLg9c45S1XgyV4CrH8AZF7EpWJOXWIrZ9Cg9pggyJJg5JsPeixq93R4KOGIRsu6RLWPepjvN4KUBwpagxkwo03fyU9GcSgjCUnNq9-2BTHkpNEnAQFWWIFbiMXHPUwOXqBoNH9gEhqsF-2FNHoPURLLGoeaBgxQhPYPf7ALCwTbW96GnOGSgqZnKLCZo-2Fit2D-2B1qWVvm1I392O1TAT2xXs7f173Pd6IPoXclYUMXEJSwascmy5p6x6Aa7iw3NUDri7YF0</a>
Analysis system description:	Windows 10 64 bit (version 1803) with <b>Office 2016</b> , Adobe Reader DC 19, Chrome 70, Firefox 63, Java 8.171, Flash 30.0.0.113
Number of analysed new started processes analysed:	8
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:	<ul style="list-style-type: none"> <li>• EGA enabled</li> <li>• AMSI enabled</li> </ul>
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal56.win@3/163@3/2
Cookbook Comments:	<ul style="list-style-type: none"> <li>• Adjust boot time</li> <li>• Enable AMSI</li> <li>• Browsing link: <a href="https://campbak.er.org/OFFICE3655/#content">https://campbak.er.org/OFFICE3655/#content</a></li> <li>• Browsing link: <a href="https://campbaker.org/">https://campbaker.org/</a></li> </ul>
Warnings:	<p>Show All</p> <ul style="list-style-type: none"> <li>• Exclude process from analysis (whitelisted): ielowutil.exe, WMIADAP.exe, MusNotifyIcon.exe, Usoclient.exe</li> <li>• TCP Packets have been reduced to 100</li> <li>• Created / dropped Files have been reduced to 100</li> <li>• Excluded IPs from analysis (whitelisted): 23.10.69.125, 216.58.212.170, 216.58.212.136, 216.58.208.35, 216.58.212.142, 152.199.19.161, 104.80.23.128</li> <li>• Excluded domains from analysis (whitelisted): gstaticadssl.l.google.com, fonts.googleapis.com, fs.microsoft.com, www-google-analytics.l.google.com, fonts.gstatic.com, ie9comview.vo.msecnd.net, www-googleletagmanager.l.google.com, e1723.g.akamaiedge.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, go.microsoft.com, www.googleletagmanager.com, go.microsoft.com.edgekey.net, prod.fs.microsoft.com.akadns.net, www.google-analytics.com, cs9.wpc.v0cdn.net</li> <li>• Report size getting too big, too many NtCreateFile calls found.</li> <li>• Report size getting too big, too many NtDeviceIoControlFile calls found.</li> </ul>

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\D1YBPPLZ\campbaker[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Size (bytes):	866
Entropy (8bit):	4.927478157233517
Encrypted:	false
MD5:	36ED0016F77A6DCC9A6C33FA3111F952
SHA1:	B7349EE0CA480B2EB12BC03878A41A9DABA4FEB1
SHA-256:	D8EF8F3E8D0D84365592AC1B3E404E31F48966C9243DEDF65CAC5A20AA78C439
SHA-512:	A502D66E9D4C6223DC24DA918D142BCECC5C1C9162BA92714D647B426414625B26ABBD10D2578C49F2FA224D3CA5FFC9E3D15BE5372AA98C45F9FF05C19BE53
Malicious:	false
Reputation:	low
Preview:	<root></root><root><item name="modernizr" value="modernizr" ltime="599696352" htime="30817813" /></root><root></root><root><item name="wc" value="test" ltime="604706352" htime="30817813" /></root><root></root><root><item name="wc_cart_hash_7a80af1a4a99285b6bddb2ea3d75fb04" value="" ltime="615496352" htime="30817813" /></root><root><item name="wc_cart_hash_7a80af1a4a99285b6bddb2ea3d75fb04" value="" ltime="615496352" htime="30817813" /></root><root><item name="wc_cart_hash_7a80af1a4a99285b6bddb2ea3d75fb04" value="" ltime="615496352" htime="30817813" /></root><root><item name="wc" value="test" ltime="1138906352" htime="30817813" /></root><root><item name="wc_cart_hash_7a80af1a4a99285b6bddb2ea3d75fb04" value="" ltime="615496352" htime="30817813" /></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{5E7EE388-AA08-11EA-AADE-C25F135D3C65}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Size (bytes):	30296
Entropy (8bit):	1.8521499623562099
Encrypted:	false
MD5:	6C03A6C321E33BF88ABFB89F4B978D49
SHA1:	36316E4F4A256A23B1FAB768C57A00B3BC3ADC0F
SHA-256:	A73806735E3C0A8C59FD5E378D3A29FAE717288C38404C2F62FC80990D902137

<b>C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{5E7EE388-AA08-11EA-AADE-C25F135D3C65}.dat</b>	
SHA-512:	A50700146D3E72C04E7C52FD35DCB80C4B670AF1A35EE69DFD5909668ED5C5A97E1B4C0C7DCAF223BCB1192DC8A6B128260569891C8514615FC4502C7BD1E19
Malicious:	false
Reputation:	low
Preview:	..... .....R.o.o.t. .E.n.t.r. y..... .....

<b>C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{5E7EE38A-AA08-11EA-AADE-C25F135D3C65}.dat</b>	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Size (bytes):	51492
Entropy (8bit):	2.0586829061776464
Encrypted:	false
MD5:	36D8F10B7A9CD4EE0FD6E57517F1EBB4
SHA1:	80AC39C562405A0F5DE381BF28E51B1D1CD0F0DD
SHA-256:	D844AA6299E92321473177DC62A44164B1459A5D513F59C6A53539863A6ECEA8
SHA-512:	1D2B7F097CEF110309C3DE23E47EB5992DD736E32F245C56217D5C8D81913F0DBCA7FE290E47A0263C11035FCD77646D7DFD3F3E45BF9FF8EDCF23284B812BD
Malicious:	false
Reputation:	low
Preview:	..... .....R.o.o.t. .E.n.t.r. y..... .....

<b>C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{650A0859-AA08-11EA-AADE-C25F135D3C65}.dat</b>	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Size (bytes):	16984
Entropy (8bit):	1.5652477594933978
Encrypted:	false
MD5:	DCDE959B1925BC5996E1A0F6408D425D
SHA1:	EFDB3A8823CF88C0FCC603A89EB86467C09EC927
SHA-256:	5D893F3E38C6FFF81FE5E2C5AADDD2E6DB4D173A8A273160EE3218D6C2E421B
SHA-512:	4096C8AA2B4F11646C893B35995146155EDA6545E67C0CFB8B83DC1DD02C81191F453BAE7E77632D16D1A360034732AB14595203CE151DAD8D2DCF7443677
Malicious:	false
Reputation:	low
Preview:	..... .....R.o.o.t. .E.n.t.r. y..... .....

<b>C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml</b>	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Size (bytes):	656
Entropy (8bit):	5.103800559258851
Encrypted:	false
MD5:	334C200938074DCE45B48C9AD61A7EDD
SHA1:	9D2F3279C974A6613022B28390094AD7F10F150F
SHA-256:	717007E69292DDE1AAF6B82471A5B5677077F302D3A9D74EA629C73B24AC5AE7
SHA-512:	35B52E9C439DAF3168CF3944FA450862CF08D9D337CB127389D464869FE27C8D8DC429A78214CB761AF2BCBD2EA9B8334DBF1BAFCA2C7379EDB5102CC25A7C
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x36205124,0x01d63e15</date><accdate>0x36205124,0x01d63e15</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>0x36205124,0x01d63e15</date><accdate>0x3621d063,0x01d63e15</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Twitter.url"/></tile></msapplication></browserconfig>..

<b>C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml</b>	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators

<b>C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml</b>	
Size (bytes):	653
Entropy (8bit):	5.126621185293582
Encrypted:	false
MD5:	59A601305EF0537D7596700B3919B3A2
SHA1:	C34E49474098452A992B771C86730F185D60F9EA
SHA-256:	EC787ABAF3A8D27462EEBB817262CB241AF05E1475F5EDAC09B613D6EA8080EF
SHA-512:	FBB16BA53FD12332C32E5955F4BF07DC3E86BC56CEE4A1572F1E78C3A49183CA829C2CB5ED5A7044DCBC8422D709A6650C76515727C3DCD7906054C93289515
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x36091207,0x01d63e15</date><accdate>0x36091207,0x01d63e15</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>0x36091207,0x01d63e15</date><accdate>0x36111e47,0x01d63e15</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Amazon.url"/></tile></msapplication></browserconfig>..

<b>C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml</b>	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Size (bytes):	662
Entropy (8bit):	5.1001769557181404
Encrypted:	false
MD5:	FBA0752DD333A32AB8BE06274DA3453A
SHA1:	734621964490893F2AAC1E22DCB02B2E5E9FF3A0
SHA-256:	2FA4935F1FEBE92D141A38DB7C7BED8762178745238E3519C09F8E4C55D107DC
SHA-512:	2AF0BC9936ED4E519B6B1C16BA9B07959B407B53C6C8D36E05A53F0E96BA59B6D4B5AF4C10E501F9500B9D0776EC48AAE611D7C80A12D2D60BA570C646BAD434
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x36235f0d,0x01d63e15</date><accdate>0x36235f0d,0x01d63e15</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>0x36235f0d,0x01d63e15</date><accdate>0x36235f0d,0x01d63e15</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Wikipedia.url"/></tile></msapplication></browserconfig>..

<b>C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml</b>	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Size (bytes):	647
Entropy (8bit):	5.099626666295816
Encrypted:	false
MD5:	04AB8F2E344CA314D42A6E4177180279
SHA1:	C2B4B8542B49D115E3BE08309B505239F1297EBA
SHA-256:	D51ABBB003A4EE3A6DBDD1D77BCCAFDD9C52E730AC06CCD65653F21B56A71AC9
SHA-512:	FCDC078B254443954406D1EC82321205F0037BCA2DB65ED7F3097E2C68EA5885D8F13C706D6B278999CFF9CB4972E2F66B7247F10F3F43D9A6DDA5A73AF203A
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x3615704d,0x01d63e15</date><accdate>0x3615704d,0x01d63e15</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>0x3615704d,0x01d63e15</date><accdate>0x36180bce,0x01d63e15</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Live.url"/></tile></msapplication></browserconfig>..

<b>C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml</b>	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Size (bytes):	656
Entropy (8bit):	5.1261021452931015
Encrypted:	false
MD5:	B140A029907F7B6AD9527A3CE24E55F9
SHA1:	DDCEEC54F16B28DF73FA94FDB8B33E924B12DD63
SHA-256:	BAAC83CFAB0DA24DB4F0BA4241AA95A9CE27DA788D7CAF728C183FD89F3C6C00
SHA-512:	68E6ACF44C18A08B318E8EDB72522175B00C7B84432D5283BD4EB16DB5A367C8442146BA6B396F3DAD92A8ACB0A3712F80B559997A616FF5241E9DCDBDCAF61
Malicious:	false
Reputation:	low



C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml

Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/" /><date>0x36265c11,0x01d63e15</date><accdate>0x36265c11,0x01d63e15</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>0x36265c11,0x01d63e15</date><accdate>0x362718c9,0x01d63e15</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
Size (bytes):	653
Entropy (8bit):	5.068464038037464
Encrypted:	false
MD5:	DAF7237EFB2C1D9EF4171BAB0A9D768F
SHA1:	CD8117684A6A6E73834C1AC3B90BE5DAE2FEC22C
SHA-256:	53F7097322635FD57DAF715637E34E7B3B7783EF016113EA25145A3DF12A8611
SHA-512:	5BE9BDE292F27FF3C814720B07C2A817FC64C42D1A43E5D8077005AC866CD10AF0F5E47A763B0901BA5F1D3AA79D37F68F375C9971E0769DA9DA81A129C7027
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/" /><date>0x361d1cc8,0x01d63e15</date><accdate>0x361d1cc8,0x01d63e15</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>0x361d1cc8,0x01d63e15</date><accdate>0x361fb84c,0x01d63e15</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
Size (bytes):	656
Entropy (8bit):	5.132577594819916
Encrypted:	false
MD5:	B6B13E31378AD9516040B07138A236C4
SHA1:	F2A423DC6B778EBC5C549F9C0B0820A0A230D04B
SHA-256:	714E115C1F4437A07CA19E81479C23C85B90335D957513C8AA35555FE50812BB
SHA-512:	1D925326E00447EFC77B65E0DA0A0D1A449AB552896DCB25949EF80ABAD47F1759D03EB4E56685DD549AF936A90E4E578A5CF57B3B8B32E100E061E8BBBF23B
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/" /><date>0x361a943d,0x01d63e15</date><accdate>0x361a943d,0x01d63e15</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>0x361a943d,0x01d63e15</date><accdate>0x361a943d,0x01d63e15</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\NYTimes.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Size (bytes):	659
Entropy (8bit):	5.122621380364386
Encrypted:	false
MD5:	4FDC57C960722EA18F96536AD836B4B8
SHA1:	E31919504E230541ADE1354989CD80ADE197DBF0
SHA-256:	2C842A4EAED2B8E6ACD4A3600E557A2183180EDFD8F39A35F9B76602595773E2
SHA-512:	87DEF606CD44A5267FF7AD942EAE88BC69987C70C9AC7E620051793AEF6B535E2DED3EB1E2633EE8489FF2196C72BC311A74DD7E54093F70F7977DB1E76BFD
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/" /><date>0x3612d588,0x01d63e15</date><accdate>0x3612d588,0x01d63e15</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>0x3612d588,0x01d63e15</date><accdate>0x3612d588,0x01d63e15</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
Size (bytes):	653
Entropy (8bit):	5.084665515547942

<b>C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml</b>	
Encrypted:	false
MD5:	74D751F50104A8C69F89F151FDEDB3C3
SHA1:	03277317086C642D24A676DFBDAB642754C65D7C
SHA-256:	3CCF589B8E6BB6D4ABA989AB8D5ACFE9C3D76313A50C425ECF2C8B09FA508910
SHA-512:	063DB5A34ED99F97FA68C7F94E97FA028E13CE950256CAF91092C70B4F005D2D7276CBD9259CF20023826AAC84FADA0F21E545EEEE057E4E67F31443A32CDA0C
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x3615704d,0x01d63e15</date><acccdate>0x3615704d,0x01d63e15</acccdate></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>0x3615704d,0x01d63e15</date><acccdate>0x3615704d,0x01d63e15</acccdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Google.url"/></tile></msapplication></browserconfig>..

<b>C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\6aw4uvh\imagestore.dat</b>	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	data
Size (bytes):	1269
Entropy (8bit):	6.130911479650321
Encrypted:	false
MD5:	65234C671DD262068DBB9F4C30DC218E
SHA1:	2CC9CC76EFE2ED3C9C9379A7CE956A510A883AAE
SHA-256:	0FCE2413AA473EA0A1E243305BF5506B92443389CB14DA750EFA33CC5371C8E7
SHA-512:	C7C106051EE6E947BDC7F3F995178DCDDC3CDAF61C3419C76B4DC79691AC209C4D9E555D715E3BEA1FBD60FB7C6336E2B6B4E994D5302FE55A4595545360E74
Malicious:	false
Reputation:	low
Preview:	R.h.t.t.p.s.:.//c.a.m.p.b.a.k.e.r...o.r.g./w.p.-c.o.n.t.e.n.t./u.p.l.o.a.d.s/.2.0.1.9/.0.3/.c.r.o.p.p.e.d.-c.a.m.p.-b.a.k.e.r.-i.c.o.n.-3.2.x.3.2...p.n.g.+....PNG.....IHDR... ..D.....gAMA.....a.....sRGB.....cHRM..z&.....u0...'......p..Q<...PPLTE.....otRNS.....m.n.a.Z!.V.@.d...]A...._..c.P.UM..OK..C.96.E.....RT.5..D2...<0.;.4..l./e.....pHYs...H...H.F.k>...6IDAT8..IS.1...@F.....F.pE.....}.y.h2....K....<w.....-M.....jj..'(.....p_D7.=.?....m.4......5b..@bl.k.dj"....LMI.+..B...rUL>=3;.Q.....y. ....U4.Rl..4m)A.....r.T..!..YE....VM.....@R...1....quM.....,*z

<b>C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\KSU5XQMC\0QI6MX1D_JOuGQbT0gvTJPa787weuxJBkqs[1].woff</b>	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 22384, version 1.1
Size (bytes):	22384
Entropy (8bit):	7.97707110129453
Encrypted:	false
MD5:	66B42B940A002A17884BDA6CA992391F
SHA1:	28FC9B6CBECCFAC68C9CC6ECE0F3277305EF239B
SHA-256:	80D4CAC945D546A45EBDEB0FF32E8DC94F485ED29CF1FD4FC2D0DF56F9319874
SHA-512:	9237A12B37D6CFE92F046C757AD0133A8AF594DF44AC550707DD2B1FD8AC85D40B12FE534C35AA3044573FF5271799551B72FDED60D8D191A8AF91ABC589440
Malicious:	false
Reputation:	low
IE Cache URL:	<a href="http://https://fonts.gstatic.com/s/lora/v15/0QI6MX1D_JOuGQbT0gvTJPa787weuxJBkqs.woff">http://https://fonts.gstatic.com/s/lora/v15/0QI6MX1D_JOuGQbT0gvTJPa787weuxJBkqs.woff</a>
Preview:	wOFF.....Wp.....0.....GDEF...l..z.....GPOS.....).?*.GSUB.....OS/2.....O...`dY.dSTAT...D...8...D...cmap...[.....r".@.gasp.. .....glyph.. (.1...N(K.D.head..Q....6...hhea..Q.....\$.b..hmtx..R....""^"loca..T(.....".maxp..V.....name..V...5...fy[.post.WT.....2prep..Wh.....h...x.....L.PHO.....@....R.c.H+.{t>w.....P0\$.BO.T.P..c?Q.....\a..d.....?p'..E...y...K....!).j./.....?.....x.T..t.P...?....6.k...m.m.m.m....=E...a...f...Ck.[...M{tB..@.Q.).[v.W....HJ.*N.Hu.t.BQ...]....%H....i.i.A....8..f..'.S.E.Jv...2.)n.....O.t..!/>_..n.N....XHt2..e0..F.O...l=..U...G.#f.p.{...=.....W.. ...B.R5.3v.....tE...a..J.....cD..q.;"WEi.A1]?...8"qZ.%U.....>...>.U...s..k.k-k+k.....{....*&...+})#.81.JLf83.Hf1.Q..c.....g..j.0.ulf:..).p.....9.9.p.+..Xl...%~...%.D...d...j]%,o.A82D.0...7f_...?7.....\$W..\$.~{2^E..*..T...!"...N+....C;....k3.E.p.....

<b>C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\KSU5XQMC\0QI6MX1D_JOuGQbT0gvTJPa787z5vBjBkqs[1].woff</b>	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 22512, version 1.1
Size (bytes):	22512
Entropy (8bit):	7.979299697763813
Encrypted:	false
MD5:	5492F7AC3734D124D2233E35FDE13AB5
SHA1:	CD30A453228ADF3EB266D72C76C85387720B8512
SHA-256:	B26115D50952F757DC4AAE7988B2C248D5242720CD37DFC3050C5A58283DB478
SHA-512:	7006F31AE9FEA2EE2A3E7DCCD55C6612B9FBE26426EEF62640F9067934482CA5E7D8D4E2CE7395CF272C7A221D4137DE8D51DD0D1FB5568F13B837D6A8F829C
Malicious:	false
Reputation:	low
IE Cache URL:	<a href="http://https://fonts.gstatic.com/s/lora/v15/0QI6MX1D_JOuGQbT0gvTJPa787z5vBjBkqs.woff">http://https://fonts.gstatic.com/s/lora/v15/0QI6MX1D_JOuGQbT0gvTJPa787z5vBjBkqs.woff</a>

<b>C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\E\KSU5XQMC\0QI6MX1D_JOuGQbT0gvTJPa787z5vBJBkqs[1].woff</b>	
Preview:	wOFF.....W.....L.....GDEF...l...z.....GPOS.....?Hjo.GSUB.....OS/2.....O...`e..DSTAT..D...8...D....cmap.. .....r".@.gasp..".....glyf.."(..0...M. {RNhead..R8...6...6...hhea..Rp.....\$b..hmtx..R.....loca..T.....maxp..V......name..V...6...T::X.post..W.....2prep..W.....h...x.....L.PH0.....@....R..c.H+.{ t>w.....P0\$.BO.T.P..c?Q.....\a..d.....?p'..E...y...K...!..j./.....?.....x.L...[Q...?"X.k.mj..dP...m.m.6.....Sn.<B...b.x+...w.v..5....~J...m..l.wi+9..S..(YVN.Is..t.:{W...2F ..Ab.a.1...!... .....(p...K.....'.X\..q...>z\$.S..).j.Z.?(*(DL.....>q.a.....>...K.....]...7...c.;YjW.....OL..q1.b.6...{"R.#...?~R...[Q.....O>\$.....Zv..E.w4.VX.h.U....%...;.....=Vt.... [~...c.&0..L...LF0[b...B.2..b+y.d...la.T..0.9&r...X.M...F.....=...3..{..tV...O..01H)a...LW...3Wr..n...Q.X..rE.....?y...4..m.H2[ff.Q.f...\$.XW.....

