

# Compromised?

**Scenario:** You work for Pledge Insurance on the security team. You have been told by multiple employees and customers that the website seems to be running slow. The system administrators tell you that they do not see the website showing any performance issues. You have been tasked with investigating if the performance issues the users are experiencing are security related.

**Goal:** Identify cases of users complaining of slow activity and weird behavior with their insurance website.

**Objective 1:** Is the website compromised? If so, how and why?

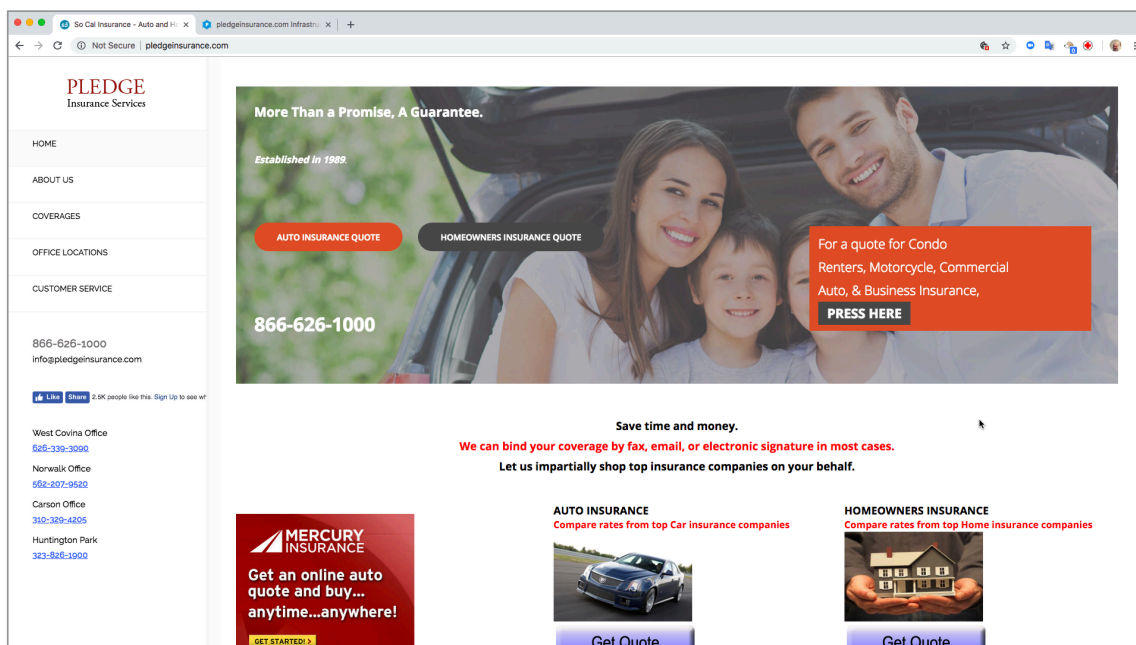
**Objective 2:** Are there any other websites that may exhibit the same behavior?

**Objective 3:** What does the infrastructure look like and does it appear malicious?

## STEP 1: Pledge Insurance website

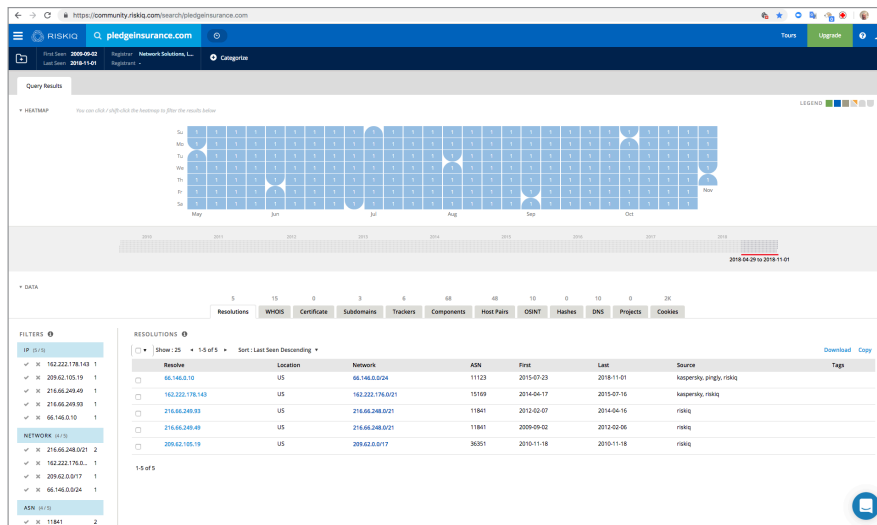
Open a browser and go to [pledgeinsurance.com](http://pledgeinsurance.com)

[So Cal Insurance - Auto and Home Insurance in Los Angeles, West Covina, Carson, Huntington Park, Norwalk and Garden Grove](#)



You see your organization's website and everything appears to be normal.