<b>C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\E\KSU5XQMC\0QI6MX1D_JOuGQbT0gvTJPa787zAvBJBkqs[1].woff</b>	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 23268, version 1.1
Size (bytes):	23268
Entropy (8bit):	7.97982784074553
Encrypted:	false
MD5:	E9E41B8C67220D4B9A000205E05CB659
SHA1:	9443C4BBDEB3ED32D068E4CB2645ACD402683AB8
SHA-256:	8B08551906DD3A4825031B1A793B8E57594DD4E5F113931CCA4403894D742E24
SHA-512:	D83789CD721237B03A8FCECF1A125160E079C732FADCB2738351D1C1662B0BA0561035EA3354F2D3486E66894372299676042CC8F27142E486D820620E68EC21
Malicious:	false
Reputation:	low
IE Cache URL:	<a href="http://https://fonts.gstatic.com/s/lora/v15/0QI6MX1D_JOuGQbT0gvTJPa787zAvBJBkqs.woff">http://https://fonts.gstatic.com/s/lora/v15/0QI6MX1D_JOuGQbT0gvTJPa787zAvBJBkqs.woff</a>
Preview:	wOFF.....Z.....0.....GDEF...l...z.....GPOS.....?K.GSUB.....OS/2.....N...`e!.dSTAT..!...1...6....cmap..!H.....r".@.gasp..".....glyf.."...2"..N"g _..head..U...6...6...hhea..UP.....\$b..hmtx..Up.....oloca..W.....maxp..Yd......name..Y...E...>b.post..Z.....2prep..Z.....h...x.....L.PH0.....@....R..c.H+.{t >w.....P0\$.BO.T.P..c?Q.....\a..d.....?p'..E...y...K...!..j./.....?.....x.T...A...f.k.m.b...m.m..N..)\'.!@..(W..~v-.Z.....!P...y.v.0...9....H*~.....E...H9.0..#...C.....}.g...? K.:?Y.+p..~!P.0.s...j}.7.7.q.5.....sl...s.8TG~.1...((.....U."M...Ssvr.....\!xO.?B...O.....!R..Z.."OE~...U(jPt..y1..cJ.....(N..Kh...N.....] ?K..~.euUpuq-rmp.s....+...7y.x.. ..Pq.P..lWy..']&c....i...JC...2...g.4...a.X.x...`3#..(.)0..BB..!b;..r"...H.6."m...G...E.Jd....C&..L.g..s3...W./X..pJ..8.5..."..~'.....JKb...Y+!..=f..A..3

<b>C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\E\KSU5XQMC\0QI8MX1D_JOuMw_hLdO6T2wV9KnW-PgFq92mg[1].woff</b>	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 25588, version 1.1
Size (bytes):	25588
Entropy (8bit):	7.980491911982066
Encrypted:	false
MD5:	58AE3BA621868D4A2DE07A5F73AD5D24
SHA1:	7F261C11C789900A4C0C9B96E3F00FBA8E6D29F9
SHA-256:	C6B3C67B8AF3AB83F0E74FEE66AFCE9721F216EC5A7D2FC4F48426288238E2D2
SHA-512:	8145D64002D6547B0844B62F6A79722F5226B040F6E29DE5A4FAACE7F2385F6B44F8631A5886DC4D2278C771F9E435CC7A80B52BB70627BF3596846357A37916
Malicious:	false
Reputation:	low
IE Cache URL:	<a href="http://https://fonts.gstatic.com/s/lora/v15/0QI8MX1D_JOuMw_hLdO6T2wV9KnW-PgFq92mg.woff">http://https://fonts.gstatic.com/s/lora/v15/0QI8MX1D_JOuMw_hLdO6T2wV9KnW-PgFq92mg.woff</a>
Preview:	wOFF.....c.....GDEF...l... .....SGPOS.....z..D.._IK.GSUB..ld.....D..y.OS/2.."...R...`d.5STAT.."....6...@....cmap..#.....rl.@.gasp..\$.....glyf..\$...9n..V. P.3.head..^O...6...6.p..hhea..^h...!..\$...hmtx..^.....b.Cloca..`.....?..maxp..b ......name..b....<...A.d.post..c.....2prep..c.....h...X.....\$d0I0.....@.J.@).....z...S t>w...>..".BO..0...#?V.(.SF~PX..k...Va...8...Y.p...<S..Vhh...P.5.B..GK..L..x.L...@.E...ZiT.m.m...j.....y.....Q..b%U.i.i...`o.[..!..!..8)m.K...7..=V(_"...j.M..DR.....Q...d.*.* ...k..."k...eT...tAM#m..8)..j...3.0..k.k.,~2..{5.....lEl.....>3.3~..G.3.Q.....r.s...%u.rMp.qol..-X.....2.y.?..[[<g.^4..-W.W.7...?.....?k.k.l.#.1;.... s.*P"...gB-p..H r%\$.beb....d.T.T.Ha..M.4GO.}1=0...xL..L#C1.3..%.ed"Vc.&a...8.8J...Nb...<g/...5."&"... ..x...-J.7.%..x...):g..).W'..?....."b(k.tq.s.l.co...jL.sX.[.o..y{.....@

<b>C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\E\KSU5XQMC\SIGDmQSNjdsmc35JDF1K5E55YMjF_7DPuGi-2fRkBI95[1].woff</b>	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 35140, version 1.1
Size (bytes):	35140
Entropy (8bit):	7.985168951591403
Encrypted:	false
MD5:	60ADDBDDEA9263655F411F26457FC023
SHA1:	A93CC65B3F29545EBB83238463AC151A8D2AD10E
SHA-256:	0183CCE439ABAF9356AA47EF3C433C605A8CDC05E732898322782480AB95A52D
SHA-512:	ED49D67BBC8A47532FBF58B885BE530F27191F74AB71F75A6E1E3D64851BA2CFF4478931BC6435EA89B64C2E8127C360D4673DE49794F2DB9481517A6906AD05
Malicious:	false
Reputation:	low
IE Cache URL:	<a href="http://https://fonts.gstatic.com/s/ebgaramond/v13/SIGDmQSNjdsmc35JDF1K5E55YMjF_7DPuGi-2fRkBI95.woff">http://https://fonts.gstatic.com/s/ebgaramond/v13/SIGDmQSNjdsmc35JDF1K5E55YMjF_7DPuGi-2fRkBI95.woff</a>
Preview:	wOFF.....D.....GDEF.....=...F...GPOS.....GSUB.....#.....OS/2.....S...`Y...STAT...D...8...D....cmap.. ...f...t..9cvt .....&^2pgm..... 6..gasp.....glyf.....g.....>.head.....6...6...hhea.....\$.lhmtx.....{.....kloca..h...l..lW@..maxp......name.....D...Dwh.post..8.....2prep..L.....&x...P.. ...".....l... .....*...y2..7{>..r..?R.....x.T...A.E..z7[.m.....m.m..juN..y...D.G. 5j5hA..#..lE..C...?s...9..a..T..hx...../...d...&..6W.s.B\$.D..g..a{.....KdW...f.....S\7.....x*. ...D.4...a...`G.S'L.r.LpXpm.X.@\x...B@r."..... .(...(A..S...HEC...0.G..OZ...L...D.s...8-ZsY..h.M...=DG.61...ID7.w...to9..+[d...>.g.yc.....}r.j6...D...+\$.RH"!..JiBi..T Nyy.....?....~Rv..n.6.....v/...!9..L.3r.T...t..".S...T.....l...rM.k.?..&.x.p...>(e...m3..K.....(..=i..WtP.n+2.Wx.i.^.{6...glz7sP.m..).)....9.n.

<b>C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\E\KSU5XQMC\SIGDmQSNjdsmc35JDF1K5E55YMjF_7DPuGi-6_RkBI95[1].woff</b>	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 33616, version 1.1

<b>C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\KSU5XQMC\SIGDmQSNjdsmc35JDF1K5E55YMjF_7DPuGi-6_RkBI95[1].woff</b>	
Size (bytes):	33616
Entropy (8bit):	7.9842194468743735
Encrypted:	false
MD5:	B3D44D9727786F711F8D9F0E0C2BA85E
SHA1:	A4A3C173DC64A572F3568A926460F7F8D5606ED1
SHA-256:	310EA45E98F6EF6721342ADD3E9263DB7F98EF7D5E92C85C94DC552F0F2B6FBA
SHA-512:	1E8F578C53DFB81FF171858D3E3F5F04E3EC7366A78B2A5E575DBED6106D12DCD0294484493192B5B1C8C0FB21D499163560A8CB6F9264D5927890571B7FAB66
Malicious:	false
Reputation:	low
IE Cache URL:	<a href="http://https://fonts.gstatic.com/s/ebgaramond/v13/SIGDmQSNjdsmc35JDF1K5E55YMjF_7DPuGi-6_RkBI95.woff">http://https://fonts.gstatic.com/s/ebgaramond/v13/SIGDmQSNjdsmc35JDF1K5E55YMjF_7DPuGi-6_RkBI95.woff</a>
Preview:	wOFF.....P.....GDEF.....=...F....GPOS.....V...\$GSUB.....#.....OS/2.....S...`X...STAT...l...8...D...cmap.....f...t...9cvt .....&^2fpgm.....6...gasp.....glyf.....e....d\$(\head...{...6...6...hhea...}...\$...lhmtx...}0...R.....}loca...~...l...lKay.maxp..... ..name.....2...@...^post...D..... ..2prep...X.....&...x....P.....".....l...;...*...y2...7{>...r...?R.....x...\$!.../c.y.z.v.v.m.zn...m.7...dowU.....?*"!#...&+...dY...[.]*...]u.5+Q.q.e.o.F.D.Y...9...[In...0.*...2...f.....iM`.~.x.z.x~.z.z.a=m=...E.L.#...\. ...oq.7.{W:u...w...9...o6.....+H... ..j...M.h*.M...J)T.E.q.Z.T...y...Xk4S...r...^R.^#{...8G.....<}.u.%4..L7.]2.F.....Z.....[{...Y.*...t.g.F.a...>RH#.,BD....._...^o..."-F_Q.-0.G ...x...x....G.:1. o.3.Z.?.....`.....Un.LZ3.=_K..l.W.d.&a...>..gh...}>y..W'.....\$....M.+..E.=n.o.dv.:bo.F...e....[.].",..

<b>C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\KSU5XQMC\SIGDmQSNjdsmc35JDF1K5E55YMjF_7DPuGi-DPNkBI95[1].woff</b>	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 35156, version 1.1
Size (bytes):	35156
Entropy (8bit):	7.985711973143503
Encrypted:	false
MD5:	5A3FD4B13DA3295810F2BA3EDC7FBDD6
SHA1:	CC1C0039369BBBD4592F0BD2CCB9888D3F01D12D7
SHA-256:	2BB8BD3D2C7ED0B05222692A0E8911BB590BCC357B2632028B608868DAF3449D
SHA-512:	404C28E0EB56EE3E83FB3678999BCA413E1F7DD2F8F72C95C24CF9A249F8CD4139FD8B6CA387E84EAE46E216586983DE303A6566871E3309EF0E84C88DAB235
Malicious:	false
Reputation:	low
IE Cache URL:	<a href="http://https://fonts.gstatic.com/s/ebgaramond/v13/SIGDmQSNjdsmc35JDF1K5E55YMjF_7DPuGi-DPNkBI95.woff">http://https://fonts.gstatic.com/s/ebgaramond/v13/SIGDmQSNjdsmc35JDF1K5E55YMjF_7DPuGi-DPNkBI95.woff</a>
Preview:	wOFF.....T.....GDEF.....=...F....GPOS.....VGSUB.....#.....OS/2.....S...`Y...STAT...H...9...D...cmap.....f...t...9cvt .....&^2fpgm.....6...gasp.....glyf.....h.....l.yhead.....6...6...hhea..... ..\$...lhmtx.....k...5...loca.....l...lZi.maxp..... ..name.....4...=*]Kpost...H..... ..2prep...l.....&...x....P.....".....l...;...*...y2...7{>...r...?R.....x...stdl..._ =O2:g.'t...6...m.m.Y...{.O..wo...\$2.R4N...g.....W.y.c...9.v. E.=s.!%...K...g.a.f.9.a.2...}.N../.....6...y...s..CP.m0x.....]>y.....{.....~...V...[.hB..Z..B{[...h".e.R5..4..r.P7%.nMV.z.T.k.#.u..+C..Nn.V.Dk.=..T.....q..."...;A..8X..c..O..LdRu..b..JF.....t.w...l.m...e....}d_5..?.....B.. \..G.l.y.x.m..6...WD.:z/...>".}u.."<...W.....~...~V".W.....%..i....2U.+...6...U.Q..6U7.T~V.....J..T?J%kl..q6v.e9T.J.%Z/?D}j}L.....'D=s}

<b>C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\KSU5XQMC\SIGDmQSNjdsmc35JDF1K5E55YMjF_7DPuGi-NfNkBI95[1].woff</b>	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 35320, version 1.1
Size (bytes):	35320
Entropy (8bit):	7.984184116884901
Encrypted:	false
MD5:	81440EDAB5FA679D55DA9464AE5797A8
SHA1:	46329E0C509623FFE672E2F2235E5CACAC19CB50
SHA-256:	2476CDD6ED5E282A9DF6A796E4158D223BB534866553A08CCD61E0F7B2AECE95
SHA-512:	6993A72483AC3F2EA2A82D5D708EB5E1024B3A1A58E2BA01766ECAE636D98553B874DC57659875FB9063BE056EE123451664B36D7452498F791FCBD848C5ACE3
Malicious:	false
Reputation:	low
IE Cache URL:	<a href="http://https://fonts.gstatic.com/s/ebgaramond/v13/SIGDmQSNjdsmc35JDF1K5E55YMjF_7DPuGi-NfNkBI95.woff">http://https://fonts.gstatic.com/s/ebgaramond/v13/SIGDmQSNjdsmc35JDF1K5E55YMjF_7DPuGi-NfNkBI95.woff</a>
Preview:	wOFF.....GDEF.....=...F....GPOS.....GSUB.....#.....OS/2.....Q...`Y...STAT...P...8...D.r.cmap.....f...t...9cvt .....&^2fpgm.....6...gasp.....glyf.....h.....head...H...6...6...hhea..... ..\$...lhmtx.....t.....)loca.....l...l.b..]maxp..... ..name.....l...E.i.post..... ..2prep...l.....&...x....P.....".....l...;...*...y2...7{>...r...?R.....x.T...[A.E...].m.m.j.n.F.j.m....=9.g..B..... E.....O.!H...u1...sP?.....*.....1 T.=.>f..bf..f..m..."-.\$Z.???.y.R.....=X.N{8....i...4...x~..U.D.4....a.....>./...o.....S,P P.O.KZ...l8d ...0.DB..D...)GyRP.z.!JGQ.....X&l.G9IS.V...)p[...h.C.'...0.LB..n.....f.....&{.....<3...>by.^7A.nj.gX.#y9%.....TR*..JKe.r..K^.{N=~.u.M..V);.}.N..#..D.=.=v.G.srl.....G.....Sw..D...C...kE.).8..&.j?...j...}.X.g.F..x....E...'.7....q.F.g"...t.....P.....G}.9v...m..

<b>C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\KSU5XQMC\SIGFmQSNjdsmc35JDF1K5GRwUjcdlttVFm-rI7diR799U64[1].woff</b>	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 36256, version 1.1
Size (bytes):	36256
Entropy (8bit):	7.9860408370540314
Encrypted:	false
MD5:	677A4940B58A6C72058EA6E7DAB02ED6
SHA1:	D042259677C3383F264DC264C2263CEE4996CE41
SHA-256:	30923EB7F16A37703017B56DC30A010BD4D667486F88047EFBF64583D580643C
SHA-512:	3C3A75C0E1057437697C511ACE0F758945D9A41CA29E1A6E3916A660851B21F835804EE684DDE0E7042D1427C4A2CDA5CF3D516E197E177A6B3AE524242D
Malicious:	false
Reputation:	low

<b>C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\KSU5XQMC\SIGFmQSNjdsmc35JDF1K5GRwUjcdlttVFm-r17diR799U64[1].woff</b>	
IE Cache URL:	<a href="http://https://fonts.gstatic.com/s/ebgaramond/v13/SIGFmQSNjdsmc35JDF1K5GRwUjcdlttVFm-r17diR799U64.woff">http://https://fonts.gstatic.com/s/ebgaramond/v13/SIGFmQSNjdsmc35JDF1K5GRwUjcdlttVFm-r17diR799U64.woff</a>
Preview:	wOFF.....GDEF.....M...j.X.GPOS.....3...b6...GSUB.....7... . @.OS/2...P...U...`Y...STAT.....6...@.p.cmap.....^...n.cvt ...@.....Q..Ofpgm...\$.....6..gasp.....glyf.....n&...F.8..head.....6...6.m..hhea...L...\$...\$.dhmtx...p.....X...loca.....e.maxp...8... ..name...X...@...+iNpost..... ..prep.....s=ax.....`.{. @. \$Z . !...(-.F.I.N.).l.....N{...tf.....; z[X.XZ.....d...x ...\$;...l...6.g.7.m.m.m{m.u.)O.<u..tU%..@...l.2...q..8.../+.zt...].L1...WF.l.....k.....3.K..m..#^F.MS...Ela..>2...;qKF."6.l.D\k.....o...hFo.?.o.XO.e.>~*^l.R{...g?.....<w...v3.gd.@.2\$e)...j.\Ug...z...".....t..0.L.4.....+^..u.....>...:G...{"..E\...K.[.t.j...r..9)..Po?Z}.t.....TDv9.}...:Q..y2t..z....q2.a. ....{1P}.b.4."S...T.V...!S.....h....Gu...>.c9.....6u..c.....qT.(.8..#{-V=-.b...+..0..4..M.?..0.....~.....\$l...0..hy...r.l.o[Z...

<b>C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\KSU5XQMC\SIGFmQSNjdsmc35JDF1K5GRwUjcdlttVFm-r17e8QL99U64[1].woff</b>	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 34660, version 1.1
Size (bytes):	34660
Entropy (8bit):	7.985342684210453
Encrypted:	false
MD5:	D600209A6764EA1EE8277CA6CA95BA6F
SHA1:	6965C47B2E21FA2C5A15B6715E37250D7C4A5520
SHA-256:	08643C3305F6AAA9172B4691458DA58E2E1C40135BA1332832C21607A835C558
SHA-512:	D7CF2B7E0F8A3BC0E7F922FE479636D9F346225662558B9E0366A94D52215267061EE13CB0278B57BB4C56571F6EA49BF7B6C83AA29EE118D928F7D51955BBD
Malicious:	false
Reputation:	low
IE Cache URL:	<a href="http://https://fonts.gstatic.com/s/ebgaramond/v13/SIGFmQSNjdsmc35JDF1K5GRwUjcdlttVFm-r17e8QL99U64.woff">http://https://fonts.gstatic.com/s/ebgaramond/v13/SIGFmQSNjdsmc35JDF1K5GRwUjcdlttVFm-r17e8QL99U64.woff</a>
Preview:	wOFF.....d.....GDEF.....M...j.X.GPOS.....>h..GSUB.....7... . @.OS/2.....U...`X...STAT.....6...@...cmap...d...^...n.cvt .....Q..Ofpgm.....6..gasp...h.....glyf...p.j....&x...head.....6...6.m..hhea...<...\$...\$.dhmtx...`.....X.\$..loca....._2Omaxp..... ..name...<.....j9.V.post...\. ..prep...t.....s=ax.....`. ..{. @. \$Z . !...(-.F.I.N.).l.....N{...tf.....; z[X.XZ.....d...x ...K...gU...g.m.6.....m.vX.q...u..o2s.....\$. 4..>.KiG.P.!..+/. ..@...v.5\].Y..N..Gs.9...s6..g..E.B;cB..8=..Y..n.O.3.....f...o..6....=...7^..6..f.5/..?~5...J.\$...S.....#>?.7.B.+9.....m...3..tc..4.....@...8+tr;.....q.....8...k...g..G. a..7.. .q.M.rR/^..b.....Df...~P.3..+Q.L.z...k*...../..FS-x...7.o.]x....%z....O.xu..d]...y..7..-#\\...izvgv4.pF.#.y.e.y.P....p.+@S...Nke...].E.<(V.T.r.....K{0}.u...].0.....V.Cku. ....0...../..d.*y.u.e

<b>C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\KSU5XQMC\SIGFmQSNjdsmc35JDF1K5GRwUjcdlttVFm-r17eOQL99U64[1].woff</b>	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 36180, version 1.1
Size (bytes):	36180
Entropy (8bit):	7.98493499870222
Encrypted:	false
MD5:	4286F64F063E6184BBCBE7379C15B629
SHA1:	9CF8D6BBC4C1544CAAC82A47401A11414E959A87
SHA-256:	6CCA18A82D089B014AB97C5978BEE4FF2EB59CD4E3510317B880AF0CB74AA20E
SHA-512:	526F9748F82C34F0906CAE31F771532847E0FFAA1C347D864EA8E599E833E5C3A3D551D85EC9EC8169E6B35F37B64177BDCC7754FDBC37568E3C77A8EAE6A76E
Malicious:	false
Reputation:	low
IE Cache URL:	<a href="http://https://fonts.gstatic.com/s/ebgaramond/v13/SIGFmQSNjdsmc35JDF1K5GRwUjcdlttVFm-r17eOQL99U64.woff">http://https://fonts.gstatic.com/s/ebgaramond/v13/SIGFmQSNjdsmc35JDF1K5GRwUjcdlttVFm-r17eOQL99U64.woff</a>
Preview:	wOFF.....T.....GDEF.....M...j.X.GPOS.....%..b=R#.GSUB.....7... . @.OS/2...D...U...`Y ..STAT.....6...@...cmap.....^...n.cvt ...4.....Q..Ofpgm... ..6..gasp.....glyf.....m.....head.....6...6.m..hhea.....\$...\$.dhmtx...(.....X...Rloca.....=Yamaxp..... ..name.....?...G.g.post...L..... ..prep...d.....s=ax.....`.{. @. \$Z . !...(-.F.I.N.).l.....N{...tf.....; z[X.XZ.....d...x ...\$l...0..6=..m.m.m{[...y...f..UgED...l.....j..h+...Q.(W.y..zp..G..t..9#3i.....D..\\@.N\ C..D...3....n. w.q. {..N.....S....]A.&.-.-&^pu..).X.....42.C...%a{42*.....^.....G..\$e(.....l.x.i...V!j-k...Fh.mKe.....N.Y...M...{lb..B.7..T.F.V..`u..).}....+..j...m.....f.k.....3...Z.."B.i..aX=k?J.....P...g_1...J...V.....u.Z8..T.P#&.V&a.....t<K...h%...../Pm.....g"-.-.l..^..Xu...>..._.;0+...o.7..}.VV.....T.}c.7....Dr.e....V..t.U.{

<b>C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\KSU5XQMC\TK3_WkUHHAljg75cFRf3bXL8LICs13FvsUZiYw[1].woff</b>	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 19852, version 1.1
Size (bytes):	19852
Entropy (8bit):	7.96652101671826
Encrypted:	false
MD5:	5CC7D7EE406E32DBAA00A811BE2956F2
SHA1:	8425499880A63CE1715AF0168E7E961822ABC60C
SHA-256:	0D42D15D51E5BB0CB59A26AEE176B25516D15F1C2DEB66E436507DBA20C07BDE
SHA-512:	B1B11899306DBCA112DA223A49471A1AFAFB558FE2F42AB98FAA205BA5FF2390FE4782737F0F449F303C2799C8CDBD6F42FAD0705C73AC1D89F486B6AA3AD45E
Malicious:	false
Reputation:	low
IE Cache URL:	<a href="http://https://fonts.gstatic.com/s/oswald/v31/TK3_WkUHHAljg75cFRf3bXL8LICs13FvsUZiYw.woff">http://https://fonts.gstatic.com/s/oswald/v31/TK3_WkUHHAljg75cFRf3bXL8LICs13FvsUZiYw.woff</a>
Preview:	wOFF.....M.....@.....GDEF.....E...^...nGPOS.....GSUB.....rOS/2.....O...`.>.STAT...@...&...*y.iUcmap...h.....n..@.cvt .....E.....s.fpgm...T.....6..gasp.....glyf... ..6...b.Kdhuhead..G...6...6...hhea..GP.....\$...\$.hmtx...(Gp...)....].\$.loca..l.....`maxp..Kx... ..<.;name..K...4...>zrjKpost..L..... ..2prep..L.....<l.x.....@P.....k@....z0.U.\$8...h0 ...l..R..l_..K.....N...r...k...x....]g.@.w.IV.m56wc.msTwX..(rP.v..{[...m.w...~-.@..iA..k..J..b..H..c..?s"...DH.f\$U.w.).4/.....{dH0+X..3b.<....`OxExC.. >Q.a.M...H.po.....Xv.A....hO.B.R.I.U.Ct0:HH...@:%..(M.*S.R..94..4.)hE;.. j..4a.3...a.]Y-=.\$=-".lc7.<(yX..L#.U..K.<.?#.Bf\p\$...K]..4S.\....G..>CD...j]..:..^..'..>wx'.')....v.kw.Z.O.o...a.\$..l..).Z)...@...5...ZW.i}m.M...Q'j'.].v...S.@{k.....4...u..N.).U..l5..X..%./.....%..2....ZKkk.....6.&...-=-"...V!...{.D...L...xH.q.g\$g...3...+9K...z..O.*oi

<b>C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\E\KSU5XQMC\TK3_WkUHHA\lg75cFRf3bXL8LICs169vsUziYw[1].woff</b>	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 19932, version 1.1
Size (bytes):	19932
Entropy (8bit):	7.967229171498271
Encrypted:	false
MD5:	34BD8BE6A179B0547377D9399A45EAA0
SHA1:	4F6012C4436879102E1B39D3892ABCA6D660FB1C
SHA-256:	EE8256CDE1EA6D97CB874344C303B2DF1B96119DD5A6F396C78E8AD66C9A60FD
SHA-512:	8E0120D033CB0613A51798001F1CDDBC2BFAC08AE3986A3CD8D86E48AF43820D1B8EF6817A7F5E2B3F278DA9A62BD3674C77EA10767B98B61AC5E219DBAD3A2E
Malicious:	false
Reputation:	low
IE Cache URL:	<a href="http://https://fonts.gstatic.com/s/oswald/v31/TK3_WkUHHA\lg75cFRf3bXL8LICs169vsUziYw.woff">http://https://fonts.gstatic.com/s/oswald/v31/TK3_WkUHHA\lg75cFRf3bXL8LICs169vsUziYw.woff</a>
Preview:	wOFF.....M.....GDEF.....E...^...nGPOS.....f.GSUB.....rOS/2.....O...`>.STAT...L...&...*y.i.cmap...t.....n..@.cvt .....E.....&fpgm...`.....6 ..gasp...\$......glyf....7J..b.p...head..Gx...6...6...hhea..G.....\$.hmtx..G....(....i.#.loca..l.....maxp..K....<.;name..K.....\8.ZEpost..M.....2prep..M0.....<l .x.....@P.....k@...z0.U.\$8...h0 ...l..R...l_..K.....N...r...k...x...p.l.O...;c.gb..8Y.vi...6J).UX.v.....N}....}.....Z*.WPv.RO.<.d.*\$l..usB..'+&F...b.....n.....p.)A...L.9.O.Y.n.; l.h.....w.;z/.m.F.k..{h7.%A.....O..Ac.R.F.Y.....IVY2.JJP.}.....TM.,eh..yZ.1Z.....T..t.j...U.k..A[u1.kQ...5..#T..2.5.9-w..T.G.Kz."Jr}....8.*...}...{..(.-...c.s..0'....!z )g!P.+7..9{.8+..v%X2 .^".....A"...D.J.l..~.DIS.O.i0.f.L...a...uh.....6.f...l.....J....(....8.*.....@..lg->j..Z.U...-c..R(.)..a.L.i0.f.L...a....._.....l...t}%PM+..P).L..np]~....\....*