Pledge insurance has had five different IP addresses since 2009 — all have been in the US.

In order to determine if the website has been compromised, we will have to examine the advanced crawled data sets. These are dynamic data sets that are created when RiskIQ's virtual user interact with the websites. The crawl data sets we will be looking at are tracker, components, and host pairs.

### Step 3: Components

Click on the Components tab and review the components that are listed to see if there is anything unusual.

Component	Version	First	Last	Source	Tags
jQuery	(v1.11.2)	2018-07-31	2018-10-08	jQuery	
PHP	(v5.6.22)	2016-06-29	2018-10-07	PHP	
FreeBSD		2015-12-01	2018-10-07	FreeBSD	
Joomla!	(v1.7.3)	2016-07-29	2018-10-06	Joomla!	
Facebook		2015-12-01	2018-10-06	Facebook	
Joomla!	(v1.7.3)	2015-12-01	2018-09-23	Joomla!	
Joomla!	(v3.4)	2017-10-08	2018-08-14	Joomla!	
Google Ads - DoubleClick		2016-06-29	2018-04-30	Google Ads - DoubleClick	
YouTube CDN		2015-12-01	2018-04-30	YouTube CDN	
YouTube		2015-12-01	2018-04-30	YouTube	
jQuery		2015-12-01	2018-04-30	jQuery	
Coin Hive		2017-10-08	2018-01-09	Coin Hive	
Twitter.js (v1.4)		2017-02-23	2018-01-09	Twitter.js (v1.4)	
Google Tag Manager		2017-12-23	2018-01-09	Google Tag Manager	
Google Analytics		2014-06-17	2018-01-09	Google Analytics	
Google Analytics		2017-12-23	2017-12-23	Google Analytics	
Google Ads		2017-12-23	2017-12-23	Google Ads	
Google Search		2015-12-01	2017-11-12	Google Search	
Google Ads - DoubleClick		2016-06-29	2017-07-10	Google Ads - DoubleClick	

The components that tend to be compromised will be PHP, CMS (like Joomla!), Word Press, and Drupal.

Domain	First Seen	Last Seen	Category	Service
www.pledgeinsurance.com	2015-12-01	2018-10-06	Tracking Pixel	Facebook
www.pledgeinsurance.com	2015-12-01	2018-09-23	CMG	Joomla! (v1.7.3)
www.pledgeinsurance.com	2017-10-08	2018-08-14	CMG	Joomla! (v3.4)
www.pledgeinsurance.com	2016-06-29	2018-04-30	Ad Exchange	Google Ads - DoubleClick
www.pledgeinsurance.com	2015-12-01	2018-04-30	CDN	YouTube CDN
www.pledgeinsurance.com	2015-12-01	2018-04-30	Online Videos	YouTube
www.pledgeinsurance.com	2015-12-01	2018-04-30	JavaScript Library	jQuery
www.pledgeinsurance.com	2017-10-08	2018-01-09	Cryptocurrency Miner	Coin Hive
www.pledgeinsurance.com	2017-02-23	2018-01-09	JavaScript Library	twilio.js (vNA)
www.pledgeinsurance.com	2017-12-23	2018-01-09	Analytics Service	Google Tag Manager
www.pledgeinsurance.com	2014-06-17	2018-01-09	Analytics Service	Google Analytics
www.pledgeinsurance.com	2017-12-23	2017-12-23	Tracking Pixel	Google Analytics
www.pledgeinsurance.com	2017-12-23	2017-12-23	Ad Exchange	Google Ads
www.pledgeinsurance.com	2015-12-01	2017-11-12	Search	Google Search
pledgeinsurance.com	2016-06-23	2017-07-10	Ad Exchange	Google Ads - DoubleClick
pledgeinsurance.com	2016-03-17	2017-07-10	Online Videos	YouTube
pledgeinsurance.com	2016-03-17	2017-07-10	Search	Google Search
pledgeinsurance.com	2016-03-17	2017-07-10	CDN	YouTube CDN
pledgeinsurance.com	2017-02-25	2017-07-10	JavaScript Library	twilio.js (vNA)

Here we see Coinhive, and RiskIQ has labeled it as a cryptocurrency miner.