<b>C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\E\KSU5XQMC\TK3_WkUHHA\lg75cFRf3bXL8LICs18NvsUziYw[1].woff</b>	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 20228, version 1.1
Size (bytes):	20228
Entropy (8bit):	7.965830219347884
Encrypted:	false
MD5:	5937C6CB6A7AD1219ECA4204286DD3B2
SHA1:	ACF9CB41FE123D1CCEBF80577CC73ACEAF720AC4
SHA-256:	4D59695F5305720802A4FFC0519420B95546FB9DD438A563706A769321AAF2E5
SHA-512:	1ADDD8080210411C6D558DEBCBDF93A90F0C01B6A99E5175B93F0EC5758D906CE39765504C06FA78521ACDCE098F7F1FC8DED8FB4525F946D3FFFAE29B33EE9
Malicious:	false
Reputation:	low
IE Cache URL:	<a href="http://https://fonts.gstatic.com/s/oswald/v31/TK3_WkUHHA\lg75cFRf3bXL8LICs18NvsUziYw.woff">http://https://fonts.gstatic.com/s/oswald/v31/TK3_WkUHHA\lg75cFRf3bXL8LICs18NvsUziYw.woff</a>
Preview:	wOFF.....O.....\.....GDEF.....E...^...nGPOS.....=.....x.GSUB.....rOS/2.....O...`>.STAT...p...&...*y.j.cmap.....n..@.cvt ...<...E.....].fpgm.....6 ..gasp...H.....glyf...P..8=.c....'head..H...6...6...hhea..H.....\$.hmtx..H.....Jloca..K.....~maxp..L.....<.;name..M...../...b9{Z.post..ND.....2prep..NX.....<l .....@P.....k@...z0.U.\$8...h0 ...l..R...l_..K.....N...r...k...x.l..7....m...y..5.6..qf...h>u ...y{..m@g.2.XU.t... ..t...3..Gl?h*%D*.\ju.54....'5}....].p.....*....O.W.u.....<l '.....T.S8...H..tOz....J.O.7..R....>..'@'.Q..KW.2..b....d.d....\2..T1.Z.....{...c9...b..lc...U..%Ts...F.E.....}.V..or.Jt..H...<?.v....#...gl.?...>.u?;Y...w.....0..Q.....\...9m....[...X.[ 8Xs..MTRAE.TV..+}.WC...e{..h..i.&h.....h..i.Vh.ViM..*U.Vu.W...uZ...M..-..uh.....<...g....w..._Fg...Fi..h..i.&h..h.+.#...?r..u0_...7t...4.....=.>&QpVr.W..8X..O#...O.l

<b>C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\E\KSU5XQMC\TK3_WkUHHA\lg75cFRf3bXL8LICs1_FvsUziYw[1].woff</b>	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 19740, version 1.1
Size (bytes):	19740
Entropy (8bit):	7.96718105168869
Encrypted:	false
MD5:	0E88EC239D6256E2C889DF2E3F0D51F2
SHA1:	6C1C1638CF7CCF809ADB7E22E3939252259B342D
SHA-256:	C2DE2E045916EC52E4C0CEE38FF283332551D4187262AFE453CA8C7153BAFEC
SHA-512:	1A304DDD9AA90E9E03310754EFE4BCFAB8BE659DC8A724608115FA32EA500C1AC37410062B7EDFBC1581587DA1BE8651310BB14AB3875226313884ACD88AF1F1
Malicious:	false
Reputation:	low
IE Cache URL:	<a href="http://https://fonts.gstatic.com/s/oswald/v31/TK3_WkUHHA\lg75cFRf3bXL8LICs1_FvsUziYw.woff">http://https://fonts.gstatic.com/s/oswald/v31/TK3_WkUHHA\lg75cFRf3bXL8LICs1_FvsUziYw.woff</a>
Preview:	wOFF.....M.....GDEF.....E...^...nGPOS.....v.GSUB.....rOS/2.....O...`>3>.STAT.....&...*y.j.cmap...4.....n..@.cvt .....D.....%.fpgm.....6 ..gasp.....glyf....6...b..N(head..F...6...6...hhea..F.....\$.hmtx..G...*.....loca..l@.....maxp..K....<.;name..K<.....B4.Q.post..L\.....2prep..Lp.....<l x.....@P.....k@...z0.U.\$8...h0 ...l..R...l_..K.....N...r...k...x...\$l@_U.k...m.3.g.]....{.../f.4.M.dR...K..%w...%....@0e.....\$J3.e..5.nA.Jr...r'...A\.....F...!l..*5=.. ...Q..ot{d. .B.J.V.E.J.K).DH....r.,P.I.R.*Q.B...>.hJK..\$.n.c(.l.l.:@:..\R.f.y<&W.t%:.....13...k<.d...%9.B{ .....="G..f..F[p_c_q.K<g..F...z...@.9.M....c.5..C.4.).i.....k%? W.*ZU.iu..5...Z..6.V.i{...vq...z.^W...y.Z...BG.(.ct.N...Z.{q..FF.C&..E..V.*ZU.iu..5.....9~s_..N.f..u'>..l.....[pM...!<3#u.0^..x..l{...4...}. .

<b>C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\E\KSU5XQMC\TK3_WkUHHA\lg75cFRf3bXL8LICs1y9osUziYw[1].woff</b>	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 20248, version 1.1
Size (bytes):	20248
Entropy (8bit):	7.964302094943577
Encrypted:	false
MD5:	6A98169CE7D291E352B05F574181E0BC

<b>C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\KSU5XQMC\TK3_WkUHHA\lg75cFRf3bXL8LICs1y9osUZiYw[1].woff</b>	
SHA1:	95D391FOB7868A42A8E4FBE65117EBF6107B096D
SHA-256:	0074E1A9794B23075A941C35490996F79AAAB6C4698FD0F4B5B0BEC8A7BEA3F1
SHA-512:	99A11C0592E1B061AD6FEB7F4A99FC2A23D2F361FFA42A4B307F0099A6BE171B947E12A91F86C4EBC4328AE2A7B4CE144645AC704964307C3818A756BDF6652C
Malicious:	false
Reputation:	low
IE Cache URL:	<a href="http://https://fonts.gstatic.com/s/oswald/v31/TK3_WkUHHA\lg75cFRf3bXL8LICs1y9osUZiYw.woff">http://https://fonts.gstatic.com/s/oswald/v31/TK3_WkUHHA\lg75cFRf3bXL8LICs1y9osUZiYw.woff</a>
Preview:	wOFF.....O.....t.....GDEF.....E..^...nGPOS.....B.....F.1GSUB.....rOS/2...\$.M...`>.STAT...t...&...*y.j.cmap.....n...@.cvt...@...E.....1fpgm.....6..gasp...L.....glyf...T..8L..c\$\\a.head..H....6...6...hhea..H.....\$....hmtx..H...*.....loca..K\$.....lmaxp..M.....<.;name..M...8...n:.[post..NX.....2prep..NL.....<I.x.....@P....k@....z0..U.\$8...h0 ...l..R...l..K.....N...f...k...x...pnG...={...}...f.=1...Am.V.F.gv...<...~./I).....*..T...9...;Jlb...(R..n.{+..H...G{...4zV=t%..i.7O...k...O...=e...?..?.....^b...}....Y..}.o?...f..*....(QR...s..&M.t...*4QK\...v.4.R\U.U.J-'......m.Yh..Aq...U..P..A...O..}.c\..v..^HP*...."m..v.)P.u..Y...t.HVK....1..X..W.....C..0X5.nN.....Y.fF...n...B...R\!..H...Y.g.....`>.....Q*...5...z...a3.....J.....`8...j.....NjT.J...V...G.J.O.<...a..y0...BX..\...79.t...#..._.....J.:Y..S9..U%..C.1.[Su..)dW"

<b>C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\KSU5XQMC\bootstrap[1].js</b>	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Size (bytes):	69126
Entropy (8bit):	4.875402738692249
Encrypted:	false
MD5:	8EF4C3CBA038D98C92143D2914621D6A
SHA1:	ACEF29390AAE8F95966512402C93ED82B5D4182D
SHA-256:	4436FF8EBFC05FFF3B2100853664A43C48B227B7CFDCA7E1FC64F765ED53DB3
SHA-512:	6E3AD181DEB497EDEA7FC5C02075EB488F028B783E2BCCFA2F5B1F8868A59FAD22154461BB5335DB2968E9D8F57F00BF2E6ED3264A53283092C72BFE9251B501
Malicious:	false
Reputation:	low
IE Cache URL:	<a href="http://https://campbaker.org/wp-content/plugins/booking/assets/libs/bootstrap/js/bootstrap.js?ver=3.3.5.1">http://https://campbaker.org/wp-content/plugins/booking/assets/libs/bootstrap/js/bootstrap.js?ver=3.3.5.1</a>
Preview:	/*! * Bootstrap v3.3.5 (http://getbootstrap.com). * Copyright 2011-2015 Twitter, Inc.. * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE). */./*!. * Generated using the Bootstrap Customizer (http://getbootstrap.com/customize/?id=f4b4c9cb85df757ca08c). * Config saved to config.json and https://gist.github.com/f4b4c9cb85df757ca08c. */.if (typeof jQuery === 'undefined') { throw new Error('Bootstrap's JavaScript requires jQuery').}.+function (\$) { 'use strict';. var version = \$.fn.jquery.split(' ')[0].split('.') . if ((version[0] < 2 && version[1] < 9)    (version[0] == 1 && version[1] == 9 && version[2] < 1)) { throw new Error('Bootstrap's JavaScript requires jQuery version 1.9.1 or higher'). }.}(jQuery);./* =====. * Bootstrap: alert.js v3.3.5. * http://getbootstrap.com/javascript/#alerts. * =====. * Copyright 2011-2

<b>C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\KSU5XQMC\client[1].css</b>	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Size (bytes):	13259
Entropy (8bit):	5.079999773424296
Encrypted:	false
MD5:	0764F745F34359AF3581B238F36D0891
SHA1:	C3B23637AD20CBDB5E9C38877C7A96201D45EAB9
SHA-256:	6EB58266134A0507D916EC403F0B4F5EBA85804101D1B119FFDD68875E2E9841
SHA-512:	9CEAD9829C092D971E4B2FEA20C5B9D708FF4B3E1BF87A72EC51EDFF758DAF3395AFBF5B3E7FFF69C7F2FCACAF92D0EF6994CA870CC9BFF03C9CDD40057EA15B0
Malicious:	false
Reputation:	low
IE Cache URL:	<a href="http://https://campbaker.org/wp-content/plugins/booking/css/client.css?ver=8.7.6">http://https://campbaker.org/wp-content/plugins/booking/css/client.css?ver=8.7.6</a>
Preview:	/*! * @version 1.0. * @package: Booking Calendar. * @category: Front-End. * @author wpdevelop. * * @web-site https://wpbookingcalendar.com/. * @email info@wpbookingcalendar.com . * . * @modified 2016-02-14. */./* Booking form structure //Fixln: 8.0.1.5 */..wpbc_booking_form_structure {..}.wpbc_booking_form_structure .wpbc_structure_calendar {..}.wpbc_booking_form_structure .wpbc_structure_form {..}.* form_center */..wpbc_booking_form_structure.wpbc_form_center { width:100%;}.wpbc_booking_form_structure.wpbc_form_center .wpbc_structure_calendar,..wpbc_booking_form_structure.wpbc_form_center .wpbc_structure_form { margin:1px auto;. width:290px;}./* form_dark */..wpbc_booking_form_structure.wpbc_form_dark .wpbc_structure_form label{ color:#ddd;}.wpbc_booking_form_structure.wpbc_form_dark .wpbc_structure_form input[type="text"],..wpbc_booking_form_structure.wpbc_form_dark .wpbc_structure_form textarea,..wpbc_booking_form_structure.wpbc_form_dark .wpbc_structure_

<b>C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\KSU5XQMC\client[1].js</b>	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Size (bytes):	77096
Entropy (8bit):	4.612761723928001
Encrypted:	false
MD5:	95314A0B10A250679A4BCF26E2FF6422
SHA1:	587F44C13487640D20F82FAA13956DDDF01640682
SHA-256:	0C518A3C844052008D81ADAC53C9981EBC918D2645DB7E3BE1A41D71F8929A41
SHA-512:	97215B4C2F382C62EDE0EC6C2A1752E60809BCACCCE65B346027829606E6C0D9F185064D86FEB2BA90152594F180992CB6153C6AE1EA39A4AFF86949F9434982
Malicious:	false
Reputation:	low



<b>C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\E\KSU5XQMC\client[1].js</b>	
IE Cache URL:	<a href="http://https://campbaker.org/wp-content/plugins/booking/js/client.js?ver=8.7.6">http://https://campbaker.org/wp-content/plugins/booking/js/client.js?ver=8.7.6</a>
Preview:	var is_booking_without_payment = false;var date_approved = [];var date2approve = [];var date_admin_blank = [];var dates_additional_info = [];var is_all_days_available = [];var avaibility_filters = [];var is_show_cost_in_tooltips = false;var is_show_cost_in_date_cell = false;var is_show_availability_in_tooltips = false;var global_avalaibility_times = [];var numbb = 0;var is_use_visitors_number_for_availability;var timeoutID_of_thank_you_page = null;...**. * Booking Calendar - JavaScript Settings. *. * Example or redefine some settings:. * <script type="text/javascript"> wpbc_settings.set_option( 'pending_days_selectable', true ); </script>. * [booking type=1]. * //FixIn: 8.6.1.18. */var wpbc_settings = (function ( obj, \$) {...// Define private property..var p_options = obj.options = obj.options    [];...p_options['pending_days_selectable'] = false;...// Get Option..obj.get_option = function ( item_id ) {...return p_options[ item_id ];};...// Set Option..obj.s

<b>C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\E\KSU5XQMC\flickity.min[1].css</b>	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Size (bytes):	2025
Entropy (8bit):	4.9243449923780025
Encrypted:	false
MD5:	DE74FC91BEDE5288675C1D7D13256F53
SHA1:	E1A39B0B821B69C4C580D4C5AA6DCEDA41C91E81
SHA-256:	FA65E5F741FE4A01C598BE6DF67B5A1AC8F996E1B37D421E0F2A0A3E36788EA2
SHA-512:	79297C004169C02326D3C01B5E7DEFF24E1B1863E99BF789414B9D32F6F20FEFDB72B439DC9DB66D555FDADB69CF6136FB6EE9B17A815C7DDF190636F35CF516
Malicious:	false
Reputation:	low
IE Cache URL:	<a href="http://https://campbaker.org/wp-content/themes/diwine/css/flickity.min.css?ver=5.4.1">http://https://campbaker.org/wp-content/themes/diwine/css/flickity.min.css?ver=5.4.1</a>
Preview:	/*! Flickity v2.0.2..http://flickity.metafizzy.co..----- */..ul.flickity-enabled{padding-left: 0 !important;margin-left: 0 !important;}...flickity-enabled{position:relative;margin-bottom: 70px;}.flickity-enabled.pagedots-false{margin-bottom: 0;}.flickity-enabled:focus{outline:0;}.flickity-viewport{overflow:hidden;position:relative;height:100%;}.flickity-slider{position:absolute;width:100%;height:100%;}.flickity-enabled.is-draggable{-webkit-tap-highlight-color:transparent;tap-highlight-color:transparent;-webkit-user-select:none;-moz-user-select:none;-ms-user-select:none;user-select:none;}.flickity-enabled.is-draggable .flickity-viewport{cursor:move;cursor:-webkit-grab;cursor:grab;}.flickity-enabled.is-draggable .flickity-viewport.is-pointer-down{cursor:-webkit-grabbing;cursor:grabbing;}.flickity-prev-next-button{position:absolute;top: 50%;width:44px;height:44px;border:none;background-color:rgba(0,0,0,.2);cursor:pointer;-webkit-transform:translateY(-50%)

<b>C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\E\KSU5XQMC\font.min[1].css</b>	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Size (bytes):	59662
Entropy (8bit):	4.615114437965821
Encrypted:	false
MD5:	A42BEF955E4495114089EDB107115858
SHA1:	D38B3C26D29654A9438B163AADA642FAD026785B
SHA-256:	F06391A9380345198934407A4980EC4FADDB146C91ABFD59CAC2FA01399A2425
SHA-512:	148633C8C77249188962DFF698DFC9158F32BB6D78C55DA62DF505015AB5D9269F3CD9BA7A52E88946B011C8366856220FA3658D074F85C4797F7614647E7DC1
Malicious:	false
Reputation:	low
IE Cache URL:	<a href="http://https://campbaker.org/wp-content/themes/diwine/font/font.min.css?ver=5.4.1">http://https://campbaker.org/wp-content/themes/diwine/font/font.min.css?ver=5.4.1</a>
Preview:	@charset "UTF-8";@font-face{font-family:"ozythemes";src:url("ozy/fonts/ozythemes.eot");src:url("ozy/fonts/ozythemes.eot?#iefix") format("embedded-opentype"),url("ozy/fonts/ozythemes.woff") format("woff"),url("ozy/fonts/ozythemes.ttf") format("truetype"),url("ozy/fonts/ozythemes.svg#ozythemes") format("svg");font-weight:normal;font-style:normal}@media screen and (-webkit-min-device-pixel-ratio:0){@font-face{font-family:'ozythemes';src:url("ozy/fonts/ozythemes.svg#fontset") format("svg")}}[data-icon]:before{font-family:"ozythemes";content:attr(data-icon);font-style:normal!important;font-weight:normal!important;font-variant:normal!important;text-transform:none!important;position:absolute;top: 50%;width:44px;height:44px;border:none;background-color:rgba(0,0,0,.2);cursor:pointer;-webkit-transform:translateY(-50%)

<b>C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\E\KSU5XQMC\frontend-style[1].css</b>	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Size (bytes):	773
Entropy (8bit):	4.92216752045998
Encrypted:	false
MD5:	4AB6737F61FA5852E9310587224627CC
SHA1:	6829F17A30FE694B5B582D43B40AFFB671E1F8CD
SHA-256:	DD47157157687391ACE14A7952DDF1CB2D78EAD0E2D02391E72CF1B983FE6026
SHA-512:	44FE0547880B3771AA24F828569FFD6702E52ACB6ECC49CDB71B729F3AEBBFBCDFB35C4B928FA66F0AD071F08D4CCA724561319640520EC63CF043181DABE78
Malicious:	false
Reputation:	low
IE Cache URL:	<a href="http://https://campbaker.org/wp-content/plugins/booked-woocommerce-payments/css/frontend-style.css?ver=5.4.1">http://https://campbaker.org/wp-content/plugins/booked-woocommerce-payments/css/frontend-style.css?ver=5.4.1</a>



C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\KSU5XQMC\frontend-style[1].css	
Preview:	.paid-variations { margin-top: 10px; }...body #booked-profile-page .booked-profile-appt-list .appt-block .pay,...body #booked-profile-page .booked-profile-appt-list .appt-block .edit { font-size:12px; padding-left:10px; border:1px solid #ccc; background:#eee; color:#888; }..body #booked-profile-page .booked-profile-appt-list .appt-block .pay:hover, ..body #booked-profile-page .booked-profile-appt-list .appt-block .edit:hover { background:#ddd; }....div.booked-wc-checkout-section { line-height:1.3; padding:0 0 10px; }...woocommerce-checkout-review-order div.booked-wc-checkout-section:last-child { padding:0; margin:0 0 -1.4em; }....span.booked_wc_payment_pending { color: #E35656; font-weight:600; }..span.booked_wc_payment_completed { color:#000; font-weight:600; }..

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\KSU5XQMC\icons[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Size (bytes):	11040
Entropy (8bit):	6.005800404503291
Encrypted:	false
MD5:	0E5C7E85AC425DB35DF81D0F587B4704
SHA1:	877C006E4D15B85513A956ACB4EB33D94F5C1823
SHA-256:	E32F18022A5DDB2F3168BC12781ADCBE741B5B34CB775161EFFCCFE7BF5E6FF
SHA-512:	FE5083D9BE8E96076BF23DF8533015305AA35570EDB9D41BAED0D87AC2A02DB269AD2097CB896359809BB1B7717765CBDD92925D75F90C507E19C2291BECB7A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://campbaker.org/wp-content/plugins/booked/assets/css/icons.css?ver=2.2.6
Preview:	@font-face{font-family:"BookedIcons";src:url(data:application/font-woff;charset=utf-8;base64,d09GRGABAAAAABWkAA0AAAAAAIrQAAAAAAAAAAAAAAAAAAAAAABGRIRNAAAVIAAAABoAAAAcgEOAw09TLzIAAAGkAAAAARQAAAGAQ+ZHdY21hcAAAAjwAAABgAAABcuCe68VjdnQgAAACnAAAAAQAAAAEACECf2dhc3AAABWAAAAACAAAAaj/wADZ2x5ZgAAAYAAABBMAAAZila7HAZoZWfkAAABMAAADQAAAA2Dwe+OmhoZWEAAAFkAAAAIAAACQlwwXfaG10eAAAAewAAABOAAAA+OxuAOpsb2NhAAACoAAAAH4AAAB+trCwem1heHAAAGAAAAHwAAACAAhwCzbmFIZQAAE4gAAAEMAAAB+AVCGRRwb3N0AAAAUIAAAAOoAAAJmx+JtA3jaY2BkYGA4AolPN3f89t8ZeBm/gAUyBhatJcTSnP9//w/mVWA+TqQy8HABBIFAIWfDbt42mNgZGBgTmCYwBDNKvD/MwMDqwADUAQF2AEAV+IDq3jaY2BkYGCwY2hiYGCaASYgZmQAIkTw6IEEABb8ATsAeNpjYGH+yjiBgZWBgamf6SADA0MvhGZ8zGDEyAIUZWBIZoABRgEGNNDAwPDBnjjhfwFDNHMCwwQglxJVJoGBEQBsSAtvAAAAeNpjzGFQZAAcXgAGBuYPGJiDpQGrOANIHIaxyUoElhmcbgBjWQ5pgslvchmYBNjTsC0G27O4v+fgXQoGKOpY2UDqv2BjiYAoQEJ5zMUAAB42mNgYGBmgGAZBkYGEgB8hjBfBaGACAtAITMYBleBoUPrB8UPhh8sP//Hy7C8oHjg9lHI6AI8//v/58KMAkw8P/nwc1DQUwsjFAjQKymYAEC7oCBgZWhuENAOINFCMAIQJ/AAAAKgAqACo

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\KSU5XQMC\isotope.pkgd.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Size (bytes):	35722
Entropy (8bit):	5.0905752391464825
Encrypted:	false
MD5:	38FC018B2A3E21B4FC9D85C31055FBE1
SHA1:	9080223675416C00AA51161DDDC90CCC27E2905F
SHA-256:	808975B6CF4AE51C0555C592409A545A54A842EACDE7C5408F6D77FCC754CC61
SHA-512:	91CA13FCDD504382F8DE0BE0D654C274F117637E47A410811D1D5E4632C8E9FD20F312435BCDC5B0E89E7901F43B09A11D915529ABD49EDB9FF41C1C882BEA3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://campbaker.org/wp-content/plugins/js_composer/assets/lib/bower/isotope/dist/isotope.pkgd.min.js?ver=6.1
Preview:	/*! * WPBakery Page Builder v6.0.0 (https://wpbakery.com). * Copyright 2011-2019 Michael M, WPBakery. * License: Commercial. More details: http://go.wpbakery.com/licensing. */...! jscs:disable // jshint ignore: start. /*! * Isotope PACKAGED v3.0.5. * * Licensed GPLv3 for open source use. * or Isotope Commercial License for commercial use. * * https://isotope.metafizzy.co. * Copyright 2017 Metafizzy. */...function(t,e){"function"==typeof define&&define.amd?define("jquery-bridget/jquery-bridget",["jquery"],function(){return e(t,i)}):"object"==typeof module&&module.exports?module.exports=e(t,require("jquery")):t.jQueryBridget=e(t,t.jQuery)}(window,function(t,e){"use strict";function i(i,s,a){function u(t,e,o){var n,s="\$()."+i+"("+e+")";return t.each(function(t,u){var h=a.data(u,i);if(!h)return void r(i+" not initialized. Cannot call methods, i.e. "+s);var d=h[e];if(!d  "_"==e.charAt(0))return void r(s+" is not a valid method");var l=d.apply(h,o);n=void 0===n?!n},void 0)!=n?n:t}fu

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\KSU5XQMC\jquery.datepick[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Size (bytes):	98302
Entropy (8bit):	5.1593909672933576
Encrypted:	false
MD5:	4023E52A4524B3860DF0353E3CE26F82
SHA1:	81EB8056E1C806CF74282A7CB4DF3999446C717F
SHA-256:	AF102962981CD70B4F24D7D1905A9EC63958044FA42D6EB8F37E04B4D27919FF
SHA-512:	E9D6CB7964D3DC22D21B40F172DCC475126F71B87914072FA357A432375C7205C2EBB5AEC6E54BF821DE671DF9808F406A083BC731082F143D8C1574A2947D38
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://campbaker.org/wp-content/plugins/booking/js/datepick/jquery.datepick.js?ver=1.1

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\KSU5XQMC\jquery.datepick[1].js	
Preview:	<pre>/* http://keith-wood.name/datepick.html.. Datepicker for jQuery 3.7.1... Written by Marc Grabanski (m@marcgrabanski.com) and.. Keith Wood (kbwood{at}iine t.com.au)... Dual licensed under the GPL (http://dev.jquery.com/browser/trunk/jquery/GPL-LICENSE.txt) and.. MIT (http://dev.jquery.com/browser/trunk/jquery/MIT- LICENSE.txt) licenses... Please attribute the authors if you use it. */... (function (\$) { // Hide the namespace... var PROP_NAME = 'datepicker';... /* Date picker manager... Use the singleton instance of this class, \$.datepicker, to interact with the date picker... Settings for (groups of) date pickers are maintained in an instance object... allowing multiple different settings on the same page. */... function Datepick() { ... this._uid = new Date().getTime(); // Unique identifier seed... this._curInst = null; // The current ins tance in use... this._keyEvent = false; // If the last event was a key event... this._disabledInputs = []; // List of date picker in</pre>

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\KSU5XQMC\packery-mode.pkgd[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Size (bytes):	32670
Entropy (8bit):	4.947778003325715
Encrypted:	false
MD5:	4F56F376C28E24828176A5F5742ABDB7
SHA1:	D8F3E41B7685853F4187A1C37A96863BADF1FBE7
SHA-256:	FFE8B498FD01EDB7097201A8B82B41BB1A2E7F2B8002705E53485A1D1F686ED9
SHA-512:	188FE74D4BE995C4355C9903F383F257C3AE0EE034ECE62D106EB04580173A9B4E364751CA54044C8AE8099BE9B5241E2AB41248FECF4BF3F21C36608B1DA8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://campbaker.org/wp-content/themes/diwine/scripts/vendor/isotope/packery-mode.pkgd.js?ver=5.4.1
Preview:	<pre>/*!.. * Packery layout mode PACKAGED v2.0.0.. * sub-classes Packery.. */... /* Rect.. * low-level utility class for basic geometry.. */... ( function( window, factory ) {.. // universal module definition.. /* jshint strict: false */ /* globals define, module */.. if ( typeof define == 'function' &amp;&amp; define.amd ) {.. // AMD.. define( 'packery/js/rect', fact ory );... } else if ( typeof module == 'object' &amp;&amp; module.exports ) {.. // CommonJS.. module.exports = factory();... } else {.. // browser global.. window.Packery = win dow.Packery    {};.. window.Packery.Rect = factory();... }... }( window, function factory() {.....// ----- Rect ----- //....function Rect( props ) {.. // extend properties from defaults.. for ( var prop in Rect.defaults ) {.. this[ prop ] = Rect.defaults[ prop ];... }.... for ( prop in props ) {.. this[ prop ] = props[ prop ];... }.. }....Rect.defaults = {.. x: 0,.. y: 0,.. width: 0,.. h</pre>

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\KSU5XQMC\rsvp_plugin[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Size (bytes):	829
Entropy (8bit):	4.894043624337833
Encrypted:	false
MD5:	48A07D0292EA001F0002416F5A7FAC33
SHA1:	3D221E98595951F1E09655A7A9A7CD7C317263E2
SHA-256:	5EC5E4DE606A7A1F2E49A1C370CAAEF4540F96FBD19D0734033B1C6BC78D0DFC
SHA-512:	F06E870536934338F0BCC7C91A247DC5557B7FCA3400D91A2823E588600ED89F1A023A467038D656BF49850CD7D3BC3A1A9F617E20FFAC9C4F12A2FB521F1B1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://campbaker.org/wp-content/plugins/rsvp/rsvp_plugin.css?ver=5.4.1
Preview:	<pre>label.error { font-weight: bold; clear: both; }.input.error, textarea.error { border: 2px solid red; }.rsvpFormField { margin: 10px 0px; }.#rsvpCustomGreeting { margin-top: 20px; margin-bottom: 20px; }.rsvpBorderTop { border-top: 1px solid #ccc; }.rsvpAdditionalAttendee { text-align: left; border-top: 1px solid #ccc; }.rsvpCheckboxCus tomQ { float: left; padding-right: 10px; }.rsvpClear { clear: both; height: 1px; line-height: 1px; }.#rsvpPlugin input { display: inline; visibility: visible; }.#rsvpPlugin in put[type="radio"], #rsvpPlugin input[type="checkbox"] { display: inline !important; }.rsvpFormField label { display: inline; }.rsvpParagraph { position: relative; }.rsvp Paragraph .required { position: relative; }.#rsvp_upgrade_to_pro_link { font-weight: bold; color: red; }</pre>

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\KSU5XQMC\style-classic-menu[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Size (bytes):	24605
Entropy (8bit):	5.106987826192578
Encrypted:	false
MD5:	8077755CABC4BF05F4CC9DC553B3AE26
SHA1:	9C41EBAC96CFE6FD6E598A378E1CB66333D9EF40
SHA-256:	F9CADEFD0C5019DF44A13F7C1863204FA64FB91FC27B2832E0F1C92D80AED78C
SHA-512:	7FE15A6B890352D04BBA227968962B09AF8C2B9E4E897D9A4CD06041B10620F79BD9EA60835A0C7603B1988D51D5AE00D08915E7507C84B93CBBBD71C383AA66
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://campbaker.org/wp-content/themes/diwine/css/style-classic-menu.css?ver=5.4.1
Preview:	<pre>.nav-container {.. position: fixed;.. width: 100%;... top: 0;...left: 0;...right: 0;.. z-index: 999;...}.nav-container .diwine-primary-nav&gt;li&gt;a {...text-transform: uppercase;... font-weight: 500;...}.nav-container&gt;div {...margin: 0 auto;...}.diwine-primary-nav {...display: block;...max-width: 45%;...float: left;...}.diwine-primary-nav[id="-right"] {...float: right;...}.@media only screen and (min-width: 769px) {...diwine-primary-nav&gt;li:first-child&gt;a {...padding-left: 0;...}.diwine-primary-nav:last-child&gt;li:not(.dropdown):nth-last- child(2)&gt;a {...padding-right: 0;...}.diwine-primary-nav&gt;li.logo {...margin-left: auto;...margin-right: auto;...}.diwine-primary-nav&gt;li.logo&gt;a {...padding: 10px 0 !important;.. margin-top: -20px; /*half height of top info bar*/...}.diwine-primary-nav&gt;li.logo img {...height: 100%;...}.menu-top-section {...overflow: hidden;...color: var(--text-color);... height: 40px;...line-height: 40px;...max-height: 40px;...}.menu-top-section&gt;div</pre>

<b>C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\E\KSU5XQMC\style[1].css</b>	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Size (bytes):	66058
Entropy (8bit):	5.143844050339833
Encrypted:	false
MD5:	E7E6A0406A3FC00F71BEC2706C3D7C75
SHA1:	7D978C127F614128616A6D6D0F628728BD7BBC88
SHA-256:	A68103CF6F0359010607EAC8ECCA00CC18F75F820928FBC280D20E4B3E860702
SHA-512:	1A4AD7AE01E3F3A173EE28BCF202A494F4A98257F6794AD1E3A6CAA0589CE6CD35D5A57960A8EBC7C5D84C9BE82562200D063D02B9025DA8AFCAA2A675F386D3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://campbaker.org/wp-content/plugins/woocommerce/packages/woocommerce-blocks/build/style.css?ver=2.5.16
Preview:	.wc-block-featured-category{position:relative;background-color:#24292d;background-size:cover;background-position:50%;width:100%;margin:0 0 1.5em}.wc-block-featu red-category,.wc-block-featured-category .wc-block-featured-category__wrapper{display:-webkit-box;display:flex;-webkit-box-pack:center;justify-content:center;-webkit-box- align:center;align-items:center;flex-wrap:wrap;align-content:center}.wc-block-featured-category .wc-block-featured-category__wrapper{overflow:hidden;height:100%}.wc- block-featured-category.has-left-content{-webkit-box-pack:start;justify-content:flex-start}.wc-block-featured-category.has-left-content .wc-block-featured-category__ description,.wc-block-featured-category.has-left-content .wc-block-featured-category__price,.wc-block-featured-category.has-left-content .wc-block-featured-category__titl e{margin-left:0;text-align:left}.wc-block-featured-category.has-right-content{-webkit-box-pack:end;justify-content:flex-end}.wc-block-featured-category.has-right-content

<b>C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\E\KSU5XQMC\style[2].css</b>	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Size (bytes):	176396
Entropy (8bit):	5.224714103655058
Encrypted:	false
MD5:	2C203426EA626415DF21240B600A9B7F
SHA1:	7084A3C2B290545EA041116D5144EFE51CFA2E47
SHA-256:	E47A5C971573CA032922EBFEB95F083C84EB34890079316DBF158245CBE414E6
SHA-512:	59CA9CD4E26D474667966BAFD46F9A2C9F7AF8349E5B81D70F09BC93B8091109C1657860F96C6EB1DE76804222BAC8F8DB2BD8C87D9FB59319F7509FA43C893
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://campbaker.org/wp-content/themes/diwine/style.css?ver=5.4.1
Preview:	@charset "utf-8";.../*..Theme Name: Baker..Theme URI: http://diwine.freevision.me/..Author: freevision..Author URI: http://theforest.net/user/freevision/portfolio..Descr iption: Baker WordPress theme is a standout not for the excellent imagery and fonts (both beautiful), but for the concept. Baker is specially designed for all the wineries, wine shops & bars, online wine sales, breweries, blogs, vineyards as well as independent dining, restaurants and premium bars and cafes. Winery theme is a delightful w ine responsive multi-purpose template...Version: 1.2..Text Domain: diwine..Domain Path: /lang..License: GNU General Public License v2 or later..License URI: htt p://www.gnu.org/licenses/gpl-2.0.html..Tags: one-column, two-columns, right-sidebar, custom-header, custom-menu, editor-style, featured-images, microformats, post- formats, sticky-post, translation-ready..*/.../*..[Table of contents]..1 - Resets..2 - Typography presets..3 - Mono social icon font..4 - Default layout..5 - If is ad

<b>C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\E\KSU5XQMC\timeline_v2[1].js</b>	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Size (bytes):	8244
Entropy (8bit):	5.947403526754274
Encrypted:	false
MD5:	203517F0F13A3E58D178C368CE5D2AA9
SHA1:	1205D0B8D99D7BABEA8D338C2D5804848CE1D2C7
SHA-256:	31AC56C0455B8793B6BF2B5445CC0D6EBABD50DA8B32D844D36E995565BC44A0
SHA-512:	5CE5312060DA8345FBFFFA7B5334045640A480D504A496CFF470A25D6DB40B15718B312B84281496E16CEE6152D07D1BFC82465AF8D492CDA9573D46DBEF9518
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://campbaker.org/wp-content/plugins/booking/core/timeline/v2/_out/timeline_v2.js?ver=8.7.6
Preview:	"use strict";...function wpbc_flextimeline_nav(timeline_obj, nav_step) { . jQuery(".wpbc_timeline_front_end").trigger("timeline_nav", [timeline_obj, nav_step]); //FixIn:7. 0.1.48. // jQuery( '#'+timeline_obj.html_client_id + ' .wpbc_tl_prev,#'+timeline_obj.html_client_id + ' .wpbc_tl_next').remove();. // jQuery( '#'+timeline_obj.html_client_id + ' . wpbc_tl_title').html( '<span class="glyphicon glyphicon-refresh wpbc_spin"></span> &nbsp; Loading...'); // '<div style="height:20px;width:100%;text-align:center;marg in:15px auto;">Loading ... <img style="vertical-align:middle;box-shadow:none;width:14px;" src="" +wpdev_bk_plugin_url+"/assets/img/ajax-loader.gif"></div>'.. jQuery( '#'+ timeline_obj.html_client_id + ' .flex_tl_prev,#'+ timeline_obj.html_client_id + ' .flex_tl_next').remove();. jQuery( '#'+ timeline_obj.html_client_id + ' .flex_tl_title').html('<span class="glyphicon glyphicon-refresh wpbc_spin"></span> &nbsp; Loading...'); // '<div style="height:20px;width:100%;text-align

<b>C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\E\KSU5XQMC\woocommerce[1].css</b>	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Size (bytes):	62511
Entropy (8bit):	4.8520199693148
Encrypted:	false
MD5:	A5AECABFF1E91F708586E81F991E450A

<b>C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\KSU5XQMC\woocommerce[1].css</b>	
SHA1:	B58AEC5B2776053A1C0D2D319B79A0E7473D1921
SHA-256:	AE3F857E0ECEBDF3782B884B2BB1937E67B065AF2F5F1C813588CB94D4C8BA82
SHA-512:	9EAB7C1126D0B31B39CC81508F5AD1C35B1203C30FBF50ADF5F5C4D52B7035D7267FF34BA0E69A4764816DD5CC259A3BF40849CD25AA796E0D478605BE3B280
Malicious:	false
Reputation:	low
IE Cache URL:	<a href="http://https://campbaker.org/wp-content/plugins/woocommerce/assets/css/woocommerce.css?ver=4.1.1">http://https://campbaker.org/wp-content/plugins/woocommerce/assets/css/woocommerce.css?ver=4.1.1</a>
Preview:	@charset "UTF-8";@-webkit-keyframes spin{100%{-webkit-transform:rotate(360deg);transform:rotate(360deg)}}@keyframes spin{100%{-webkit-transform:rotate(360deg);transform:rotate(360deg)}}@font-face{font-family:star;src:url(..\fonts/star.eot);src:url(..\fonts/star.eot?#iefix) format("embedded-opentype"),url(..\fonts/star.woff) format("woff"),url(..\fonts/star.ttf) format("truetype"),url(..\fonts/star.svg#star) format("svg");font-weight:400;font-style:normal}@font-face{font-family:WooCommerce;src:url(..\fonts/WooCommerce.eot);src:url(..\fonts/WooCommerce.eot?#iefix) format("embedded-opentype"),url(..\fonts/WooCommerce.woff) format("woff"),url(..\fonts/WooCommerce.ttf) format("truetype"),url(..\fonts/WooCommerce.svg#WooCommerce) format("svg");font-weight:400;font-style:normal}.woocommerce-store-notice,p.demo_store{position:absolute;top:0;left:0;right:0;margin:0;width:100%;font-size:1em;padding:1em 0;text-align:center;background-color:#a46497;color:#fff;z-index:9999;box-shadow:0 1px 1em rgb

<b>C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\KSU5XQMC\wpbc-migrate[1].js</b>	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Size (bytes):	2418
Entropy (8bit):	4.665316833604038
Encrypted:	false
MD5:	DD05C0C1D6CAA5A1DDEABD13F44C832B
SHA1:	B723312019C275C9B6B1433B1017BDC4FA652F14
SHA-256:	4D0BB3443BAD8E0A12CD34FA582107DAFE27B038D85478E690F6DE17D7958D9C
SHA-512:	DDB2DC56079EEB743970BB3D1C67A1C2EAE9FD49160C4A2BC850F92ABEB5D707C9B1EF37C53BDAE1DB86D24FF1462683B4FD4B5701EE067E5AEC1CD078EE8BD
Malicious:	false
Reputation:	low
IE Cache URL:	<a href="http://https://campbaker.org/wp-content/plugins/booking/js/wpbc-migrate.js?ver=1.1">http://https://campbaker.org/wp-content/plugins/booking/js/wpbc-migrate.js?ver=1.1</a>
Preview:	(function() { ... var matched, browser; ... jQuery.uaMatch = function( ua ) { ua = ua.toLowerCase(); ... var match = /(chrome)[ \/]([\w.]+)/.exec( ua )    . /(webkit)[ \/]([\w.]+)/.exec( ua )    . /(opera)(?:.*version ) [ \/]([\w.]+)/.exec( ua )    . /(msie) [ \/]([\w.]+)/.exec( ua )    . /(trident)?(?:.*rv:([\w.]+)))/.exec( ua )    . ua.indexOf( "compatible" ) < 0 && /(mozilla)(?:.*? rv:([\w.]+)))/.exec( ua )    . []; ... return { browser: match[ 1 ]    "", version: match[ 2 ]    "0" }; ... matched = jQuery.uaMatch( navigator.userAgent ); ... //IE 11+ fix (Trident).. matched.browser = matched.browser == 'trident' ? 'msie' : matched.browser; ... browser = {}; ... if ( matched.browser ) { browser[ matched.browser ] = true; ... browser.version = matched.version; ... } ... // Chrome is Webkit, but Webkit is also Safari... if

<b>C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\KSU5XQMC\wpbc_times[1].js</b>	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Size (bytes):	53955
Entropy (8bit):	5.075457307363245
Encrypted:	false
MD5:	D3E5E28B116A162722B565F2CB0E28BC
SHA1:	4B43BB7E69F1F1D38BAD76F2317BB4EED6F6AA11
SHA-256:	0494DD05C411B253247A4BFCA1456B45853A5CB07DB47F33E8E09B62E2CBF325
SHA-512:	CD701B320ADF917CF95BFED636EBF8B832D0E277CDA54AB7F4F90B9FBF71F5F763AF94B189B3CB641FC1488A7EAE8C43733C32FD25F12BB8FF6806DB1F939790
Malicious:	false
Reputation:	low
IE Cache URL:	<a href="http://https://campbaker.org/wp-content/plugins/booking/js/wpbc_times.js?ver=8.7.6">http://https://campbaker.org/wp-content/plugins/booking/js/wpbc_times.js?ver=8.7.6</a>
Preview:	var time_buffer_value = 0;.....// Customization of bufer time for DAN..var is_check_start_time_gone = false;..// Check start time or end time for the time, which is gone already TODAY...var start_time_checking_index;.....//Fixln: Deprecated..function prepare_tooltip( myParam ){...wpbc_set_popover_in_cal( myParam );...}.....//Fixln: Deprecated..function hoverDayTime( value, date_obj, resource_id ){...wpbc_prepare_tooltip_content( value, date_obj, resource_id );...}.....//Fixln: Deprecated..function is_this_time_selections_not_available( resource_id, form_elements ){... var reslt = wpbc_c_is_this_time_selection_not_available( resource_id, form_elements );... return reslt;...}.....//**..* Prepare for showing popovers in calendar at front-end side.. *..

<b>C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\KSU5XQMC\wpbc_vars[1].js</b>	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Size (bytes):	6612
Entropy (8bit):	4.673160032369297
Encrypted:	false
MD5:	2C144FF01B267292D71B40AF830B8AC8
SHA1:	1C320E69584251CC12192824AEB983CC664893A0
SHA-256:	22E08EB2BC89075BB737C14312EEEC182CD1C6F1B085DA696A9DA0F3F75C7FB3
SHA-512:	2DD4B842494D42D83CFE4BBB912CCE4302430508DA57783248834288D6A5809F9A13DE8A3E840DB21927FF5410986CF38630E2F8C019B896C12D2B078742D9C
Malicious:	false

<b>C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\KSU5XQMC\wpbc_vars[1].js</b>	
Reputation:	low
IE Cache URL:	<a href="http://https://campbaker.org/wp-content/plugins/booking/js/wpbc_vars.js?ver=8.7.6">http://https://campbaker.org/wp-content/plugins/booking/js/wpbc_vars.js?ver=8.7.6</a>
Preview:	<pre>/*.* @version 1.0.* @package Booking Calendar . * @subpackage JS Variables.* @category Scripts.*.* @author wpdevelop.* @link https://wpbookingcalendar.com/. *@email info@wpbookingcalendar.com.*.* @modified 2014.05.20.*!.....// Eval specific variable value (integer, bool, arrays, etc...)//.....function wpbc_define_var( wpbc_global_var ) {  if (wpbc_global_var === undefined) { return null; }. else { return jQuery.parseJSON(wpbc_global_var); }          //FixIn:6.1.}.....// Define global Booking Calendar Varibales based on Localization......var wpbc_ajaxurl          = wpbc_global1.wpbc_ajaxurl; .var wpdev_bk_pl ugin_url              = wpbc</pre>

<b>C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\VS02472\analytics[1].js</b>	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Size (bytes):	45892
Entropy (8bit):	5.519221828657939
Encrypted:	false
MD5:	0DD54814529C411F153BE5C5ED7D575F
SHA1:	6E49EE873C717AA81B90A0D44939B2505BFFD553
SHA-256:	2F1FD973E6C48489AE07C467E3278635B856C698D1F502E06AF3AB555937DEAC
SHA-512:	79424A1826F3B7EB58C4F972C406B357466F1A3C43ED76B49788C54D2459C910031A67E0813BC852CC0062051070DEEDCBFA68B9268EF41708FF2204ACB4210D
Malicious:	false
Reputation:	low
IE Cache URL:	<a href="http://https://www.google-analytics.com/analytics.js">http://https://www.google-analytics.com/analytics.js</a>
Preview:	<pre>(function(){/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var m=this  self,n=function(a,b){a=a.split(".");var c=m;a[0]in c  "undefin ed"===typeof c.execScript  c.execScript("var "+a[0]);for(var d;a.length&amp;&amp;(d=a.shift());)a.length  void 0===b?c=c[d]&amp;&amp;c[d]!==Object.prototype[d]?c[d]:c[d]={}:c[d]=b};var p= function(a,b){for(var c in b)b.hasOwnProperty(c)&amp;&amp;(a[c]=b[c]);q=function(a){for(var b in a)if(a.hasOwnProperty(b))return!0;return!1};var r=window,t=document,u=function(a ,b){t.addEventListener?t.addEventListener(a,b,!1):t.attachEvent&amp;&amp;t.attachEvent("on"+a,b)};var v=/^(?:(?:https? mailto ftp) [^\s:/?#]*(?:/?\# \$))/i;var w={},x=function(){fw .TAGGING=w.TAGGING  [];w.TAGGING[1]=!0};var y=/:/[0-9]+\$/;A=function(a,b){b&amp;&amp;(b=String(b).toLowerCase());if("protocol"===b  "port"===b)a.protocol=z(a.protocol)   z(r.location.protocol);"port"===b?a.port=String(Number(a.hostname?a.port:r.location.port))  ("http"===a.protocol?80:"https"===a.protocol?443:"");"host"===b&amp;&amp;(a ho</pre>

<b>C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\VS02472\animations[1].js</b>	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Size (bytes):	5556
Entropy (8bit):	5.026132381697075
Encrypted:	false
MD5:	FC9B54B8F12BD4C26E30F8CF3A796B62
SHA1:	83F1892440D5B6C9D17B0EAC935F5BB9512C313E
SHA-256:	E660E91FB1E4381D50141952B02A5BEC468153E2C288F2B2274A10D31D6A769B
SHA-512:	9439165BC5508E02A0F52AF3F68459F30A7CAC53EB8BFE04E32CC3FC645D0E22FCB9E64BBA0DBD3BEFD8C4F56EC416A2CCC3F8C041E01F17CB10CD595B877CED
Malicious:	false
Reputation:	low
IE Cache URL:	<a href="http://https://campbaker.org/wp-content/themes/diwine/scripts/vendor/plugins/animations.js">http://https://campbaker.org/wp-content/themes/diwine/scripts/vendor/plugins/animations.js</a>
Preview:	<pre>/*!.. * animations v4.0.1.. * A simple and easy jQuery plugin for CSS animated page transitions... * http://blivesta.github.io/animations.. * License : MIT.. * Author : blivesta (h ttp://blivesta.com/).. *!..function(t){"use strict";function"===typeof define&amp;&amp;define.amd?define(["jquery"],t):"object"===typeof exports?module.exports=t(require("jquery" )):(jQuery)}(function(t){"use strict";var n="animations",i={init:function(a){a=L.extend({inClass:"fade-in",outClass:"fade-out",inDuration:1500,outDuration:800,linkElemen t:".animations-link",loading:!0,loadingParentElement:"body",loadingClass:"animations-loading",loadingInner:"",timeout:!1,timeoutCountdown:5e3,onLoadEvent:!0,browser: ["animation-duration","-webkit-animation-duration"],overlay:!1,overlayClass:"animations-overlay-slide",overlayParentElement:"body",transition:function(t){window.loca tion.href=t}},a),i.settings={timer:!1,data:{inClass:"animations-in-class",inDuration:"animations-in-duration",outClass:"animations-out-class",outDurat</pre>

<b>C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\VS02472\calendar[1].css</b>	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Size (bytes):	20230
Entropy (8bit):	4.815170428876309
Encrypted:	false
MD5:	6B8C8EE11396A574AD27B9603D50AD51
SHA1:	14CD3855BDC08AB2F24C03C76940B26BA2FEEBC7
SHA-256:	6E7826D536FF5B49DB70E690AD884D8C57FF6F32636AF17F3C3722730CAAA4FF
SHA-512:	9399B71B49FE40E8E1CFF11DC7C356EB586B6C7316F498A48ED9CF791EE12480E133A4549E37A442635164E79279E181F3AA3D602E0FD2706D57439D8549DEE6
Malicious:	false
Reputation:	low
IE Cache URL:	<a href="http://https://campbaker.org/wp-content/plugins/booking/css/calendar.css?ver=8.7.6">http://https://campbaker.org/wp-content/plugins/booking/css/calendar.css?ver=8.7.6</a>





<b>C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\5D02472\camp-baker-logo[1].png</b>	
Preview:	.PNG.....IHDR...z...f.....M.....IEXtSoftware.Adobe ImageReadyq.e<...(iTxTML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?><x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c145 79.163499, 2018/08/13-16:40:22 "><rdf:RDF xmlns:rd="http://www.w3.org/1999/02/22-rdf-syntax-ns#"><rdf:Description rdf:about="" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmp:CreatorTool="Adobe Photoshop CC 2019 (Macintosh)" xmpMM:InstanceID="xmp.iid:27A4B40A365411E9A0B18D225E5D02AC" xmpMM:DocumentID="xmp.did:AF52B866365411E9A0B18D225E5D02AC"><xmpMM:DerivedFrom stRef:instanceID="xmp.iid:27A4B408365411E9A0B18D225E5D02AC" stRef:documentID="xmp.did:27A4B409365411E9A0B18D225E5D02AC"/></rdf:Description></rdf:RDF></x:xmpmeta><?xpacket end="r"?>.dx.....IDATx.....U.....6#+%T.....e.QF!aj..fkk[K?vM(.D*..X*.HIHK..53...].5....4)(*H0.(v..{v..X..To.....8..