## Step 4: Research what is coinhive

Now open a new tab and search for Coinhive.

[coinhive - Google Search](#)

Google search results for 'coinhive'.

**Coinhive - Monero Mining Club**  
<https://coinhive.com/> • Coinhive offers a JavaScript miner for the Monero Blockchain (Digi Money) that you can embed in your website. You users run the miner directly on their ...  
 Coinhive - JavaScript Miner - Blog - Documentation

**Who and What is Coinhive? — Krebs on Security**  
<https://krebsonsecurity.com/2018/03/who-and-what-is-coinhive/> • May 26, 2018 - Malware security firm recently identified cryptocurrency mining service Coinhive as the top malicious threat to Web users, thanks to the ...

**Top stories**

- Brazil Tops List of Cryptjacking Coinhive Victims, Iranian Cybersecurity Authority Warns**  
 Contingent - 4 hours ago
- Coinhive Monero Crypto Jacking Epidemic Hits Iran Hard**  
 Financial Tribune - 10 hours ago
- Coinhive Monero Crypto Mining Epidemic Hits 30 Thousand Routers Pan India**  
 Contingent - 4 days ago

[More for coinhive](#)

**Why is Malwarebytes blocking Coinhive? - Malwarebytes Labs**  
<https://blog.malwarebytes.com/security/why-is-malwarebytes-blocking-coinhive/> • Oct 18, 2017 - Malwarebytes security started blocking Coin Hive, the creators of a scripting based crypto miner that runs on user systems while they visit a ...

**Making money mining Coinhive? Yeah, you and nine other people**  
[https://www.theringer.co.uk/2018/08/15/coinhive\\_mining\\_money/](https://www.theringer.co.uk/2018/08/15/coinhive_mining_money/) • Aug 15, 2018 - Mining internet currency on websites with Coinhive scripts is a lucrative endeavor, but only for a handful of people. The according to ...

We see Coinhive is part of the Monero Mining Club. The second link is from Krebs on Security, a popular reputable security site.

Click on Who and What is Coinhive? — Krebs on Security

[Who and What Is Coinhive? — Krebs on Security](#)



“Multiple security firms recently identified cryptocurrency mining service Coinhive as the top malicious threat to Web users, thanks to the tendency for Coinhive’s computer code to be used on hacked Websites to steal the processing power of its visitors’ devices.”

This would explain why user to the website experience slowness.

---

**Objective 1 completed:** Is the website compromised? If so, how and why?

Now we have that we have determined that the Pledge Insurance website was compromised with Coinhive, a cryptocurrency mining service that steals the processing power of its visitors’ devices. This matches complaints from customers and employees you were told.

Since the Coinhive is a client-side application and does not run from the server this would also matches the system administrators observations that no performance issues were observed on the servers for Pledge Insurance.

We can now explain that [pledgeinsurance.com](https://pledgeinsurance.com) was compromised by a threat actor or group and installed coinhive on the server. But is this an isolated compromise or part of a larger attack? To find out, we need to investigate the other advanced data sets, Trackers, and Host Pairs.

---

## Step 5: Trackers

The screenshot shows the RiskIQ interface with search results for trackers on the domain pledgedinsurance.com. The 'CoinHiveSiteKey' is highlighted in the table.

Hostname	First	Last	Type	Value	Tags
www.pledgedinsurance.com	2017-12-23	2018-01-09	CoinHiveSiteKey	cnpuhgprubjwuijpwznq3mtjgwjndi	
www.pledgedinsurance.com	2017-12-23	2018-01-09	GoogleTagManagerId	gtm-pdd2zh	
pledgedinsurance.com	2014-07-18	2014-07-18	GoogleAnalyticsAccountNumber	ua-20774683	
pledgedinsurance.com	2014-07-18	2014-07-18	GoogleAnalyticsTrackingId	ua-20774683-1	
www.pledgedinsurance.com	2014-06-17	2014-06-17	GoogleAnalyticsAccountNumber	ua-20774683	
www.pledgedinsurance.com	2014-06-17	2014-06-17	GoogleAnalyticsTrackingId	ua-20774683-1	

RiskIQ identified the CoinHiveSiteKey associated with this particular instance running on pledgedinsurance.com.

Every coinhive instance uses a unique site key in order to allow the mined coins to be collected. That means that the key that was identified belongs to the threat actor or group who compromised the Pledge Insurance website.

If you pivot search on the CoinHiveSiteKey, it will identify all coinhive instances in the world that is using the same site key which would belong to the same threat actor or group.

Right click on the CoinHiveSiteKey value and open it in a new tab

The screenshot shows a right-click context menu over the CoinHiveSiteKey value. The menu options include:

- Open Link in New Tab
- Open Link in New Window
- Open Link in Incognito Window
- Save Link As...
- Copy Link Address
- Copy
- Search Google for "cnpuhgprubjwuijpwznq3mtjgwjndi"
- Print...
- Blockade
- FatBeagle
- Google Translate
- Inspect
- Speech
- Services

Tracker Search: Hosts

Tracker Search: IP Addresses

DATA

FILTERS

HOSTNAME (9/9)

- ✓ www-center.org 1
- ✓ mastercardco... 1
- ✓ www-center... 1
- ✓ www.broadip... 1
- ✓ www.conafiva... 1

SHOW MORE

TAG

SYSTEM TAG

TRACKER SEARCH

Show: 25 1-9 of 9 Sort: Last Seen Descending Total Records: 9

Hostname	First Seen	Last Seen	Tags
www.conafivas.com	2018-04-05	2018-09-28	
www.dvcc.it	2018-04-04	2018-08-30	
www-center.org	2018-05-06	2018-08-13	
www.cooperativatubajb.hn	2018-07-28	2018-07-28	
www.renovacaoesantimica.com.br	2018-07-09	2018-07-09	
www.broadiplock.com	2017-12-26	2018-04-22	
www-center.org	2018-03-22	2018-03-22	
mastercardconcerge-globalairportconcerge.com	2018-03-03	2018-03-03	
www.pledgeinsurance.com	2017-12-23	2018-01-09	

1-9 of 9

Download Copy

4.0.0-98d29d © 2018, RiskIQ Inc. All Rights Reserved. Proprietary and confidential, do not distribute without prior approval. Privacy Policy Terms and Conditions

[Tracker Search for cnpufgprubjwuijpwznq3mtjtgwujndi \(CoinHiveSiteKey\) | RiskIQ Community Edition](#)

We see 9 entries associated with this same CoinHiveSiteKey. That means that the same threat actor or group also has coinhive instances running on these websites.

**Objective 2 Completed:** Are there any other websites that may exhibit the same behavior?

We have now found a total of 9 websites that all have coinhive running on them with the same CoinHiveSiteKey. The next step will be to determine if the threat actor compromised a single server with multiple website instances or 9 different domains.

On the same page, click on the Tracker Search: IP Addresses tab.

Tracker Search: Hosts

Tracker Search: IP Addresses

DATA

FILTERS

HOSTNAME (8/8)

- ✓ 181.189.235.2 1
- ✓ 184.107.167.170 1
- ✓ 200.31.14.89 1
- ✓ 209.43.112.33 1
- ✓ 222.165.133.145 1

SHOW MORE

TAG

SYSTEM TAG

TRACKER SEARCH

Show: 25 1-8 of 8 Sort: Last Seen Descending Total Records: 8

Hostname	First Seen	Last Seen	Tags
200.31.14.89	2018-04-05	2018-10-09	
222.165.133.145	2018-04-04	2018-10-08	
88.107.229.16	2018-03-22	2018-08-13	
181.189.235.2	2018-07-28	2018-07-28	
184.107.167.170	2018-07-09	2018-07-09	
209.43.112.33	2017-12-26	2018-04-22	
40.127.167.95	2018-03-03	2018-03-03	
66.146.0.10	2017-12-23	2018-01-09	

1-8 of 8

Download Copy

4.0.0-98d29d © 2018, RiskIQ Inc. All Rights Reserved. Proprietary and confidential, do not distribute without prior approval. Privacy Policy Terms and Conditions

We can determine that all of the website are not on the same IP address. It appears that the websites might have been compromised the same way as pledgeinsurance.com, most likely by compromising the same web components to gain access and install Coinhive.