<b>C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\5D02472\datepicker.min[1].js</b>	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Size (bytes):	36380
Entropy (8bit):	5.3199689653908955
Encrypted:	false
MD5:	70B4930DC8E018F851F8530C330B1456
SHA1:	45E5B2927E248E37A7FA762BFAA2BE33755E32A8
SHA-256:	79D249BAB4461FA4ADC1FAB32DE3371BF64689F83B9D77929279FC7E4AF7D929
SHA-512:	5480190B63DF50DF5AFEE4C52B817B6550B749F2ED21553C3585A73714C90BFF289E00581EFD302BFB1BCF5661AEFEF9937CEBB5D8DC227F89246D9681E55B35
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://campbaker.org/wp-includes/js/jquery/ui/datepicker.min.js?ver=1.11.4
Preview:	/*! * jQuery UI Datepicker 1.11.4. * http://jqueryui.com. * * Copyright jQuery Foundation and other contributors. * Released under the MIT license.. * http://jquery.org/license. * * http://api.jqueryui.com/datepicker/. */!(function(e){("function"==typeof define&&define.amd?define(["jquery","./core"],e):(jQuery))(function(b){var r;function e(){this._curInst=null,this._keyEvent=!1,this._disabledInputs=[],this._datepickerShowing=!1,this._inDialog=!1,this._mainDivId="ui-datepicker-div",this._inlineClass="ui-datepicker-inline",this._appendClass="ui-datepicker-append",this._triggerClass="ui-datepicker-trigger",this._dialogClass="ui-datepicker-dialog",this._disableClass="ui-datepicker-disabled",this._unselectableClass="ui-datepicker-unselectable",this._currentClass="ui-datepicker-current-day",this._dayOverClass="ui-datepicker-days-cell-over",this.regional=[];this.regional[""]={closeText:"Done",prevText:"Prev",nextText:"Next",currentText:"Today",monthNames:["January","February","March","Apr

<b>C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\5D02472\diwine[1].js</b>	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Size (bytes):	51474
Entropy (8bit):	5.265178557902925
Encrypted:	false
MD5:	A352D5DA3A33A871CF30DD5AE89B765D
SHA1:	A140200E48285625C7F9911E3DC629F4E498B78B
SHA-256:	2AD71E1C51CE8513DCAA2FB4720E5BF2E1BFFBD3DD186F34899728CA2C78D2F4
SHA-512:	6355A5EEA15B789EF066BBDFCF3453C3753156259D68ADB23CB6B0C90564B6CA47B01703D4C3A74859650FA9CFFED609894D5A9CC09E1929A08D7E164E168
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://campbaker.org/wp-content/themes/diwine/scripts/diwine.js
Preview:	/*jslint browser: true*/./*jslint white: true */./*global \$,jQuery,ozy_headerType,alert,ozy_Animition,TweenMax,Power1,ozy_facebookWidget,Flickity,wc_add_to_cart_params*/./* Diwine WordPress Theme Main JS File */./*** * Read cookie.* * @key - Cookie key.*/.function getCookieValue(key) {..use strict:. var currentcookie = document.cookie, firstidx, lastidx;. if (currentcookie.length > 0). { firstidx = currentcookie.indexOf(key + "=");. if (firstidx !== -1). { firstidx = firstidx + key.length + 1;. lastidx = currentcookie.indexOf(";", firstidx);. if (lastidx === -1). { lastidx = currentcookie.length;. return decodeURIComponent(currentcookie.substr(firstidx, lastidx));. }. return "";.}.* * Cookie Notice Banner.*/.function ozy_cookie_notice_banner() {..use strict:.if(getCookieValue( "diwine_cookie_banner" ) != '1' ) {..jQuery("#ozy-cookie_notice_

<b>C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\5D02472\dotimeout[1].js</b>	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Size (bytes):	1073
Entropy (8bit):	5.350123526657701
Encrypted:	false
MD5:	12B8FDC02376E2A702A31319383BCC4E
SHA1:	7E41FA76FD477D3642AA245415E4275C5294F724
SHA-256:	5346EC934D7DA53B367A2BACB1BE2D48FB8E022EE66544E9ED4CFC64B0A7D868
SHA-512:	4CF90B7F0A381F88151C83A18E01E8C0A087A61BA8D4D3C494DA1E5A632C36AFAFE5029E67622309698D6CDCD57335248ACB4BB4935D540E6075FE044D1FA4E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://campbaker.org/wp-content/themes/diwine/scripts/vendor/plugins/dotimeout.js
Preview:	/*.. * jQuery doTimeout: Like setTimeout, but better! - v1.0 - 3/3/2010.. * http://benalman.com/projects/jquery-dotimeout-plugin/.. * .. * Copyright (c) 2010 "Cowboy" Ben Alman.. * Dual licensed under the MIT and GPL licenses.. * http://benalman.com/about/license/.. */..(function(\$){var a={},c="doTimeout",d=Array.prototype.slice;\$.fn=function(){return b.apply(window,[0].concat(d.call(arguments))));\$.fn[c]=function(){var f=d.call(arguments),e=b.apply(this,[c+f[0]].concat(f));return typeof f[0]=== "number"   typeof f[1]=== "number"?this:e;function b(l){var m=this,h,k={},g=?\$.fn.\$,n=arguments,i=4,f=n[1],j=n[2],p=n[3];if(typeof f!=="string"){f--;f-=0;j=n[1];p=n[2]}if(l){h=m.eq(0);h.data(l,k=h.data(l)  {});}else{if(f){k=a[f]}(a[f]={});k.id&&clearTimeout(k.id);delete k.id;function e(){if(l){h.removeData(l)}else{if(f){delete a[f]}}function o(){k.id=setTimeout(function(){k.fn(l),j})if(p){k.fn=function(o){if(typeof p=== "string"){p=[p,p].p.apply(m,d.call(n,i))===true&&l?q:o();o()}}else{if(k

<b>C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\5D02472\fb-circle[1].png</b>	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 60 x 60, 8-bit/color RGBA, non-interlaced
Size (bytes):	3750
Entropy (8bit):	7.797562359884141
Encrypted:	false
MD5:	8965C14D4E7DD64CB5E5778C27DA9A60
SHA1:	3E1395C188775FC674334B65AD42F278E663FA09
SHA-256:	4DD96C388C8B5710AB43E897B2163546E38E1C8F84CEA55E8A3546398574BEFE
SHA-512:	3735556EDB9C5DA9C60120A4E157514F497C8AD910AF5FA68A63AC66273C47632ECFE56D204D2C18E3B73A9067FCAF16216DDCAD6A76B15E286D0CBADFDB74
Malicious:	false
Reputation:	low
IE Cache URL:	<a href="http://https://campbaker.org/wp-content/uploads/2019/05/fb-circle.png">http://https://campbaker.org/wp-content/uploads/2019/05/fb-circle.png</a>
Preview:	.PNG.....IHDR...<...<.....f....tEXtSoftware.Adobe ImageReadyq.e<...(iTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d">><x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c145 79.163499, 2018/08/13-16:40:22 "> <rdf:RDF xmlns:rd="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmp:CreatorTool="Adobe Photoshop CC 2019 (Macintosh)" xmpMM:InstanceID="xmp.iid:94921AE463F711E99631EF961CF82C5B" xmpMM:DocumentID="xmp.did:94921AE563F711E99631EF961CF82C5B"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:94921AE263F711E99631EF961CF82C5B" stRef:documentID="xmp.did:94921AE363F711E99631EF961CF82C5B"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?'>..`... ..IDATx..[{.g.?{w.....Bj.5@4...A.i..j)..M.ii..h...1*!5...6.iM.?.....G4e..Y.....w.y.....

<b>C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\5D02472\lickity[1].js</b>	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Size (bytes):	55158
Entropy (8bit):	5.085793003934809
Encrypted:	false
MD5:	6FD670F1D74F2A08CCE5E44B080F5F74
SHA1:	525D5CEEA36382AD53503CA0AB66B86515FBCF36
SHA-256:	3BBD6F6EAB66960E4472DA168EB005338DAC3E40C4F8653B3167F62228F03B9B4
SHA-512:	3657FF01D70D849E06A85CE6F5AE74543B5ACD3DF5805D06693D809E4718D75E3E5B74A5E8F8C736790F666158DA36D5A3CE951A1C7ABA9C6C935DA41EC386;
Malicious:	false
Reputation:	low
IE Cache URL:	<a href="http://https://campbaker.org/wp-content/themes/diwine/scripts/vendor/plugins/lickity.js">http://https://campbaker.org/wp-content/themes/diwine/scripts/vendor/plugins/lickity.js</a>
Preview:	/*!.. * Flickity PACKAGED v2.0.2.. * Touch, responsive, flickable carousels.. *.. * Licensed GPLv3 for open source use.. * or Flickity Commercial License for commercial use.. *.. * http://flickity.metafizzy.co.. * Copyright 2016 Metafizzy.. */.....!function(t,e){("use strict";"function"==typeof define&&define.amd?define(["jquery-bridget/jquery-bridget",["jquery"],function(i){e(t,i)}):"object"==typeof module&&module.exports?module.exports=e(t,require("jquery")):t.jQueryBridget=e(t,t.jQuery)})(window,function(t,e){("use strict";function i(i,o,a){function h(t,e,n){var s,o="\$. "+"i+"+"e+";return t.each(function(t,h){var l=a.data(h,i);if(!l)return void r(i+" not initialized. Cannot call methods, i.e. "+o);var c=[e];if(!c["_"==e.charAt(0)]return void r(o+" is not a valid method");var d=c.apply(l,n);s=void 0===s?s:d;s},void 0===s?s:t);function l(t,e){t.each(function(t,n){var s=a.data(n,i);s?s.option(e),s._init():(s=new o(n,e),a.data(n,i,s))));a=al[t.jQuery,a&&(o.prototype.option)](o,prot

<b>C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\5D02472\frontend-functions[1].js</b>	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Size (bytes):	6902
Entropy (8bit):	5.075539092846965
Encrypted:	false
MD5:	C6F0913F37BE673CA48A4EC149E36B40
SHA1:	2D9E192644F7D2A8603325C534F51A5A207B9E39
SHA-256:	1F9FCD04FCF83EA8145CFE20D0459D0AA39787FC0D2F561CE2EB5469674277FA
SHA-512:	F84C899E724E68C51C1329AC5803D98BF8A520900CCF5F645F8563302544F98F2851B461323BF46E2D02D54B620756070CB8F0199E1976F1137C9EA5AA603258
Malicious:	false
Reputation:	low
IE Cache URL:	<a href="http://https://campbaker.org/wp-content/plugins/booked-woocommerce-payments/ljs/frontend-functions.js?ver=5.4.1">http://https://campbaker.org/wp-content/plugins/booked-woocommerce-payments/ljs/frontend-functions.js?ver=5.4.1</a>
Preview:	;(function(\$, window, document, undefined) {...var \$win = \$(window);...var \$doc = \$(document);...var \$field_container;.....\$doc.ready(function() {.....\$(document).on("booked-on-new-app", function(event) {.....\$field_container = \$('field.field-paid-service');.....booked_wc_products_field(\$field_container);.....});.....booked_wc_btn_edit_appointment_shortcode();.....booked_wc_btn_edit_appointment_popup_app();.....booked_wc_btn_pay_appointment_shortcode();.....\$(document).on("booked-before-loading-calendar-booking-options", function(event) {.....booked_wc_change_calendar_loading_parameters();.....});.....\$(document).on("booked-before-loading-booking-form", function(event) {.....booked_wc_change_booking_form_parameters();.....});.....\$(document).on("booked-on-requested-appointment", function(event,redirectObj) {.....redirectObj.redirect = booked_wc_redirect_to_checkout_if_product_option();.....});.....});.....function booked_wc_products_field(field_container) {.....var \$dropdown = \$('se

<b>C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\5D02472\frontend[1].css</b>	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Size (bytes):	14097
Entropy (8bit):	4.601058168542163



<b>C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\VS5D02472\frontend[1].css</b>	
Encrypted:	false
MD5:	59B286EE3319D3FCB97A0ED77FC8AB5E
SHA1:	E32B55A8D6A0643A23171CEF88D3132FCBB61074
SHA-256:	4FD2779C279C766EE47B5FF74B2C4298620A729290A15FC2B20E99340B416CA4
SHA-512:	42426E1B615C9A2883CBB0D5163F9B26EA403EFE43A6915DC1673BBB5A34943BF622FB7D88D1293C55CE7800AC9804C1A59A70E4959CDFD3BAE8995E4F0F1432
Malicious:	false
Reputation:	low
IE Cache URL:	<a href="http://https://campbaker.org/wp-content/plugins/wp-job-manager-applications/assets/css/frontend.css?ver=5.4.1">http://https://campbaker.org/wp-content/plugins/wp-job-manager-applications/assets/css/frontend.css?ver=5.4.1</a>
Preview:	<div>ul.job_listings .job-manager-applications-applied-notice{color:#2ecc71;font-weight:400;float:right}ul.job_listings .job-manager-applications-applied-notice::before{content:"\e802";display:inline-block;width:16px;height:16px;-webkit-font-smoothing:antialiased;font-family:job-manager!important;text-decoration:none;font-weight:400;font-style:normal;vertical-align:top;font-size:16px;margin:0 2px 0 0}.single_job_listing .job-manager-applications-applied-notice{margin:0;display:block;padding:1em;text-decoration:none;margin:2em 0;overflow:hidden;border:1px solid #eee;border-bottom-width:2px}.single_job_listing .job-manager-applications-applied-notice::before{content:"\e802";display:inline-block;width:16px;height:16px;-webkit-font-smoothing:antialiased;font-family:job-manager!important;text-decoration:none;font-weight:400;font-style:normal;vertical-align:top;font-size:16px;margin:0 2px 0 0}.single_job_listing .application .application_details form.job-manager-application-form{padding:.25em 0 0</div>

<b>C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\VS5D02472\hale-partner-logo[1].png</b>	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 195 x 61, 8-bit/color RGBA, non-interlaced
Size (bytes):	16312
Entropy (8bit):	7.971585822800822
Encrypted:	false
MD5:	E54D51623EB31BD8893FF8E412638C45
SHA1:	7199441CFD9ECEE1FB39F98F33A4B593C807F0C7
SHA-256:	8BCB38DCCC93C732B7D40D2CA9431EC891CE47EA089324359F16AA3425D424BF
SHA-512:	698C3579000E702834A89465C8AC235C30B8529558D94AC5D517C234FD4958A18CEBDDF75949DED84F4EA191F79FC57FEC40673B8B14E1B205D892D20971307
Malicious:	false
Reputation:	low
IE Cache URL:	<a href="http://https://campbaker.org/wp-content/uploads/2019/04/hale-partner-logo.png">http://https://campbaker.org/wp-content/uploads/2019/04/hale-partner-logo.png</a>
Preview:	<div>.PNG.....IHDR.....=.....tEXtSoftware.Adobe ImageReadyq.e&lt;...(T)XTXML:com.adobe.xmp.....&lt;?xpacket begin="," id="W5M0MpCehiHzreSzNTczkc9d"?&gt; &lt;x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmpptk="Adobe XMP Core 5.6-c145 79.163499, 2018/08/13-16:40:22 "&gt; &lt;rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"&gt; &lt;rdf:Description rdf:about="" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xa p/1.0/sType/ResourceRef#" xmp:CreatorTool="Adobe Photoshop CC 2019 (Macintosh)" xmpMM:InstanceID="xmp.iid:164779BE505611E997CADB7831DC6039" xmpMM:DocumentID="xmp.did:164779BF505611E997CADB7831DC6039"&gt; &lt;xmpMM:DerivedFrom stRef:instanceID="xmp.iid:164779BC505611E997CADB78 31DC6039" stRef:documentID="xmp.did:164779BD505611E997CADB7831DC6039"/&gt; &lt;/rdf:Description&gt; &lt;/rdf:RDF&gt; &lt;/x:xmpmeta&gt; &lt;?xpacket end="?"?&gt;/.....&lt;&amp;IDATx...  \$Wu k..U.jl...53.....@0/.....[&gt;...B.H.G...y.....G...../.....gF..h4.jj..V.^..S.il..</div>

<b>C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\VS5D02472\jbcc-logo-white[1].png</b>	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 200 x 54, 8-bit/color RGBA, non-interlaced
Size (bytes):	6263
Entropy (8bit):	7.909077581001706
Encrypted:	false
MD5:	893A93D700F23FFCE3410CB6CB4BBBFB
SHA1:	D6EF8365F9C38C4FDB42D3E10E4207A4711B1E4A
SHA-256:	CB34700D70DBCE98A417F5BBA5E3BC08F57DBD071B989E7EED742605BA2C0C5
SHA-512:	6F53B276AF75F7788C6C3A7C7BE27E9FB3A48996D9B0CD3D4B63DF25859E26441C728377FE868F76924E78DEDCBCA42C6E90210EA2131CA16C87A264BFE580C E
Malicious:	false
Reputation:	low
IE Cache URL:	<a href="http://https://campbaker.org/wp-content/uploads/2019/05/jbcc-logo-white.png">http://https://campbaker.org/wp-content/uploads/2019/05/jbcc-logo-white.png</a>
Preview:	<div>.PNG.....IHDR.....6.....tEXtSoftware.Adobe ImageReadyq.e&lt;...(T)XTXML:com.adobe.xmp.....&lt;?xpacket begin="," id="W5M0MpCehiHzreSzNTczkc9d"?&gt; &lt;x:xmpme ta xmlns:x="adobe:ns:meta/" x:xmpptk="Adobe XMP Core 5.6-c145 79.163499, 2018/08/13-16:40:22 "&gt; &lt;rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax- ns#"&gt; &lt;rdf:Description rdf:about="" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xa p/1.0/sType/ResourceRef#" xmp:CreatorTool="Adobe Photoshop CC 2019 (Macintosh)" xmpMM:InstanceID="xmp.iid:E2E533EF6B4811E9A73FDDF5B248C20A" xmpMM:DocumentID="xmp.did:E2E533F06B4811E9A73FDDF5B248C20A"&gt; &lt;xmpMM:DerivedFrom stRef:instanceID="xmp.iid:E2E533ED6B4811E9A73FDDF5 B248C20A" stRef:documentID="xmp.did:E2E533EE6B4811E9A73FDDF5B248C20A"/&gt; &lt;/rdf:Description&gt; &lt;/rdf:RDF&gt; &lt;/x:xmpmeta&gt; &lt;?xpacket end="?"?&gt;/I.....IDATx..  ...?.!;!@ ..&amp;.QA.s.....b.h...b....Y.U)H..\"b..ZE.*...\"X.....".....=.....2.7Y.m..w2o..</div>

<b>C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\VS5D02472\jquery-animate-colors[1].js</b>	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Size (bytes):	2766
Entropy (8bit):	5.449071738686266
Encrypted:	false
MD5:	5A8ACF60D6D7F01874282583B29E6F45
SHA1:	697F9773A1EE2A185971BCCF5051AC5CEE1A366E
SHA-256:	33DD44549B25B4BF285918BE83377A1216D06B8FB318FBA1E2294FB27AFFA09

<b>C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\5D02472\jquery-animate-colors[1].js</b>	
SHA-512:	CEA83792D5200D60D9986B52EE13DA40376552D4DD1FAEC3CC884B8F16116C5FB6236964C36A3BDE4088D43EBB3F6A9DB3C1852491406E1022E40B0E4CF9FC6
Malicious:	false
Reputation:	low
IE Cache URL:	<a href="http://https://campbaker.org/wp-content/themes/diwine/scripts/vendor/plugins/jquery-animate-colors.js">http://https://campbaker.org/wp-content/themes/diwine/scripts/vendor/plugins/jquery-animate-colors.js</a>
Preview:	<pre>/*.. Color animation 1.6.0.. http://www.bitstorm.org/jquery/color-animation/. Copyright 2011, 2013 Edwin Martin &lt;edwin@bitstorm.org&gt;.. Released under the MIT and GPL licenses...*/.. 'use strict';(function(d){function h(a,b,e){var c="rgb"+(d.support.rgba?"a":""),"("+parseInt(a[0]+e*(b[0]-a[0]),10)+"," +parseInt(a[1]+e*(b[1]-a[1]),10)+"," +parseInt(a[2]+e*(b[2]-a[2]),10);d.support.rgba&amp;&amp;(c+="-",)+(a&amp;&amp;b?parseFloat(a[3]+e*(b[3]-a[3])):1));return c+"")function f(a){var b;return(b=#[([0-9a-fA-F]{2})]([0-9a-fA-F]{2})).exec(a))?[parseInt(b[1],16),parseInt(b[2],16),parseInt(b[3],16),1];(b=#[([0-9a-fA-F])([0-9a-fA-F])([0-9a-fA-F]).exec(a))?[17*parseInt(b[1],16),17*parseInt(b[2],16),17*parseInt(b[3],16),1];(b=/rgb\(\s*([0-9]{1,3})\s*,\s*([0-9]{1,3})\s*,\s*([0-9]{1,3})\s*\)/.exec(a))?[parseInt(b[1]),parseInt(b[2]),parseInt(b[3]),1];(b=/rgba\(\s*([0-9]{1,3})\s*,\s*([0-9]{1,3})\s*,\s*([0-9]{1,3})\s*,\s*([0-9]{1,3})\s*\)/.exec(a))?[parseInt(b[1]),parseInt(b[2]),parseInt(b[3]),1],pa</pre>

<b>C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\5D02472\jquery-easing[1].js</b>	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Size (bytes):	3716
Entropy (8bit):	5.196641046402138
Encrypted:	false
MD5:	886E09ADA20248EE5EF49E2918BB98C9
SHA1:	99EE6B67267ECA61CCEF24BC9B66F6DA5AB7865F
SHA-256:	8B5DE1D3948C144DE586A67F79FDA70710EC4EC939021A3B841EF108F3635AE0
SHA-512:	06252966FADABFBAFF854B462C56D11304AFBADD6898930D14B582B6E763B164BD2E573C0B6C6486C03A3A439C4F19FCFB7630C570601D4E453971A63EC1895
Malicious:	false
Reputation:	low
IE Cache URL:	<a href="http://https://campbaker.org/wp-content/themes/diwine/scripts/vendor/plugins/jquery-easing.js">http://https://campbaker.org/wp-content/themes/diwine/scripts/vendor/plugins/jquery-easing.js</a>
Preview:	<pre>/*Please see licensing and creator information at http://gsqd.co.uk/sandbox/jquery/easing/jquery.easing.1.3.js*/...jQuery.easing.jswing=jQuery.easing.swing;jQuery.extend(jQuery.easing,{def:"easeOutQuad",swing:function(e,f,a,h,g){return jQuery.easing[jQuery.easing.def](e,f,a,h,g)};easeInQuad:function(e,f,a,h,g){return h*(f/=g)*f+a};easeOutQuad:function(e,f,a,h,g){return -h*(f/=g)*(f-2)+a};easeInOutQuad:function(e,f,a,h,g){if((f/=g/2)&lt;1){return h/2*f*f+a};return -h/2*((-f)*(f-2)-1)+a};easeInCubic:function(e,f,a,h,g){return h*(f/=g)*f*f+a};easeOutCubic:function(e,f,a,h,g){return h*(f/=g-1)*f*f+1)+a};easeInOutCubic:function(e,f,a,h,g){if((f/=g/2)&lt;1){return h/2*f*f*f+a};return h/2*((f-2)*f*f+2)+a};easeInQuart:function(e,f,a,h,g){return h*(f/=g)*f*f*f+a};easeOutQuart:function(e,f,a,h,g){return -h*((f/=g-1)*f*f*f-1)+a};easeInOutQuart:function(e,f,a,h,g){if((f/=g/2)&lt;1){return h/2*f*f*f*f+a};return -h/2*((f-2)*f*f*f-2)+a};easeInQuint:function(e,f,a,h,g){return h*(f/=g)*f*f*f*f+a};easeOutQuin</pre>