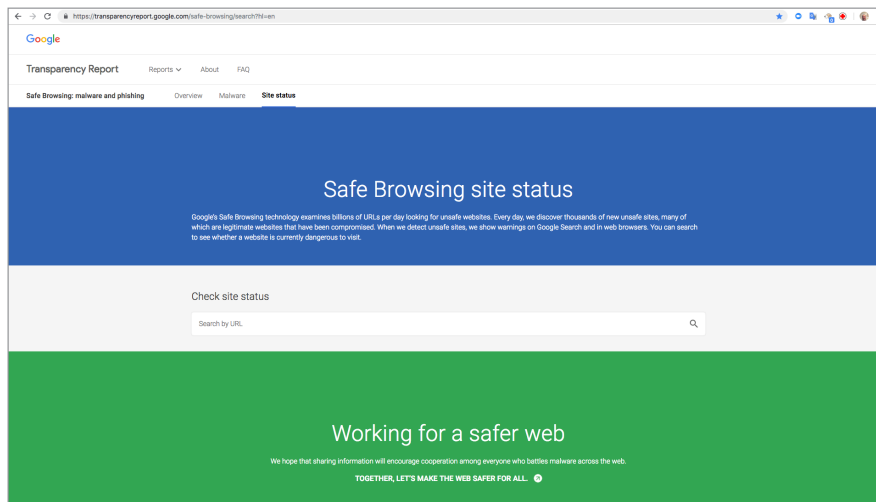
There is a chance that one of the websites listed under the Tracker Search: Hosts might be a test instance for the threat actor. We will need to investigate each entry and determine if the site was legitimate or belonging to the threat actor or group. During the investigation, try and determine if the website has similar components to pledgeinsurance.com.

## Step 6: How to check if a website is bad without visiting the site.

One way to determine if a website is malicious is to check it against the google safe browsing list.

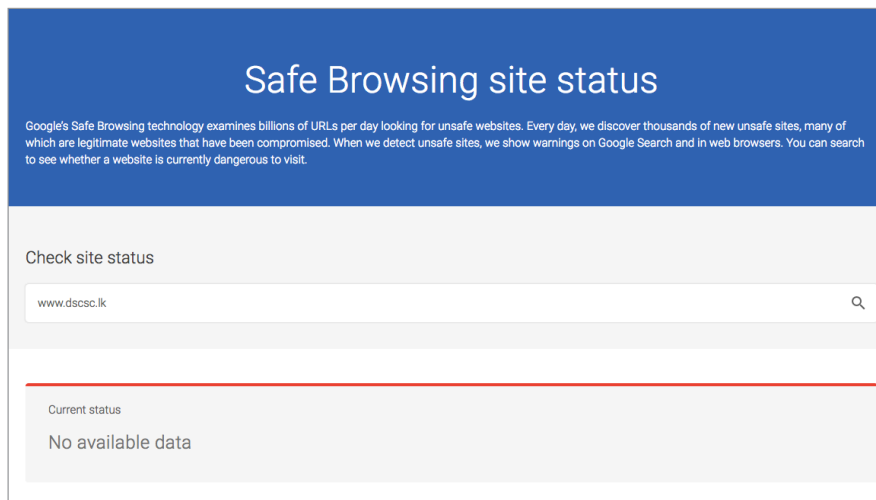
Open a new tab and search for Google safe browsing check and click on the entry “Safe Browsing: malware and phishing – Google Transparency Report.”

[Safe Browsing: malware and phishing – Google Transparency Report](https://transparencyreport.google.com/safe-browsing/search?hl=en)



Now copy and paste each domain name into the check site status and press the return key on your keyboard.

Check [www.dscsc.lk](http://www.dscsc.lk)



[www.dscsc.lk](http://www.dscsc.lk) is Not malicious.



Check [www.conalvias.com](http://www.conalvias.com)

### Safe Browsing site status

Google's Safe Browsing technology examines billions of URLs per day looking for unsafe websites. Every day, we discover thousands of new unsafe sites, many of which are legitimate websites that have been compromised. When we detect unsafe sites, we show warnings on Google Search and in web browsers. You can search to see whether a website is currently dangerous to visit.

Check site status

Q

Current status

No available data

Check [www.awer-center.org](http://www.awer-center.org), this domain appears twice in the list.

### Safe Browsing site status

Google's Safe Browsing technology examines billions of URLs per day looking for unsafe websites. Every day, we discover thousands of new unsafe sites, many of which are legitimate websites that have been compromised. When we detect unsafe sites, we show warnings on Google Search and in web browsers. You can search to see whether a website is currently dangerous to visit.

Check site status

Q

Current status

No available data

Check [www.cooperativataulabe.hn](http://www.cooperativataulabe.hn)

### Safe Browsing site status

Google's Safe Browsing technology examines billions of URLs per day looking for unsafe websites. Every day, we discover thousands of new unsafe sites, many of which are legitimate websites that have been compromised. When we detect unsafe sites, we show warnings on Google Search and in web browsers. You can search to see whether a website is currently dangerous to visit.

Check site status

Q

Current status

No available data

Check [www.renovacaocarismatica.com.br](http://www.renovacaocarismatica.com.br)

### Safe Browsing site status

Google's Safe Browsing technology examines billions of URLs per day looking for unsafe websites. Every day, we discover thousands of new unsafe sites, many of which are legitimate websites that have been compromised. When we detect unsafe sites, we show warnings on Google Search and in web browsers. You can search to see whether a website is currently dangerous to visit.

Check site status

Q

Current status

No available data

Check [www.broadripplelock.com](http://www.broadripplelock.com)

### Safe Browsing site status

Google's Safe Browsing technology examines billions of URLs per day looking for unsafe websites. Every day, we discover thousands of new unsafe sites, many of which are legitimate websites that have been compromised. When we detect unsafe sites, we show warnings on Google Search and in web browsers. You can search to see whether a website is currently dangerous to visit.

Check site status

Q

Current status

No available data

Check [mastercardconcierge.globalairportconcierge.com](http://mastercardconcierge.globalairportconcierge.com)

### Safe Browsing site status

Google's Safe Browsing technology examines billions of URLs per day looking for unsafe websites. Every day, we discover thousands of new unsafe sites, many of which are legitimate websites that have been compromised. When we detect unsafe sites, we show warnings on Google Search and in web browsers. You can search to see whether a website is currently dangerous to visit.

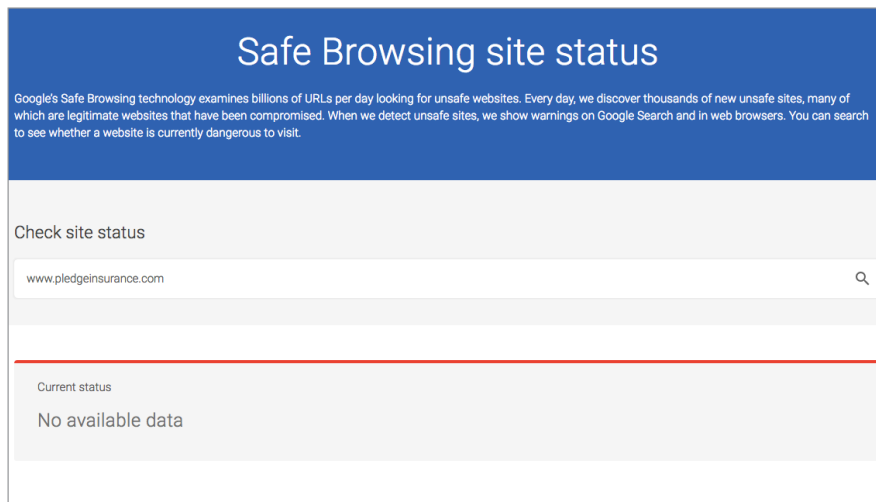
Check site status

Q

Current status

No available data

Check [www.pledgeinsurance.com](http://www.pledgeinsurance.com)



Now we have determined that Google has not seen any malicious or suspicious activity on any of the domains. All of the domains are legitimate so now we will need to use PassiveTotal® to examine each domain to see why they were also compromised.