<b>C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\5D02472\jquery-hoverintent[1].js</b>	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Size (bytes):	2252
Entropy (8bit):	5.1799684099993435
Encrypted:	false
MD5:	1B5DB710562F468E771BE6E1B6364F57
SHA1:	66A2AC25FC568C641C972A6B82E0910D94231BCA
SHA-256:	3DD9C76C449B6A9245F70B59C42CD0155A6D38B95A627EB297CD3EDAF53C3D87
SHA-512:	65B46566AF676D1E6C6CE86B0B270A23EEA75744D8092D408E6654EED458479FD180C9FDE28C4FD39BEB08EC15F46CDBA9CAA2AFD02EA1DB4C8D5DDDD067DA24
Malicious:	false
Reputation:	low
IE Cache URL:	<a href="http://https://campbaker.org/wp-content/themes/diwine/scripts/vendor/plugins/jquery-hoverintent.js">http://https://campbaker.org/wp-content/themes/diwine/scripts/vendor/plugins/jquery-hoverintent.js</a>
Preview:	<pre>/*!.. * hoverIntent v1.9.0 // 2017.09.01 // jQuery v1.7.0+... * http://briancherne.github.io/jquery-hoverIntent/.. *.. * You may use hoverIntent under the terms of the MIT license. Basically that.. * means you are free to use hoverIntent as long as this header is left intact... * Copyright 2007-2017 Brian Cherne.. */..!..function(factory){"use strict";;function"==typeof define&amp;&amp;define.amd?define(["jQuery"],factory):jQuery&amp;&amp;jQuery.fn.hoverIntent&amp;&amp;factory(jQuery)}(function(\$){"use strict";var cX,cY,_cfg={interval:100,sensitivity:6,timeout:0},INSTANCE_COUNT=0,track=function(ev){cX=ev.pageX,cY=ev.pageY},compare=function(ev,\$el,s,cfg){if(Math.sqrt((s.pX-cX)*(s.pX-cX)+(s.pY-cY)*(s.pY-cY))&lt;cfg.sensitivity)return \$el.off(s.event,track),delete s.timeoutId,s.isActive=!0,ev.pageX=cX,ev.pageY=cY,delete s.pX,delete s.pY,cfg.over.apply(\$el[0],[ev]);s.pX=cX,s.pY=cY,s.timeoutId=setTimeout(function(){compare(ev,\$el,s,cfg)},cfg.interval)},delay=function(ev,\$el,s,out){return delete \$el.data("hoverIntent")}</pre>

<b>C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\5D02472\jquery-scrolllock[1].js</b>	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Size (bytes):	4643
Entropy (8bit):	5.294741191706291
Encrypted:	false
MD5:	AF821DCB853B904204478CF8ED043E45
SHA1:	8A785EEF9D3F48E81CEE5E5029A399482C2A4368
SHA-256:	B405C2CE7E00F28B1F922631565CF07D9C48B9C9F67EE81A6473472880F9FA07
SHA-512:	E2133B99AF473648FD778B1E2201DACF9F2F7098F41D7925D0C95F85DD42195C0FDA19C8C1693606550578CA355986A47F488D3D22C1B481D1675489BC9C7A8E
Malicious:	false
Reputation:	low
IE Cache URL:	<a href="http://https://campbaker.org/wp-content/themes/diwine/scripts/vendor/plugins/jquery-scrolllock.js">http://https://campbaker.org/wp-content/themes/diwine/scripts/vendor/plugins/jquery-scrolllock.js</a>

<b>C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\5D02472\jquery-scrolllock[1].js</b>	
Preview:	<pre>/*!.. * Scroll Lock v3.1.3.. * https://github.com/MohammadYounes/jquery-scrollLock.. *.. * Copyright (c) 2017 Mohammad Younes.. * Licensed under GPL 3.. */..(function(n){typeof define=="function"&amp;&amp;define.amd?define(["jquery"],n):(function(n){"use strict";var i={space:32,pageup:33,pagedown:34,end:35,home:36,up:38,down:40},r=function(t,i){var u=i.scrollTop(),h=i.prop("scrollHeight"),c=i.prop("clientHeight"),f=t.originalEvent.wheelDelta -1*t.originalEvent.detail -1*t.originalEvent.deltaY,r=0,e,o,s;return t.type=="wheel"? (e=i.height()/n(window).height(),r=t.originalEvent.deltaY*e);this.options.touch&amp;&amp;t.type=="touchmove"&amp;&amp;(f=t.originalEvent.changedTouches[0].clientY-this.startClientY),s=(o=f&gt;0&amp;u+r&lt;=0)  f&lt;0&amp;u+r&gt;=h-c,[prevent.s,top:o,scrollTop:u,deltaY:r]},u=function(n,t){var u=t.scrollTop(),r={top:11,bottom:11},f,e;return r.top=u===0&amp;&amp;(n.keyCode===i.pageup  n.keyCode===i.home  n.keyCode===i.up),r.top  (f=t.prop("scrollHeight"),e=t.prop("clientHeight"),r.bottom=f==u+e&amp;&amp;(n.k</pre>

<b>C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\5D02472\jquery.blockUI.min[1].js</b>	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Size (bytes):	9566
Entropy (8bit):	5.419210789126146
Encrypted:	false
MD5:	81B2BE18696C4DFE620F7B6D0D75A566
SHA1:	0C3CD7BDF58A65B07E17BE39CFE4E386571BB4BD
SHA-256:	120AAF6681CA6D34A40C559779F0A0038582A79FCE1B868FF901C94D27C89C72
SHA-512:	D6234549918A770A055717C9FD1FF4B162AFC7CDB9E72459883BBDB5E0453D7AF5295B2F58A6F8A70250EFEE55AB544FBA9595C85001C204516D907937D8C9C
Malicious:	false
Reputation:	low
IE Cache URL:	<a href="http://https://campbaker.org/wp-content/plugins/woocommerce/assets/js/jquery-blockui/jquery.blockUI.min.js?ver=2.70">http://https://campbaker.org/wp-content/plugins/woocommerce/assets/js/jquery-blockui/jquery.blockUI.min.js?ver=2.70</a>
Preview:	<pre>/*!. * jQuery blockUI plugin. * Version 2.70.0-2014.11.23. * Requires jQuery v1.7 or later. *.. * Examples at: http://malsup.com/jquery/block/. * Copyright (c) 2007-2013 M. Aisup. * Dual licensed under the MIT and GPL licenses:. * http://www.opensource.org/licenses/mit-license.php. * http://www.gnu.org/licenses/gpl.html. *.. * Thanks to Amir-Hossein Sobhi for some excellent contributions!. */.function(){"use strict";function e(e){function t(t,n){var s,h,k,t==window,y=n&amp;&amp;n.message!:=undefined?n.message:undefined;if(!(n=e.extend({},e.blockUI.defaults,n)  {})).ignoreIfBlocked  e(t).data("blockUI.isBlocked")}{if(n.overlayCSS=e.extend({},e.blockUI.defaults.overlayCSS,n.overlayCSS  {}),s=e.extend({},e.blockUI.defaults.css,n.css  {}),n.onOverlayClick&amp;&amp;(n.overlayCSS.cursor="pointer"),h=e.extend({},e.blockUI.defaults.themedCSS,n.themedCSS  {}),y=y==undefined?n.message:y,k&amp;&amp;o(window,fadeOut:0)),y&amp;&amp;"string"! =typeof y&amp;&amp;(y.parentNode  y.jquery)){var m=y.jquery?y[0]:y,g={};e(t).data("blockUI.his</pre>

<b>C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\5D02472\jquery.fancybox-media[1].js</b>	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Size (bytes):	5364
Entropy (8bit):	5.180368628214494
Encrypted:	false
MD5:	6C2B5357916A3DB9F8715BFC5EED9DEE
SHA1:	6E6FA956BFA19D9360A8B7CAF13753348916A684
SHA-256:	9A75E2157163FEB56638011FDDC0F9B09E569D8289D725F8724B89D7D5E59D3C
SHA-512:	D3B57DEA669E4ED19AAF16893DE6CDC0324FA69FD240A59F568D6F35CBED7A20787CA63D17C6EE1771EF8C04EB30F2236BC1673FF4719A1766615B606287A3F1
Malicious:	false
Reputation:	low
IE Cache URL:	<a href="http://https://campbaker.org/wp-content/themes/diwine/scripts/vendor/fancybox/helpers/jquery.fancybox-media.js">http://https://campbaker.org/wp-content/themes/diwine/scripts/vendor/fancybox/helpers/jquery.fancybox-media.js</a>
Preview:	<pre>/*!.. * Media helper for fancyBox.. * version: 1.0.5 (Tue, 23 Oct 2012).. * @requires fancyBox v2.0 or later.. *.. * Usage:.. * \$(".fancybox").fancybox({.. *   helpers : {.. *     media: true.. *   }.. * });.. *.. * Set custom URL parameters:.. * \$(".fancybox").fancybox({.. *   helpers : {.. *     media: {.. *       youtube : {.. *         params : {.. *           autoplay: 0.. *         }.. *       }.. *     }.. *   }.. * Or:.. * \$(".fancybox").fancybox({.. *   helpers : {.. *     media: true.. *   }.. *   youtube : {.. *     autoplay: 0.. *   }.. * });.. *.. * Supports:.. *.. * Youtube.. * http://www.youtube.com/watch?v=opj24KnzrWo.. * http://www.youtube.com/embed/opj24KnzrWo.. * http://youtu.be/opj24KnzrWo.. * Vimeo.. * http://vimeo.com/40648169.. *</pre>

<b>C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\5D02472\jquery.validate.min[1].js</b>	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Size (bytes):	22691
Entropy (8bit):	5.224443956984208
Encrypted:	false
MD5:	24AE1CA673CBEBD97E2FEEE165DCEB09
SHA1:	10FFC4F821B573AB70139AF0BC62A2F1E378EB02
SHA-256:	F30C8CB3AB2E2723A9499EA38D8FAC4E111163D2A7EFA7E3F7110B7E5AB6C8CD
SHA-512:	194266E5BFC2D2C6A2F6F013B2ED382FEFB33ED64474695E1B79418771916A0B5F8165226EBA466153C4BC2DC0689F08599FDDDD0652386430D8A0F1E057D9103F
Malicious:	false
Reputation:	low
IE Cache URL:	<a href="http://https://campbaker.org/wp-content/plugins/rsvp/jquery.validate.min.js?ver=5.4.1">http://https://campbaker.org/wp-content/plugins/rsvp/jquery.validate.min.js?ver=5.4.1</a>
Preview:	<pre>/*! jQuery Validation Plugin - v1.15.0 - 2/24/2016.. * http://jqueryvalidation.org/. * Copyright (c) 2016 J.rn Zaefferer; Licensed MIT */.function(a){"function"!==typeof define&amp;&amp;define.amd?define(["jquery"],a):"object"!==typeof module&amp;&amp;module.exports?module.exports=a(require("jquery")):a(jQuery)}(function(a){a.extend(a.fn,{validate:function(b){if(!this.length)return void(b&amp;&amp;b.debug&amp;&amp;window.console&amp;&amp;console.warn("Nothing selected, can't validate, returning nothing."));var c=a.data(this[0],"validator");return c?(c.this.attr("novalidate","novalidate"),c=new a.validator(b,this[0]),a.data(this[0],"validator",c),c.settings.onsubmit&amp;&amp;(this.on("click.validate",".submit",function(b){c.settings.submitHandler&amp;&amp;c.submitButton=b.target},a(this).hasClass("cancel")&amp;&amp;(c.cancelSubmit=!0),void 0!==a(this).attr("formnovalidate")&amp;&amp;(c.cancelSubmit=!0))),this.on("submit.validate",function(b){function d(){var d,e;return c.settings.submitHandler?(c.submitButton&amp;&amp;(d=a("&lt;input type='hidden'&gt;").attr("name",c</pre>

<b>C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\5D02472\logo-hms_0[1].png</b>	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 191 x 66, 8-bit/color RGBA, non-interlaced
Size (bytes):	18076
Entropy (8bit):	7.974541210381111
Encrypted:	false
MD5:	8BB6F51DA9B657E044DAFAD3F5A1C14D
SHA1:	530F3BB6B2AF9A336C630EF142AF77BCE33B9C51
SHA-256:	48E7EE984044666113FF4644FB409A03B09D1597933ADA7A5677AAC1E37A34B0
SHA-512:	57E143BC000CF0274E5DC12129EA15E82FB89E83886F3D5D209F72899ADB56CC09E9BF60D120D1D0D26C61872B56D1B4754FFE3E4974EDD6ABC61B0239EAB23
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://campbaker.org/wp-content/uploads/2019/05/logo-hms_0.png
Preview:	.PNG.....IHDR.....B.....tEXtSoftware.Adobe ImageReadyq.e<...xiTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpme ta xmlns:x="adobe:ns:meta/" x:xmp:tk="Adobe XMP Core 5.6-c111 79.158325, 2015/09/10-01:10:20 " > <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#" > <rdf:Description rdf:about="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpMM:OriginalDocumentID="xmp.did:f018577d-a932-49dc-9b7f-7999a0228bbb" xmpMM:DocumentID="xmp.did:145E1C6405A411E6 9D5792860B7D85C8" xmpMM:InstanceID="xmp.iid:145E1C6305A411E69D5792860B7D85C8" xmp:CreatorTool="Adobe Photoshop CC 2015 (Macintosh)" > <xmpMM: DerivedFrom stRef:instanceID="xmp.iid:58323bf6-aefa-4155-99fc-a190dd3cc260" stRef:documentID="xmp.did:f018577d-a932-49dc-9b7f-7999a0228bbb"/> </rdf:De scription> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>.2f...B.IDATx...}.U.....[.3C.z.z.E

<b>C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\5D02472\revicons[1].eot</b>	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), revicons family
Size (bytes):	12136
Entropy (8bit):	6.261379703810077
Encrypted:	false
MD5:	2FEB69CCB596730C72920C6BA3E37EF8
SHA1:	F3A83BC4ABD0D4F968FC45EC14DA4636A8159B38
SHA-256:	9E4D4C6813568FDF70C61ECA9446D1BB80F84E79E8F2E5ED177365B6D5DE5FBF
SHA-512:	F88E5F714D87FC7C45FC4CC8DFA7C2B5452662ECF4FEA27C45DD5315D3D0F4850985C470486EC34FB97031411F76E80BF2A13791DEDD67DA9EBC053C1EFB3F3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://campbaker.org/wp-content/plugins/revslider/public/assets/fonts/revicons/revicons.eot?5510888
Preview:	h/.....LP.....r.e.v.i.c.o.n.s.....R.e.g.u.l.a.r.....V.e.r.s.i.o.n..1...0.....r.e.v.i.c.o.n.s.....`OS/2>(H.....Vcmap...&...D....cvt .... ..\$......fpgm..x;..\$.gasp.....\$.glyf.!T.....jhead.j=....4...6hhea.....l...\$hmtx c.....loca.....@...Zmaxp.[. ..... name.+!.....post.O...".!...!prep.....h...V.....z.....1 .....PfEd.@... .R.j.Z.R..... ......`..... /.4.6;.....".1.6;.....B.....&.B@?%\$#! .....B...@.....j.....j..... .M.....T...H.....&....."+.#"....&7%6..2.....#!"&5.463.5'..

<b>C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\5D02472\spin.jquery[1].js</b>	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Size (bytes):	1756
Entropy (8bit):	4.833083028501634
Encrypted:	false
MD5:	9504049571835239DF2BA0AC2EAD52DB
SHA1:	E32B58DD14CB450C079ECDC3889F232FAE8517F8
SHA-256:	624ADE0D67ADA39D136E9A4D195D6EC384C218E6A30B092E61603866B861FD03
SHA-512:	751F1AD499B138663880CB92967802C2A9C4F4B2D64D1E8A5CD32328E1FED085AC54ADC04C088FE0B436C361E2C9590152BB9D5B341AE8F9C6A4D2171C1DC08
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://campbaker.org/wp-content/plugins/booked/assets/js/spin.jquery.js?ver=2.0.1
Preview:	/**. * Copyright (c) 2011-2014 Felix Gnass. * Licensed under the MIT license. */../*..Basic Usage:=====.\$('#el').spin(); // Creates a default Spinner using the text color of #el.\$('#el').spin({ ... }); // Creates a Spinner using the provided options...\$\$('#el').spin(false); // Stops and removes the spinner...Using Presets:=====..\$\$('#el').spin('small'); // Creates a 'small' Spinner using the text color of #el.\$\$('#el').spin('large', '#fff'); // Creates a 'large' white Spinner...Adding a custom preset:=====..\$.fn.spin.presets.flower = { lines: 9. length: 10. width: 20. radius: 0;}.\$\$('#el').spin('flower', 'red');..*/..(function(factory) {.. if (typeof exports == 'object') { // CommonJS. factory(require('jquery'), require('spin')). } else if (typeof define == 'function' && define.amd) { // AMD, register as anonymous module. define(['jquery', 'spin'], factory). } else { // Browser globals. if (!window.Spinner) throw new

<b>C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\5D02472\style[1].css</b>	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Size (bytes):	10982
Entropy (8bit):	4.743003127705788

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\5D02472\style[1].css	
Encrypted:	false
MD5:	CE6D601F800F8C2B37C5813D9E8B4993
SHA1:	F8025C4F11979C041C2D46409F1982B436EFEC29
SHA-256:	F553FFA0DC22F18522C51141D8DFFC39ACBF7CE70BF46D735B999EC7874D6EF8
SHA-512:	5743B32DE42AD63D9E56900A43CFE20A9A743DA2F13A8E880007880440234FBB75F842ACA749C6368657072D219E4D3EFEB196AED3A2043A8856C76DEFEE76D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://campbaker.org/wp-content/plugins/mp-timetable/media/css/style.css?ver=2.3.11
Preview:	.mptt-main-wrapper .mptt-column.events-list .event .event-user .avatar,.mptt-main-wrapper .mptt-event.events-list .event .event-user .avatar{border-radius:50%}.twentyfourteen .tfmp{padding:12px 10px 0;max-width:474px;margin:0 auto}.twentyfourteen .tfmp div.product.hentry.has-post-thumbnail{margin-top:0}.twentythree h1{margin:0}.twentythree ul{padding:0}@media screen and (min-width:673px){.twentyfourteen .tfmp{padding-right:30px;padding-left:30px}}@media screen and (min-width:1040px){.twentyfourteen .tfmp{padding-right:15px;padding-left:15px}}@media screen and (min-width:1110px){.twentyfourteen .tfmp{padding-right:30px;padding-left:30px}}@media screen and (min-width:1218px){.twentyfourteen .tfmp{margin-right:54px}.full-width .twentyfourteen .tfmp{margin-right:auto}}.twentyfifteen .t15mp{padding-left:7.6923%;padding-right:7.6923%;padding-top:7.6923%;margin-bottom:7.6923%;background:#fff;-webkit-box-shadow:0 0 1px rgba(0,0,0,.15);box-shadow:0 0 1px rgba(0,0,0,.15)}.twentyfifteen .mp

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\5D02472\style[2].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Size (bytes):	447
Entropy (8bit):	4.984924551107894
Encrypted:	false
MD5:	49E085DE472AA7CF9E6FB92EDF3E7909
SHA1:	14AD2132459F383B97FCF63E8EBB9E32DA34D4A1
SHA-256:	CF8B6AE6E4DF82901EA13166D8772235B5E5FBCE1DA56A80F9F4B3E645D1A0A
SHA-512:	63D24D2D6B9B0833B2A52F7F607D6AD56DE9BF4651EEC7CD97F55D5A628F2CBEE408584346C5B9D70529B9ED42044CD607A7EBE8AC9F29F83843E7F196A2E51
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://campbaker.org/wp-content/themes/diwine-child/style.css?ver=5.4.1
Preview:	/* .Theme Name: Baker - Child.Version: 1.2.Text Dmain: diwine-child.Domain Path: /lang.License: GNU General Public License v2 or later.License URI: http://www.gnu.org/licenses/gpl-2.0.html.Tags: one-column, two-columns, right-sidebar, custom-header, custom-menu, editor-style, featured-images, microformats, post-formats, sticky-post, translation-ready..*/.....diwine-primary-nav > li:not(.logo) > a > span > .fl::first-letter { font-size: 100%; }.

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\5D02472\styles[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Size (bytes):	4470
Entropy (8bit):	4.8387786020784
Encrypted:	false
MD5:	C354C4152FA3FC098875AA6185D97277
SHA1:	889DCEC765845792AFA938A51FAA2E3F268CB2E7
SHA-256:	096F92193CFFC3B52C97F2CA32EE16BECDBB895475615E49456D9E0B457CED3C
SHA-512:	8703AD7F8C1DF96617C4194D1E53A3A157560917A112F117721BE68F2BA2399F19BD36226366F1D029D4F4B71180C274D50DDBB84E0AEFEE6199DBB928AA9672
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://campbaker.org/wp-content/plugins/booked-frontent-agents/css/styles.css?ver=2.2.6
Preview:	.booked-fea-appt-list { border:none; padding:0; background:transparent; margin:0; }..booked-fea-appt-list .appt-block { border-top:1px solid #ddd; padding:13px 0 18px; display:block; font-size:14px; box-sizing:border-box; line-height:1.7; font-family:"Open Sans",sans-serif; }..booked-fea-appt-list .appt-block .booked-icon { width:23px; }..booked-fea-appt-list .appt-block a { font-size:16px; font-weight:600; text-decoration:none; }..booked-fea-appt-list .appt-block button { float:right; margin:11px 0 0 0; }..booked-fea-appt-list .appt-block a.delete { float:right; margin:11px 0 0 20px; font-size:20px; line-height:1.3; color:#F59E9E; }..booked-fea-appt-list .appt-block a.delete:hover { color:#E35656; }..booked-fea-appt-list .appt-block .late-appt { color:#D54E21; }..booked-fea-appt-list .appt-block a.booked-show-cf { font-size:13px; font-weight:400; }...booked-fea-buttons, .booked-wc_status-text { float:right; margin-top:7px; }..booked-fea-appt-list .appt-block a.delete { margin:2px 0 0

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\5D02472\timeline_v2[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Size (bytes):	24416
Entropy (8bit):	4.860729194353463
Encrypted:	false
MD5:	C173991D11A9A8D9FCA9356CF0E3FAB
SHA1:	3DFADAF82060841F31E58FD667BF1D8E9A5C6698
SHA-256:	E0ECF004D1D4396CD320A69605A6D022D89CE1597FEBD4F4D3E180ACCCCF0AEF
SHA-512:	4F2647FE7B4D038AF4D4DCC7AC0CBA8F746E9B47F80A1B072940D4A678BF9BC84F2A3E33A118C1E59BC44CCFCE56598375D8A09D9EFA8F9CD9611CE2B6663EE
Malicious:	false





<b>C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\5D02472\woocommerce-add-to-cart[1].js</b>	
Size (bytes):	992
Entropy (8bit):	4.9227811183632095
Encrypted:	false
MD5:	787FE4F547A6CB7F4CE4934641085910
SHA1:	C2DEE88D5BDFEF214CE9C56F71A1Df51CDA0F328
SHA-256:	654AAEBDEA944313257827BE97EB196A8218A2CDFC9BA399DB23E2CD4C02BD79
SHA-512:	E55A14C83A65DED7853759BD3F7245E57D51062B5434D8D91BEA41551F7B81FFE6DA17BD7DD86029DA2D30CB8A74FFC955B71B137530A19094FC2C3329CDAD3
Malicious:	false
Reputation:	low
IE Cache URL:	<a href="http://https://campbaker.org/wp-content/plugins/js_composer/assets/js/vendors/woocommerce-add-to-cart.js?ver=6.1">http://https://campbaker.org/wp-content/plugins/js_composer/assets/js/vendors/woocommerce-add-to-cart.js?ver=6.1</a>
Preview:	(function ( \$ ) { 'use strict'; \$( document ).ready( function () { ...\$( 'body' ).on( 'adding_to_cart', function ( event, \$button, data ) { ...if ( \$button && \$button.hasClass( 'vc_gitem-link' ) ) { .....\$button.....addClass( 'vc-gitem-add-to-cart-loading-btn' ).....parents( '._vc_grid-item-mini' ).....addClass( 'vc-woocommerce-add-to-cart-loading' ).. .....append( \$( ' <div class="vc_wc-load-add-to-loader-wrapper"><div class="vc_wc-load-add-to-loader"></div></div>' ) ); .....}...} ) }, on( 'added_to_cart', function ( event, fragments, cart_hash, \$button ) { ...if ( 'undefined' === typeof ( \$button ) ) { .....\$button = \$( '._vc-gitem-add-to-cart-loading-btn' ); .....}...if ( \$button && \$button.hasClass( 'vc_gitem-link' ) ) { .....\$button.....removeClass( 'vc-gitem-add-to-cart-loading-btn' ).....parents( '._vc_grid-item-mini' ).....removeClass( 'vc-woocommerce-add-to-cart-loading' ).....find( '._vc_wc-load-add-to-loader-wrapper' ).remove(); .....}...}...} ); } )( window.jQuery ); }