## Step 7: Review the components tab for CoinHiveSiteKey domains

Open [www.dscsc.lk](http://www.dscsc.lk) in another tab and click on the components tab.  
[www.dscsc.lk](http://www.dscsc.lk) Infrastructure Results | RiskIQ Community Edition

**COMPONENTS**

Hostname	First	Last	Category	Value	Tags
www.dscsc.lk	2018-03-20	2018-10-31	Server	Apache	
www.dscsc.lk	2018-04-04	2018-10-31	Cryptocurrency Miner	Coinhive	
www.dscsc.lk	2018-03-20	2018-10-31	JavaScript Library	jQuery 1.8	
www.dscsc.lk	2018-03-20	2018-10-31	Framework	PHP (v5.3.3)	
www.dscsc.lk	2018-01-20	2018-10-31	JavaScript Library	jQuery	
www.dscsc.lk	2018-04-04	2018-10-31	JavaScript Library	jQuery Migrate	
www.dscsc.lk	2018-04-04	2018-04-04	JavaScript Library	jQuery Migrate	
www.dscsc.lk	2017-01-20	2017-03-21	JavaScript Library	jQuery (v1.9.1)	
www.dscsc.lk	2017-01-20	2017-03-21	CDN	jQuery CDN	
www.dscsc.lk	2017-01-20	2017-03-21	Web Design	giphy.com	
www.dscsc.lk	2018-03-20	2017-01-11	JavaScript Library	jQuery (v1.7.2)	
www.dscsc.lk	2013-01-08	2013-01-29	Server Module	mod_authenldap (v1.4)	
www.dscsc.lk	2013-01-08	2013-01-29	Operating System	Linux	
www.dscsc.lk	2013-01-08	2013-01-29	Server Module	mod_ssl (v2.2.28)	
www.dscsc.lk	2013-01-08	2013-01-29	Server	Apache (v2.2.28)	
www.dscsc.lk	2013-01-08	2013-01-29	Server Module	OpenSSL (v1.0.1-fips)	
www.dscsc.lk	2013-01-08	2013-01-29	Framework	PHP (v5.3.17)	
www.dscsc.lk	2013-01-20	2013-01-20	CMS	Joomla! (v1.5)	

PHP and Joomla, the same components as [pledgeinsurance.com](http://pledgeinsurance.com), are listed.

Open [www.conalvias.com](http://www.conalvias.com) in another tab and click on the components tab.  
[www.conalvias.com](http://www.conalvias.com) Infrastructure Results | RiskIQ Community Edition

Hostname	First	Last	Category	Value	Tags
www.conalvias.com	2015-02-27	2018-10-31	Operating System	Red Hat	
www.conalvias.com	2015-02-27	2018-10-31	Server	Apache (v2.2.15)	
www.conalvias.com	2015-02-27	2018-10-31	JavaScript Library	jQuery (v1.8.2)	
www.conalvias.com	2018-04-05	2018-10-31	Web Design	Font Awesome (v3.2.1)	
www.conalvias.com	2015-11-30	2018-10-31	Tracking Pixel	Google Analytics	
www.conalvias.com	2018-10-31	2018-10-31	JavaScript Library	jQuery (v1.8.2)	
www.conalvias.com	2017-03-12	2018-10-31	JavaScript Library	jQuery (v1.8.2)	
www.conalvias.com	2018-09-28	2018-10-31	JavaScript Library	jQuery (v1.8.2)	
www.conalvias.com	2015-02-27	2018-10-31	CDN	Google Apps CDN	
www.conalvias.com	2017-03-12	2018-10-31	Tracking Pixel	www.conalvias.com	
www.conalvias.com	2018-04-05	2018-10-31	CDN	Google Hosted Libraries	
www.conalvias.com	2015-03-27	2018-10-31	Ad Network	Google	
www.conalvias.com	2015-03-27	2018-10-31	CDN	Bootstrap CDN	
www.conalvias.com	2015-03-27	2018-10-31	Analytics Service	Google Analytics (Integrated)	
www.conalvias.com	2018-10-31	2018-10-31	Framework	PHP (v5.6.30)	
www.conalvias.com	2017-03-12	2018-10-31	JavaScript Library	jQuery (v1.8.2)	
www.conalvias.com	2015-02-27	2018-10-31	JavaScript Library	jQuery (v1.8.2)	
www.conalvias.com	2015-02-27	2018-10-31	Analytics Service	Google Analytics	
www.conalvias.com	2015-02-27	2018-10-31	Framework	PHP (v5.6.30)	
www.conalvias.com	2018-04-05	2018-10-31	JavaScript Library	Dean Edwards Packer	
www.conalvias.com	2018-04-05	2018-10-31	Cryptocurrency Miner	Coin Hive	
www.conalvias.com	2018-04-05	2018-10-31	JavaScript Library	jQuery	
www.conalvias.com	2018-04-05	2018-10-31	JavaScript Library	jQuery (v1.8.2)	
www.conalvias.com	2017-03-12	2018-10-31	CMS	Joomla (v1.7.3)	
www.conalvias.com	2015-02-27	2017-04-28	JavaScript Library	jQuery (v1.11.0)	

PHP and Joomla, the same components as pledgeinsurance.com, are listed.