<b>C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\5D02472\woocommerce-smallscreen[1].css</b>	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Size (bytes):	6758
Entropy (8bit):	4.594691317926526
Encrypted:	false
MD5:	98F4E97F86B642BF082C65AE518AD010
SHA1:	E4E05EB15EE57F2CDB00A2A97419C02CFEBB2732
SHA-256:	5302D7EF47B197C6CC07E5DB5152DCCE3B6886AC18F727875FE78BA8E8129224
SHA-512:	D2635614BACB07155499EAF1A95C146CD7D9BC55E63238C9D99CBDF6439E1D70A9570820A955EB09DB37D33E9FDC061C38CF187D466DD9544C586AB51B2A0C8
Malicious:	false
Reputation:	low
IE Cache URL:	<a href="http://https://campbaker.org/wp-content/plugins/woocommerce/assets/css/woocommerce-smallscreen.css?ver=4.1.1">http://https://campbaker.org/wp-content/plugins/woocommerce/assets/css/woocommerce-smallscreen.css?ver=4.1.1</a>
Preview:	.woocommerce table.shop_table_responsive thead,.woocommerce-page table.shop_table_responsive thead{display:none}.woocommerce table.shop_table_responsive tbody tr:first-child td:first-child,.woocommerce-page table.shop_table_responsive tbody tr:first-child td:first-child{border-top:0}.woocommerce table.shop_table_responsive tbody th,.woocommerce-page table.shop_table_responsive tbody th{display:none}.woocommerce table.shop_table_responsive tr,.woocommerce-page table.shop_table_responsive tr{display:block}.woocommerce table.shop_table_responsive tr td,.woocommerce-page table.shop_table_responsive tr td{display:block;text-align:right!important}.woocommerce table.shop_table_responsive tr td.order-actions,.woocommerce-page table.shop_table_responsive tr td.order-actions{text-align:left!important}.woocommerce table.shop_table_responsive tr td::before,.woocommerce-page table.shop_table_responsive tr td::before{content:attr(data-title) "": "","font-weight:700,float:left}.woocommerce table.shop_ta

<b>C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\5D02472\wp-emoji-release.min[1].js</b>	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Size (bytes):	13901
Entropy (8bit):	4.982641681323462
Encrypted:	false
MD5:	EC33F485BA2D4767DAE9D112B78F8B02
SHA1:	D33A60FCB35865F5E2D8B30112715329759096F1
SHA-256:	96D33F532112177EDE6BF262DCF6D0140DBE29F05A4595D17B0BE4743205B5EA
SHA-512:	A4CA6F2468B2A98123271DA6D96AF937AF0443AC506BE99F5E0A05D119C3097C1BB1184D44FF659169AA1135F3724F1FEEA0FB6551E16BEAEC75E56842E2F44
Malicious:	false
Reputation:	low
IE Cache URL:	<a href="http://https://campbaker.org/wp-includes/js/wp-emoji-release.min.js?ver=5.4.1">http://https://campbaker.org/wp-includes/js/wp-emoji-release.min.js?ver=5.4.1</a>
Preview:	/*! This file is auto-generated */ // Source: wp-includes/js/twemoji.min.js var twemoji=function(){ "use strict"; var f={base:"https://twemoji.maxcdn.com/v/12.1.3/",ext:".png",size:"72x72",className:"emoji"},convert:{fromCodePoint:function(d){var u="string"===typeof d?parseInt(d,16):d;if(u<65536)return a(u);return a(55296+(u-=65536)>>10),56320+(1023&u))},toCodePoint:i},onerror:function(){this.parentNode&&this.parentNode.replaceChild(C(this.alt,!1),this)},parse:function(d,u){u&&"function"!==typeof u   (u={callback:u});return("string"===typeof d?function(d,b){return o(d,function(d){var u,f,c=d,e=N(d),a=b.callback(e,b);if(e&&a){for(f in c)=""<img ".concat("class=",".b.class Name," " ;draggable="false" ' ,alt="",d,"" ; src="",a,""),u=b.attributes(d,e))u.hasOwnProperty(f)&&0!==f.indexOf("on")&&1===c.indexOf(" "+f+"=")}&&(c=c.concat(" ",f,"=",".u[f].replace(t,r,"")));c=c.concat(">")}return c)}}:function(d,u){var f,c,e,a,b,t,r,n,o,i,s,l,p,m=function d(u,f){var c,e,a=u.childNodes,b=a.length;for(;b-

<b>C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\VINVDFP6\SIGDmQSNjdsmc35JDF1K5E55YMjF_7DPuGi-a_NkBI95[1].woff</b>	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 34104, version 1.1
Size (bytes):	34104
Entropy (8bit):	7.9846349087088635
Encrypted:	false
MD5:	42F5FF27E4EC8C0C774D8072D357DEAB

<b>C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\INVDFP6\SIGDmQSNjdsmc35JDF1K5E55YMjF_7DPuGi-a_NkBI95[1].woff</b>	
SHA1:	61E375121FB59CCF135FB67EABE852D0338F62F5
SHA-256:	E4954039AEE34E8FE39D30B0EE7CB3EC5416AA75802FB7B2BCCA841B8420C4C0
SHA-512:	85200FB54888B0A5F60F674EE3DD32D1755FD8ABC6E346F684EA170CC236E7F47CFEB759CA019BFF62D9CE72D4ED544FAD52CE3489E6824C3F32B66A41DA663
Malicious:	false
Reputation:	low
IE Cache URL:	<a href="http://https://fonts.gstatic.com/s/ebgaramond/v13/SIGDmQSNjdsmc35JDF1K5E55YMjF_7DPuGi-a_NkBI95.woff">http://https://fonts.gstatic.com/s/ebgaramond/v13/SIGDmQSNjdsmc35JDF1K5E55YMjF_7DPuGi-a_NkBI95.woff</a>
Preview:	wOFF.....8.....GDEF.....=...F....GPOS.....GSUB.....#.....OS/2.....R...`ZK..STAT...X...8...D...cmap.....f...t.9cvt .....&^2fpgm..... .6..gasp.....glyf.....d.....g74.head.}....6...6..hhea.}....\$..lhmTx..}....>...loca...X...l..IX..Emaxp..... ..name.....G...F.jlpost.....2prep...@.....x.....P .....l.....*...y2..7{>...r..?R.....x.....H...v..c...h.m.m.sm.w..9Z.V.?.3}..%{....d\$e.....?l..Y:..OY.P..(J2.f.)@b.r.d..Oz.4....3..5..q..s.y. b'..b8.s~.wY...q...-.2.?...0. ..OZ.S.j...b7....l.8..3.....f...'.v\...E.((...Rm...! S.v.Ne...."Wet.O... .W54@c.X..BM.B.i.....'=G5DO.#..1J....1F...zCoj.&&.di.1.*..7...6=..}....].[Ews.9...2{W...`!)W&z N.l8p..G..H.B.iT0...q..X...v..F.;i7uop..h..kL..&s.....TQA6\$...a.A.";;.F."_s'.E....7.l.....U.Q..n4Y.....Q...P...r7.....H.3.z...1...l.....}Sz..5...". C.9

<b>C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\INVDFP6\SIGFmQSNjdsmc35JDF1K5GRwUjcdlttVFm-r17c8R799U64[1].woff</b>	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 35368, version 1.1
Size (bytes):	35368
Entropy (8bit):	7.985424529159467
Encrypted:	false
MD5:	22989DA1412AFF5D3EAD93F803F9B06F
SHA1:	97B1FE0B2854C7A80F8898B8162E6192E92487E1
SHA-256:	E0EBAD058FA19B8985F6F56C7D598012F34C18417668A7EDC84955F57AABA234
SHA-512:	5371CF45393E6FED6059194097E831A023DD26281CE22E01FB66F8403984BAAB0E521E3FE58E81EAF305C8F0CC0EAC191253DAEBD40286F0DB83B996AE004F3
Malicious:	false
Reputation:	low
IE Cache URL:	<a href="http://https://fonts.gstatic.com/s/ebgaramond/v13/SIGFmQSNjdsmc35JDF1K5GRwUjcdlttVFm-r17c8R799U64.woff">http://https://fonts.gstatic.com/s/ebgaramond/v13/SIGFmQSNjdsmc35JDF1K5GRwUjcdlttVFm-r17c8R799U64.woff</a>
Preview:	wOFF.....(.....GDEF.....M...j.X..GPOS.....~...B...MGSUB...d...7... . @.OS/2.....U...`ZL..STAT.....6...@.8..cmap.....^.....n..cvt .....Q..Ofpgm... p.....6..gasp...0.....glyf...8..k .....9.head.....6...6.m.hhea.....\$...\$.dhmtx.....X...loca.....@a maxp..... ..name.....@....l.j.post... ..prep...8..... s=ax.....`..{@.\$Z .!....(-.FI.N.)l.....N{...tf.....\z[X.ZX.....d...x\...]A....[Nm.m3.m..nX.m.Am.t./...Yb.\$...^f-l1.....&...<+el'.gi.f..L3..a.6K.r\U...f..MT...vu....@ !.*.o.e;.....O;...eJ.v...+.....X.....Y W.k.u.fz...~.....M0.Kz...\$...\$#.Hl.....B.S..T...iB.9...@U:1P..L9S...&.]B/..9)....\.....C.... p...'.j.f.x1.....a. ..T...V.....bV..)....c*. ..o%y...*.9 ...-.j.....N..%.....b-[2.[S..Jl.S..8*....\$T..W..#...f.....h}.....u....K.s.=Uo]...s.....L!.....Q..N...@.....&.....5..y.>F9

<b>C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\INVDFP6\SIGFmQSNjdsmc35JDF1K5GRwUjcdlttVFm-r17dbR799U64[1].woff</b>	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 36240, version 1.1
Size (bytes):	36240
Entropy (8bit):	7.985443624734326
Encrypted:	false
MD5:	0E81FA35186C5A5327D4EC10E0314C7C
SHA1:	9EBE146752C0299F669C7A5C32315968C223E696
SHA-256:	9E7F8BFC57F764EC10A6CEDB3DC77C206FA72AB471F60790622FF3BDBD7C5269
SHA-512:	4A34489C03910D43C5960B5357CF002804850A3A9A43DD0A288EDAF526B0E79068A4E9091E3B34F6CCEB3B36F66821FEE52E8EE9D68B3BE2ADF311E46000F38f
Malicious:	false
Reputation:	low
IE Cache URL:	<a href="http://https://fonts.gstatic.com/s/ebgaramond/v13/SIGFmQSNjdsmc35JDF1K5GRwUjcdlttVFm-r17dbR799U64.woff">http://https://fonts.gstatic.com/s/ebgaramond/v13/SIGFmQSNjdsmc35JDF1K5GRwUjcdlttVFm-r17dbR799U64.woff</a>
Preview:	wOFF.....p.....GDEF.....M...j.X..GPOS.....+...R+1.]GSUB.....7... . @.OS/2...H...U...`Y.>STAT.....6...@.....cmap.....^.....n..cvt ...8.....Q..Ofpgm..... 6..gasp.....glyf.....n%...B...head.....6...6.n.hhea...D...\$...\$.dhmtx...h.....X...)loca.....f.maxp...8... ..name...X...0...>dZ.post..... ..prep.....s=ax.....` ...{@.\$Z .!....(-.FI.N.)l.....N{...tf.....\z[X.ZX.....d...x\...K...ozgvol.vr...m.v...m>v...~...Zy.*J.T.Q...<l.../k ...}....@ (...[.....<.W.W...{.....#....1..7.XS.a.=...f...J...~.7 #...0\5.3..V...m.#.../w....<N...7-J...o.....{&A.'V.!(<lFi.)")YY.X9_TPE.V.*.....T.^R{#;@cU_4..b-W'&k=C...G...Vo...Yb...-u...A{A..+;k?G..l{...Z...>...#@..d b 6.cm...b....(K.l.e..-.....j..S..t..._.....{XG.v...e...R.e8`Q.\2.?Df.#...h.....v...D...f3*.f.....@<...w.sb.x...v\$.z...m.z...%..

<b>C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\INVDFP6\animations[1].css</b>	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Size (bytes):	3778
Entropy (8bit):	4.928798654332237
Encrypted:	false
MD5:	1BC68B4E9B9744C520A771E30E49A29C
SHA1:	8FEFA74ECAAFE6D7CE5AE1B9DCBF9622E87688A4
SHA-256:	E4202303588535D6C32E866487F113FF26A493FAC6445CF3DACC533C521CD161
SHA-512:	67C7737398D165F906A8B6FA24FE8E3809185CB3D4F981DCCD4D6D0572D54EDF56C113373B7DF4773AC5D31D954CE9B1AB2B1BE97012E174048C7A337573A9f
Malicious:	false
Reputation:	low
IE Cache URL:	<a href="http://https://campbaker.org/wp-content/plugins/booked/assets/css/animations.css?ver=2.2.6">http://https://campbaker.org/wp-content/plugins/booked/assets/css/animations.css?ver=2.2.6</a>



<b>C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\IN\VD\FP6\animations[1].css</b>	
Preview:	<pre>/* Modal Fly In */.keyframes booked-flyin { .0% { opacity: 0; transform: scale(0.9); }..100% { opacity: 1; transform: scale(1); } }.-webkit-keyframes booked-flyin {..0% { opacity: 0; -webkit-transform: scale(0.9); }..100% { opacity: 1; -webkit-transform: scale(1); } }.-moz-keyframes booked-flyin {..0% { opacity: 0; -moz-transform: scale(0.9); }..100% { opacity: 1; -moz-transform: scale(1); } }.-ms-keyframes booked-flyin {..0% { opacity: 0; -ms-transform: scale(0.9); }..100% { opacity: 1; -ms-transform: scale(1); } }.-o-keyframes booked-flyin {..0% { opacity: 0; -o-transform: scale(0.9); }..100% { opacity: 1; -o-transform: scale(1); } }.* Datepicker Pop Flyin */.keyframes booked-popflyin { .0% { opacity: 0; transform: scale(0.95); } .50% { opacity: 1; transform: scale(1.01); }..100% { opacity: 1; transform: scale(1); } }.-webkit-keyframes booked-popflyin {..0% { opacity: 0; -webkit-transform: scale(0.95); }..50% { opacity: 1; -webkit-transform: scale(1.01); }..100% { op</pre>

<b>C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\IN\VD\FP6\bootstrap-theme[1].css</b>	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Size (bytes):	29166
Entropy (8bit):	5.191467886427775
Encrypted:	false
MD5:	79B12342C0C9FF028ABE94DA7FC86A63
SHA1:	82CC341E1643F884FFD7F6ABCFEBC83428E5FEA4
SHA-256:	B143244B6B6B5E2163952143B94E57841D7DD53BF6E85A88DAB9C663BD73BB98
SHA-512:	3CDD52D69E25043AF2AF18F6837E72A7D1FACE41C65CCA202EE97B3FBFA23B4D6B0631A1892C15A318C7A089D9B0DE2B88A001A3BB7FBA682C2806EA644940DE
Malicious:	false
Reputation:	low
IE Cache URL:	<a href="http://https://campbaker.org/wp-content/plugins/booking/assets/libs/bootstrap/css/bootstrap-theme.css?ver=3.3.5.1">http://https://campbaker.org/wp-content/plugins/booking/assets/libs/bootstrap/css/bootstrap-theme.css?ver=3.3.5.1</a>
Preview:	<pre>/*! * Bootstrap v3.3.5 (http://getbootstrap.com).. * Copyright 2011-2015 Twitter, Inc... * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE).. */./*! * Generated using the Bootstrap Customizer (http://getbootstrap.com/customize/?id=f4b4c9cb85df757ca08c).. * Config saved to config.json and https://gist.github.com/f4b4c9cb85df757ca08c.. */./*! * Bootstrap v3.3.5 (http://getbootstrap.com).. * Copyright 2011-2015 Twitter, Inc... * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE).. */...wpdevelop .btn-default,...wpdevelop .btn-primary,...wpdevelop .btn-success,...wpdevelop .btn-info,...wpdevelop .btn-warning,...wpdevelop .btn-danger {.. text-shadow: 0 -1px 0 rgba(0, 0, 0, 0.2);.. -webkit-box-shadow: inset 0 1px 0 rgba(255, 255, 255, 0.15), 0 1px 1px rgba(0, 0, 0, 0.075);.. box-shadow: inset 0 1px 0 rgba(255, 255, 255, 0.15), 0 1px 1px rgba(0, 0, 0, 0.075);}...wpdevelop .btn-default:active,...wpdevelop .btn-primary:active,...wpd</pre>

<b>C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\IN\VD\FP6\bootstrap[1].css</b>	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Size (bytes):	182631
Entropy (8bit):	5.0262539525636605
Encrypted:	false
MD5:	CFA860F2D48CDD8B2DCF837DD07A4E2A
SHA1:	52421E957D4D3A615D989EAAB224D1F4A5DDE7C9
SHA-256:	7CF3488ACE5C95CF9951682C4DB9AF8F8199DAC61675CF7778BD18437100229DA
SHA-512:	B35AD99C8C185585DDED8B04E37043170741EB32403D45620C359B34C1D273786659AB95404427D6B47E8CEB6F0F0DAD5D0971A15E38F7BFD5AACFD44E96053
Malicious:	false
Reputation:	low
IE Cache URL:	<a href="http://https://campbaker.org/wp-content/plugins/booking/assets/libs/bootstrap/css/bootstrap.css?ver=3.3.5.1">http://https://campbaker.org/wp-content/plugins/booking/assets/libs/bootstrap/css/bootstrap.css?ver=3.3.5.1</a>
Preview:	<pre>/*! * Bootstrap v3.3.5 (http://getbootstrap.com).. * Copyright 2011-2015 Twitter, Inc... * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE).. */./*! * Generated using the Bootstrap Customizer (http://getbootstrap.com/customize/?id=f4b4c9cb85df757ca08c).. * Config saved to config.json and https://gist.github.com/f4b4c9cb85df757ca08c.. */./*! * Bootstrap v3.3.5 (http://getbootstrap.com).. * Copyright 2011-2015 Twitter, Inc... * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE).. */./*! normalize.css v3.0.3   MIT License   github.com/necolas/normalize.css */./*! Source: https://github.com/h5bp/html5-boilerplate/blob/master/src/css/main.css */...wpdevelop article,...wpdevelop aside,...wpdevelop details,...wpdevelop figcaption,...wpdevelop figure,...wpdevelop footer,...wpdevelop header,...wpdevelop hgroup,...wpdevelop main,...wpdevelop menu,...wpdevelop nav,...wpdevelop section,...wpdevelop summary {... display: block;}...wpdeve</pre>

<b>C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\IN\VD\FP6\camp-baker-faq-button-384x186[1].jpg</b>	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], baseline, precision 8, 384x186, frames 3
Size (bytes):	14866
Entropy (8bit):	7.949034338561408
Encrypted:	false
MD5:	3519B801B084EEA126B06A85891ECA15
SHA1:	B4CD09D53334DC90E95EFE02D991F392ABD757E0
SHA-256:	DEB8387C3DE42170AE449981CE9228FEB8A662BA48C50B9221DC61E02EA31A1E
SHA-512:	996FC0C9B996FE465939E5A8E2DE2352CE6136F0E63C5B32506475C6495FDE687D72BCFEA4CE7E334642CE50C516FC5E0B74C9A090CA3FD9742F6BE15EF2C3
Malicious:	false
Reputation:	low
IE Cache URL:	<a href="http://https://campbaker.org/wp-content/uploads/2019/04/camp-baker-faq-button-384x186.jpg">http://https://campbaker.org/wp-content/uploads/2019/04/camp-baker-faq-button-384x186.jpg</a>



C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\IN\VD\FP6\css[1].css

Preview:	@font-face { font-family: 'EB Garamond'; font-style: italic; font-weight: 400; src: url(https://fonts.gstatic.com/s/ebgaramond/v13/SIGFmQSNjdsmc35JDF1K5GRwUjcdlttVFm-r17e8QL99U64.woff) format('woff'); }.@font-face { font-family: 'EB Garamond'; font-style: italic; font-weight: 500; src: url(https://fonts.gstatic.com/s/ebgaramond/v13/SIGFmQSNjdsmc35JDF1K5GRwUjcdlttVFm-r17eOQL99U64.woff) format('woff'); }.@font-face { font-family: 'EB Garamond'; font-style: italic; font-weight: 600; src: url(https://fonts.gstatic.com/s/ebgaramond/v13/SIGFmQSNjdsmc35JDF1K5GRwUjcdlttVFm-r17diR799U64.woff) format('woff'); }.@font-face { font-family: 'EB Garamond'; font-style: italic; font-weight: 700; src: url(https://fonts.gstatic.com/s/ebgaramond/v13/SIGFmQSNjdsmc35JDF1K5GRwUjcdlttVFm-r17dbR799U64.woff) format('woff'); }.@font-face { font-family: 'EB Garamond'; font-style: italic; font-weight: 800; src: url(https://fonts.gstatic.com/s/ebgaramond/v13/SIGFmQSNjdsmc35JD
----------	--

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\IN\VD\FP6\date-time-picker[1].js

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Size (bytes):	42615
Entropy (8bit):	5.66691014255613
Encrypted:	false
MD5:	6EF922E126EFDA37D5672BCA837F59E5
SHA1:	94D03B9E281E17F072ABAF1F00BB75ED96F46C48
SHA-256:	B33DEA89C8288B9AD239E5FF4F197226260E61628E7330D254B031802480C866
SHA-512:	42ACF41DB46F8BD4AE5192DDFEA67BD5299D9054102E7091B62F726FFC728534D086DEB1838C44C8A52940B2E06EE3D989EECD33519B40D96CA8940EB897BB6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://campbaker.org/wp-content/themes/diwine/scripts/vendor/date-time/date-time-picker.js
Preview:	// Parse and Format Library../http://www.xaprb.com/blog/2005/12/12/javascript-closures-for-runtime-efficiency/..* Copyright (C) 2004 Baron Schwartz <baron at sequent dot org>..* * This program is free software; you can redistribute it and/or modify it..* under the terms of the GNU Lesser General Public License as published by the..* Free Software Foundation, version 2.1...* * This program is distributed in the hope that it will be useful, but WITHOUT..* ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS..* FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more..* details...*/..Date.parseFunctions=[count:0];Date.parseRegexes=[];Date.formatFunctions={count:0};Date.prototype.dateFormat=function(b){if(b=="unixtime"){return parseInt(this.getTime()/1000);}if(Date.formatFunctions[b]==null){Date.createNewFormat(b);}var a=Date.formatFunctions[b];return this[a]()};Date.createNewFormat=function(format){var funcName="format"+Date

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\IN\VD\FP6\diwine-extended-scripts[1].js

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Size (bytes):	9486
Entropy (8bit):	5.089008524353261
Encrypted:	false
MD5:	5C9A87A0DE2FC6D6146F703790EB6BCA
SHA1:	5CA1A3A6D2F9619044CDEDD2D47EBEDCEDAAAD48
SHA-256:	4B01F984D3BBF0513A4C3D4E2D93A67DB969BD405EF08AECC5B6284BB842D31F
SHA-512:	529A32F0E285C41087DFCC143A053649A75386C180FD765A816C77FF3A25A422F163802CEE960C6E04C546BBC67991E1B3D10E8322B2C40833794743934FD988
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://campbaker.org/wp-content/themes/diwine/scripts/diwine-extended-scripts.js
Preview:	/*..* SVG replacer. Replaces <img src=svg/> into SVG element...* Credits: How to change color of SVG image using CSS (jQuery SVG image replacement)?, http://stackoverflow.com/q/11978995..*/..jQuery(function(){... "use strict";...try {...jQuery('img.svg,.wpb_single_image.svg>figure>div>img').each(function(){.....var \$img = jQuery(this);.....var imgID = \$img.attr('id');.....var imgClass = \$img.attr('class');.....var imgURL = \$img.attr('src');.....jQuery.get(imgURL, function(data) {.....// Get the SVG tag, ignore the rest.....var \$svg = jQuery(data).find('svg');.....// Add replaced image's ID to the new SVG.....if(typeof imgID !== 'undefined') {.....\$svg = \$svg.attr('id', imgID);.....}.....// Add replaced image's classes to the new SVG.....if(typeof imgClass !== 'undefined') {.....\$svg = \$svg.attr('class', imgClass+' replaced-svg');.....}.....// Remove any invalid XML tags as per http://validator.w3.org.....\$svg = \$svg.removeAttr('xmlns:a');.....}.....// Che

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\IN\VD\FP6\donate-today-384x186[1].jpg

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], baseline, precision 8, 384x186, frames 3
Size (bytes):	14645
Entropy (8bit):	7.954415757726568
Encrypted:	false
MD5:	CD50D2DBFBE04EFBC1FD1379B50992F2
SHA1:	0B076AC1B5D254313DD3136DD0EBB0D1874D51FE
SHA-256:	EBE9EE9582E2040B9C81CD8BD5A2F0B1D34068BA758201265387177C63147B11
SHA-512:	7858EBC5C74574E21C17ED54B77E203AD014772855A4E9178F2F153C8C0AE98C4E793E897411A3474D75CBC280BFAF203C4303A0FFC373A814353754150F817FC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://campbaker.org/wp-content/uploads/2019/04/donate-today-384x186.jpg



Preview:

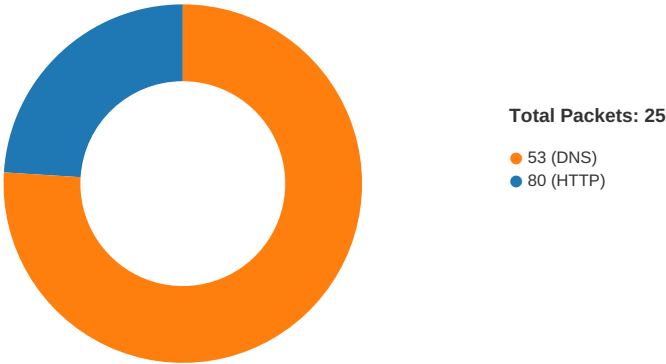
```
;(function($, window, document, undefined) {...var $win = $(window);...$win.on('load', function() {.....var ajaxRequests = [];.....// Add Pending Count to Tab...$('.booked-
tabs').find('li a div.counter').each(function(){...var thisCounter = $(this),.....thisTabName = $(this).parent().attr('href');.....thisTabName = thisTabName.split("#");.....th
isTabName = thisTabName[1];.....totalAppointments = $('#profile-'+thisTabName).find('.appt-block').length;.....if (totalAppointments > 0){.....thisCounter.html(totalAp
pointments).fadeIn('fast');.....});.....// User Info Click...$('.booked-fea-appt-list').on('click', '.user', function(e) {.....e.preventDefault();.....var $thisLink .= $(this),.....user_id...=
$thisLink.attr('data-user-id'),.....appt_id...= $thisLink.parent().attr('data-appt-id'),.....booked_ajaxURL.= booked_fea_vars.ajax_url;.....create_booked_modal();.....$.ajax({....
.url: booked_ajaxURL,.....type: 'post',.....data: {.....action: 'booked_fea_user_info_modal',.....
```

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 8, 2020 21:19:13.493494034 CEST	49732	80	192.168.2.5	167.89.118.52
Jun 8, 2020 21:19:13.493586063 CEST	49733	80	192.168.2.5	167.89.118.52
Jun 8, 2020 21:19:13.653384924 CEST	80	49732	167.89.118.52	192.168.2.5
Jun 8, 2020 21:19:13.653598070 CEST	49732	80	192.168.2.5	167.89.118.52
Jun 8, 2020 21:19:13.653742075 CEST	80	49733	167.89.118.52	192.168.2.5
Jun 8, 2020 21:19:13.653861046 CEST	49733	80	192.168.2.5	167.89.118.52
Jun 8, 2020 21:19:13.654131889 CEST	49732	80	192.168.2.5	167.89.118.52
Jun 8, 2020 21:19:13.814013958 CEST	80	49732	167.89.118.52	192.168.2.5
Jun 8, 2020 21:19:13.815409899 CEST	80	49732	167.89.118.52	192.168.2.5
Jun 8, 2020 21:19:13.815576077 CEST	49732	80	192.168.2.5	167.89.118.52
Jun 8, 2020 21:19:14.104581118 CEST	49735	443	192.168.2.5	192.185.166.140
Jun 8, 2020 21:19:14.104751110 CEST	49734	443	192.168.2.5	192.185.166.140
Jun 8, 2020 21:19:14.236517906 CEST	443	49735	192.185.166.140	192.168.2.5
Jun 8, 2020 21:19:14.236696005 CEST	49735	443	192.168.2.5	192.185.166.140
Jun 8, 2020 21:19:14.240142107 CEST	443	49734	192.185.166.140	192.168.2.5
Jun 8, 2020 21:19:14.240292072 CEST	49734	443	192.168.2.5	192.185.166.140
Jun 8, 2020 21:19:14.246222019 CEST	49734	443	192.168.2.5	192.185.166.140
Jun 8, 2020 21:19:14.246541023 CEST	49735	443	192.168.2.5	192.185.166.140
Jun 8, 2020 21:19:14.378679991 CEST	443	49735	192.185.166.140	192.168.2.5
Jun 8, 2020 21:19:14.379966974 CEST	443	49735	192.185.166.140	192.168.2.5
Jun 8, 2020 21:19:14.379997015 CEST	443	49735	192.185.166.140	192.168.2.5
Jun 8, 2020 21:19:14.380013943 CEST	443	49735	192.185.166.140	192.168.2.5
Jun 8, 2020 21:19:14.380130053 CEST	49735	443	192.168.2.5	192.185.166.140
Jun 8, 2020 21:19:14.381232023 CEST	443	49734	192.185.166.140	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 8, 2020 21:19:14.383025885 CEST	443	49734	192.185.166.140	192.168.2.5
Jun 8, 2020 21:19:14.383054972 CEST	443	49734	192.185.166.140	192.168.2.5
Jun 8, 2020 21:19:14.383075953 CEST	443	49734	192.185.166.140	192.168.2.5
Jun 8, 2020 21:19:14.383122921 CEST	49734	443	192.168.2.5	192.185.166.140
Jun 8, 2020 21:19:14.383244038 CEST	49734	443	192.168.2.5	192.185.166.140
Jun 8, 2020 21:19:14.417947054 CEST	49734	443	192.168.2.5	192.185.166.140
Jun 8, 2020 21:19:14.419980049 CEST	49735	443	192.168.2.5	192.185.166.140
Jun 8, 2020 21:19:14.424491882 CEST	49735	443	192.168.2.5	192.185.166.140
Jun 8, 2020 21:19:14.424623013 CEST	49734	443	192.168.2.5	192.185.166.140
Jun 8, 2020 21:19:14.424666882 CEST	49735	443	192.168.2.5	192.185.166.140
Jun 8, 2020 21:19:14.552083015 CEST	443	49735	192.185.166.140	192.168.2.5
Jun 8, 2020 21:19:14.552124977 CEST	443	49735	192.185.166.140	192.168.2.5
Jun 8, 2020 21:19:14.552165031 CEST	49735	443	192.168.2.5	192.185.166.140
Jun 8, 2020 21:19:14.552283049 CEST	49735	443	192.168.2.5	192.185.166.140
Jun 8, 2020 21:19:14.553267002 CEST	443	49734	192.185.166.140	192.168.2.5
Jun 8, 2020 21:19:14.553297997 CEST	49735	443	192.168.2.5	192.185.166.140
Jun 8, 2020 21:19:14.553322077 CEST	443	49734	192.185.166.140	192.168.2.5
Jun 8, 2020 21:19:14.553360939 CEST	49734	443	192.168.2.5	192.185.166.140
Jun 8, 2020 21:19:14.553436041 CEST	49734	443	192.168.2.5	192.185.166.140
Jun 8, 2020 21:19:14.554325104 CEST	49734	443	192.168.2.5	192.185.166.140
Jun 8, 2020 21:19:14.556349993 CEST	443	49735	192.185.166.140	192.168.2.5
Jun 8, 2020 21:19:14.556677103 CEST	49735	443	192.168.2.5	192.185.166.140
Jun 8, 2020 21:19:14.559696913 CEST	443	49734	192.185.166.140	192.168.2.5
Jun 8, 2020 21:19:14.559863091 CEST	49734	443	192.168.2.5	192.185.166.140
Jun 8, 2020 21:19:14.596981049 CEST	443	49735	192.185.166.140	192.168.2.5
Jun 8, 2020 21:19:14.685265064 CEST	443	49735	192.185.166.140	192.168.2.5
Jun 8, 2020 21:19:14.729953051 CEST	443	49734	192.185.166.140	192.168.2.5
Jun 8, 2020 21:19:15.381541014 CEST	443	49735	192.185.166.140	192.168.2.5
Jun 8, 2020 21:19:15.381580114 CEST	443	49735	192.185.166.140	192.168.2.5
Jun 8, 2020 21:19:15.381593943 CEST	443	49735	192.185.166.140	192.168.2.5
Jun 8, 2020 21:19:15.381609917 CEST	443	49735	192.185.166.140	192.168.2.5
Jun 8, 2020 21:19:15.381622076 CEST	443	49735	192.185.166.140	192.168.2.5
Jun 8, 2020 21:19:15.381633997 CEST	443	49735	192.185.166.140	192.168.2.5
Jun 8, 2020 21:19:15.381644964 CEST	443	49735	192.185.166.140	192.168.2.5
Jun 8, 2020 21:19:15.381661892 CEST	443	49735	192.185.166.140	192.168.2.5
Jun 8, 2020 21:19:15.381757975 CEST	443	49735	192.185.166.140	192.168.2.5
Jun 8, 2020 21:19:15.381772995 CEST	443	49735	192.185.166.140	192.168.2.5
Jun 8, 2020 21:19:15.381783009 CEST	49735	443	192.168.2.5	192.185.166.140
Jun 8, 2020 21:19:15.381827116 CEST	49735	443	192.168.2.5	192.185.166.140
Jun 8, 2020 21:19:15.513621092 CEST	443	49735	192.185.166.140	192.168.2.5
Jun 8, 2020 21:19:15.513760090 CEST	443	49735	192.185.166.140	192.168.2.5
Jun 8, 2020 21:19:15.513782024 CEST	443	49735	192.185.166.140	192.168.2.5
Jun 8, 2020 21:19:15.513842106 CEST	49735	443	192.168.2.5	192.185.166.140
Jun 8, 2020 21:19:15.513896942 CEST	49735	443	192.168.2.5	192.185.166.140
Jun 8, 2020 21:19:15.528978109 CEST	49735	443	192.168.2.5	192.185.166.140
Jun 8, 2020 21:19:15.529160976 CEST	49735	443	192.168.2.5	192.185.166.140
Jun 8, 2020 21:19:15.529406071 CEST	49735	443	192.168.2.5	192.185.166.140
Jun 8, 2020 21:19:15.533809900 CEST	49735	443	192.168.2.5	192.185.166.140
Jun 8, 2020 21:19:15.533999920 CEST	49735	443	192.168.2.5	192.185.166.140
Jun 8, 2020 21:19:15.534212112 CEST	49735	443	192.168.2.5	192.185.166.140
Jun 8, 2020 21:19:15.534421921 CEST	49735	443	192.168.2.5	192.185.166.140
Jun 8, 2020 21:19:15.534646988 CEST	49735	443	192.168.2.5	192.185.166.140
Jun 8, 2020 21:19:15.534879923 CEST	49735	443	192.168.2.5	192.185.166.140
Jun 8, 2020 21:19:15.535120010 CEST	49735	443	192.168.2.5	192.185.166.140
Jun 8, 2020 21:19:15.535337925 CEST	49735	443	192.168.2.5	192.185.166.140
Jun 8, 2020 21:19:15.535577059 CEST	49735	443	192.168.2.5	192.185.166.140
Jun 8, 2020 21:19:15.539347887 CEST	49735	443	192.168.2.5	192.185.166.140
Jun 8, 2020 21:19:15.539561987 CEST	49735	443	192.168.2.5	192.185.166.140
Jun 8, 2020 21:19:15.546926022 CEST	49735	443	192.168.2.5	192.185.166.140
Jun 8, 2020 21:19:15.547245026 CEST	49735	443	192.168.2.5	192.185.166.140
Jun 8, 2020 21:19:15.547512054 CEST	49735	443	192.168.2.5	192.185.166.140
Jun 8, 2020 21:19:15.548193932 CEST	49735	443	192.168.2.5	192.185.166.140
Jun 8, 2020 21:19:15.548283100 CEST	49735	443	192.168.2.5	192.185.166.140
Jun 8, 2020 21:19:15.548422098 CEST	49735	443	192.168.2.5	192.185.166.140

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 8, 2020 21:19:15.548547029 CEST	49735	443	192.168.2.5	192.185.166.140
Jun 8, 2020 21:19:15.548736095 CEST	49735	443	192.168.2.5	192.185.166.140
Jun 8, 2020 21:19:15.548883915 CEST	49735	443	192.168.2.5	192.185.166.140
Jun 8, 2020 21:19:15.557009935 CEST	49735	443	192.168.2.5	192.185.166.140
Jun 8, 2020 21:19:15.557266951 CEST	49735	443	192.168.2.5	192.185.166.140
Jun 8, 2020 21:19:15.557647943 CEST	49735	443	192.168.2.5	192.185.166.140
Jun 8, 2020 21:19:15.558382034 CEST	49735	443	192.168.2.5	192.185.166.140
Jun 8, 2020 21:19:15.558839083 CEST	49735	443	192.168.2.5	192.185.166.140
Jun 8, 2020 21:19:15.559060097 CEST	49735	443	192.168.2.5	192.185.166.140
Jun 8, 2020 21:19:15.598258018 CEST	49735	443	192.168.2.5	192.185.166.140
Jun 8, 2020 21:19:15.622723103 CEST	49735	443	192.168.2.5	192.185.166.140
Jun 8, 2020 21:19:15.623001099 CEST	49735	443	192.168.2.5	192.185.166.140

## UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 8, 2020 21:19:12.247829914 CEST	62823	53	192.168.2.5	8.8.8.8
Jun 8, 2020 21:19:12.282069921 CEST	53	62823	8.8.8.8	192.168.2.5
Jun 8, 2020 21:19:13.345737934 CEST	64058	53	192.168.2.5	8.8.8.8
Jun 8, 2020 21:19:13.480236053 CEST	53	64058	8.8.8.8	192.168.2.5
Jun 8, 2020 21:19:13.827393055 CEST	59700	53	192.168.2.5	8.8.8.8
Jun 8, 2020 21:19:14.095262051 CEST	53	59700	8.8.8.8	192.168.2.5
Jun 8, 2020 21:19:15.626532078 CEST	54977	53	192.168.2.5	8.8.8.8
Jun 8, 2020 21:19:15.667253971 CEST	53	54977	8.8.8.8	192.168.2.5
Jun 8, 2020 21:19:17.065924883 CEST	50690	53	192.168.2.5	8.8.8.8
Jun 8, 2020 21:19:17.107136011 CEST	53	50690	8.8.8.8	192.168.2.5
Jun 8, 2020 21:19:17.114025116 CEST	63919	53	192.168.2.5	8.8.8.8
Jun 8, 2020 21:19:17.147047043 CEST	53	63919	8.8.8.8	192.168.2.5
Jun 8, 2020 21:19:17.620415926 CEST	52477	53	192.168.2.5	8.8.8.8
Jun 8, 2020 21:19:17.653470993 CEST	53	52477	8.8.8.8	192.168.2.5
Jun 8, 2020 21:19:42.250663042 CEST	64633	53	192.168.2.5	8.8.8.8
Jun 8, 2020 21:19:42.275289059 CEST	53	64633	8.8.8.8	192.168.2.5
Jun 8, 2020 21:19:42.822329998 CEST	51961	53	192.168.2.5	8.8.8.8
Jun 8, 2020 21:19:42.846921921 CEST	53	51961	8.8.8.8	192.168.2.5
Jun 8, 2020 21:19:43.260397911 CEST	64633	53	192.168.2.5	8.8.8.8
Jun 8, 2020 21:19:43.285043001 CEST	53	64633	8.8.8.8	192.168.2.5
Jun 8, 2020 21:19:43.830677032 CEST	51961	53	192.168.2.5	8.8.8.8
Jun 8, 2020 21:19:43.855408907 CEST	53	51961	8.8.8.8	192.168.2.5
Jun 8, 2020 21:19:44.304944992 CEST	64633	53	192.168.2.5	8.8.8.8
Jun 8, 2020 21:19:44.329566002 CEST	53	64633	8.8.8.8	192.168.2.5
Jun 8, 2020 21:19:45.858486891 CEST	51961	53	192.168.2.5	8.8.8.8
Jun 8, 2020 21:19:45.883140087 CEST	53	51961	8.8.8.8	192.168.2.5
Jun 8, 2020 21:19:46.511946917 CEST	64633	53	192.168.2.5	8.8.8.8
Jun 8, 2020 21:19:46.536573887 CEST	53	64633	8.8.8.8	192.168.2.5
Jun 8, 2020 21:19:47.878412962 CEST	51961	53	192.168.2.5	8.8.8.8
Jun 8, 2020 21:19:47.902951956 CEST	53	51961	8.8.8.8	192.168.2.5
Jun 8, 2020 21:19:50.989965916 CEST	64633	53	192.168.2.5	8.8.8.8
Jun 8, 2020 21:19:51.023155928 CEST	53	64633	8.8.8.8	192.168.2.5
Jun 8, 2020 21:19:51.897193909 CEST	51961	53	192.168.2.5	8.8.8.8
Jun 8, 2020 21:19:51.922046900 CEST	53	51961	8.8.8.8	192.168.2.5
Jun 8, 2020 21:20:03.939516068 CEST	57922	53	192.168.2.5	8.8.8.8
Jun 8, 2020 21:20:03.972672939 CEST	53	57922	8.8.8.8	192.168.2.5
Jun 8, 2020 21:20:48.845408916 CEST	51411	53	192.168.2.5	8.8.8.8
Jun 8, 2020 21:20:48.880430937 CEST	53	51411	8.8.8.8	192.168.2.5

## DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 8, 2020 21:19:13.345737934 CEST	192.168.2.5	8.8.8.8	0xf089	Standard query (0)	url7220.ca apvisio.com	A (IP address)	IN (0x0001)
Jun 8, 2020 21:19:13.827393055 CEST	192.168.2.5	8.8.8.8	0x4700	Standard query (0)	campbaker.org	A (IP address)	IN (0x0001)
Jun 8, 2020 21:20:03.939516068 CEST	192.168.2.5	8.8.8.8	0xb622	Standard query (0)	campbaker.org	A (IP address)	IN (0x0001)



DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 8, 2020 21:19:13.480236053 CEST	8.8.8.8	192.168.2.5	0xf089	No error (0)	url7220.ca apvisio.com	sendgrid.net		CNAME (Canonical name)	IN (0x0001)
Jun 8, 2020 21:19:13.480236053 CEST	8.8.8.8	192.168.2.5	0xf089	No error (0)	sendgrid.net		167.89.118.52	A (IP address)	IN (0x0001)
Jun 8, 2020 21:19:13.480236053 CEST	8.8.8.8	192.168.2.5	0xf089	No error (0)	sendgrid.net		167.89.123.54	A (IP address)	IN (0x0001)
Jun 8, 2020 21:19:14.095262051 CEST	8.8.8.8	192.168.2.5	0x4700	No error (0)	campbaker.org		192.185.166.140	A (IP address)	IN (0x0001)
Jun 8, 2020 21:20:03.972672939 CEST	8.8.8.8	192.168.2.5	0xb622	No error (0)	campbaker.org		192.185.166.140	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- url7220.caapvisio.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49732	167.89.118.52	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jun 8, 2020 21:19:13.654131889 CEST	2	OUT	GET /ls/click?upn=U5wBbtTMlgqzyFeoDeLr9oYI88rjnJDKdB-2FOqe4mjsPWQeP8r8RzDIgeUom6oe-2FaiU7o_DC4y3DdDCeEScwRgaDHqvVGy56gjlVzN-2FR6WAJbPzoIndJWWMS5Nkfg9TStdNBwzzNXg19pf8z0ZDZc9DdeYbjXBEzOUQDti5Y6qNaHhwy8a1GmmWUfNIKQdV5jNijS-2FPYjImppGgMnCoKDnCFRzE-2BtlPuEuW9HL8vR8Wt5eD4RcdD-2FKL22gop-2FvXlzeVJxcDVXnSCieFHQtG0L7OWAFTFIEIOVBANnwHDrwyLzxVtqL2xBsu9e2Yuuq6z29wQB7-2FyidJCIzLUne1Rn4dgtbj2S9qSfe47d18pWh0akhpla0oEiNBwjG-2FEerblB3yotE-2B0rDgEyV1dN7xqp6lWS4wNe2SjpCq-2Bd3KysdMWKgt9-2Fyx-2Foz6kqZij-2FhoFvYJVLNlXpuCIS14ETkrvFVaSdzrl-2FAFD4CJ0lpN8haTyAlyfzLLUDNibK2-2FKRqq0VKbmPlaVSI5idyFxaDOg-2FDb8pZjZJ6FP17mdPcFXzud7tUBE0fW1sqj-2BDKXgTJ-2FOp2an5z6KllwnX6tNwnVLzn5RuoJAJmDlmua1AtTqdjip0hnCSda-2FxsdlNP0qciBTe99zuZZYqSuju2N0uix-2BiYqvDE7-2B0K0wIbHmZ38a-2BFoXgFH9dWpjZqmaF3RH2OQ-2FgS9WsoMHejqz88SBj0zdDjKSE2ve6qo0veAzLH3FJZZ2OTnVmvXVTWOnTxVMCuDNo0gTLg9c45S1XgyV4CrH8AZF7EpWJOXWrZ9Cg9pggyJJg5JsPeiqx93R4KOglRsu6RLWPejivN4KUBwpagxkwoo3fyVu9GcSgJCUnNq9-2BTHkpNEnAQFWWiFbiMXHPUwOXqBoNH9gEhqsf-2FNHoPURLLGoeaBgxQhPYP7ALCwTbW96GnOGSqZnKLcZo-2FIt2D-2B1qWVvm1l392O1TAT2xXs7f173Pd6lP0xclYuMXEjSwascmy5p6x6Aa7iw3NUDri7YFO HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: url7220.caapvisio.com Connection: Keep-Alive
Jun 8, 2020 21:19:13.815409899 CEST	2	IN	HTTP/1.1 302 Found Server: nginx Date: Mon, 08 Jun 2020 19:19:13 GMT Content-Type: text/html; charset=utf-8 Content-Length: 56 Connection: keep-alive Location: https://campbaker.org/OFFICE3655/ X-Robots-Tag: noindex, nofollow Data Raw: 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 63 61 6d 70 62 61 6b 65 72 2e 6f 72 67 2f 4f 46 46 49 43 45 33 36 35 35 2f 22 3e 46 6f 75 6e 64 3c 2f 61 3e 2e 0a 0a Data Ascii: <a href="https://campbaker.org/OFFICE3655/">Found</a>.

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 8, 2020 21:19:14.380013943 CEST	192.185.166.140	443	192.168.2.5	49735	CN=autodiscover.campbaker.org CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu May 07 20:02:46 CEST 2020	Wed Aug 05 20:02:46 CEST 2020	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=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 17 17:40:46 CET 2016	Wed Mar 17 17:40:46 CET 2021		
Jun 8, 2020 21:19:14.383075953 CEST	192.185.166.140	443	192.168.2.5	49734	CN=autodiscover.campbaker.org CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu May 07 20:02:46 CEST 2020	Wed Aug 05 20:02:46 CEST 2020	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=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 17 17:40:46 CET 2016	Wed Mar 17 17:40:46 CET 2021		
Jun 8, 2020 21:20:04.257203102 CEST	192.185.166.140	443	192.168.2.5	49748	CN=autodiscover.campbaker.org CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu May 07 20:02:46 CEST 2020	Wed Aug 05 20:02:46 CEST 2020	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 17 17:40:46 CET 2016	Wed Mar 17 17:40:46 CET 2021		

Code Manipulations

Statistics

Behavior

● iexplore.exe  
● iexplore.exe

 Click to jump to process

System Behavior

## Analysis Process: iexplore.exe PID: 5436 Parent PID: 700

### General

Start time:	21:19:11
Start date:	08/06/2020
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff6d5300000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

### File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
-----------	--------	------------	---------	------------	-------	----------------	--------

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
-----------	--------	--------	-------	-------	------------	-------	----------------	--------

File Path	Offset	Length	Completion	Count	Source Address	Symbol
-----------	--------	--------	------------	-------	----------------	--------

### Registry Activities

Key Path	Completion	Count	Source Address	Symbol
----------	------------	-------	----------------	--------

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
----------	------	------	------	------------	-------	----------------	--------

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

## Analysis Process: iexplore.exe PID: 5580 Parent PID: 5436

### General

Start time:	21:19:12
Start date:	08/06/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5436 CREDAT:17410 /prefetch:2
Imagebase:	0x1260000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEEA8013E2AB58D5A
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

### File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
-----------	--------	------------	---------	------------	-------	----------------	--------

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
-----------	--------	--------	-------	-------	------------	-------	----------------	--------

File Path	Offset	Length	Completion	Count	Source Address	Symbol
-----------	--------	--------	------------	-------	----------------	--------

Registry Activities

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

Disassembly