Open [www.awer-center.org](http://www.awer-center.org) in another tab and click on the components tab.  
[www.awer-center.org](http://www.awer-center.org) Infrastructure Results | RiskIQ Community Edition

Hostname	First	Last	Category	Value	Tags
www.awer-center.org	2015-12-06	2018-10-31	Server	Apache (v2)	
www.awer-center.org	2018-05-06	2018-10-31	Framework	PHP (v5.3.29)	
www.awer-center.org	2018-08-10	2018-10-31	Search	Google Search	
www.awer-center.org	2018-06-03	2018-10-31	Social Network	Google+	
www.awer-center.org	2018-08-10	2018-10-31	Social Media	Twitter Widgets	
www.awer-center.org	2018-08-10	2018-10-31	Ad Exchange	Facebook	
www.awer-center.org	2018-06-03	2018-10-31	WordPress Plugin	T1 Countdown	
www.awer-center.org	2015-12-06	2018-10-31	Tracking Pixel	www.awer-center.org	
www.awer-center.org	2015-12-06	2018-10-31	JavaScript Library	jQuery	
www.awer-center.org	2018-07-02	2018-10-31	JavaScript Library	jQuery Migrate (v1.4.1)	
www.awer-center.org	2018-08-10	2018-10-31	Publisher	Publisher	
www.awer-center.org	2018-07-02	2018-10-31	CMS	WordPress (v4.5.3)	
www.awer-center.org	2018-06-03	2018-10-31	WordPress Plugin	Social Media Share Buttons &amp; Social Sharing Icons (Ultimate Sharing)	
www.awer-center.org	2018-08-10	2018-10-31	Publisher	Twitter Ads	
www.awer-center.org	2018-08-03	2018-10-31	CMS	WordPress (v4.5.1)	
www.awer-center.org	2018-06-03	2018-10-31	WordPress Plugin	Contact Form 7 (v4.4.2)	
www.awer-center.org	2017-08-31	2018-10-31	JavaScript Library	jQuery Migrate (v1.2.1)	
www.awer-center.org	2015-12-06	2018-10-07	CMS	WordPress (v3.9.1)	
www.awer-center.org	2018-03-15	2018-10-07	Tracking Pixel	Facebook Pixel	
www.awer-center.org	2018-05-06	2018-08-13	Web Design	Font Awesome (v4.1.0)	
www.awer-center.org	2018-05-06	2018-08-13	JavaScript Library	jQuery (v1.8.2)	
www.awer-center.org	2016-05-07	2018-08-13	Ad Network	Google	
www.awer-center.org	2018-05-06	2018-08-13	JavaScript Library	jQuery (v1.8.2)	
www.awer-center.org	2017-03-20	2018-08-13	CDN	YouTube CDN	
www.awer-center.org	2017-03-20	2018-08-13	JavaScript Library	jQuery (v1.11.1)	

Hostname	First	Last	Category	Value	Tags
www.awer-center.org	2018-05-06	2018-08-13	Cryptocurrency Miner	Coin Hive	
www.awer-center.org	2017-03-20	2018-08-13	Online Videos	YouTube	
www.awer-center.org	2017-03-20	2018-08-13	CDN	YouTube CDN	
www.awer-center.org	2017-03-20	2018-08-13	JavaScript Library	jQuery (v1.11.1)	
www.awer-center.org	2018-05-06	2018-08-13	JavaScript Library	jQuery (v1.11.1)	
www.awer-center.org	2017-06-01	2018-08-13	JavaScript Library	jQuery Migrate	
www.awer-center.org	2018-06-23	2018-08-12	Tracking Pixel	Twitter Ads	
www.awer-center.org	2018-08-03	2018-07-28	Tracking Pixel	Facebook	
www.awer-center.org	2017-03-20	2018-05-16	CMS	Joomla (v1.7.3)	
www.awer-center.org	2018-05-10	2018-05-16	CMS	Joomla (v3.2)	
www.awer-center.org	2017-03-20	2018-05-13	CMS	Joomla (v1.7.3)	
www.awer-center.org	2018-05-10	2018-05-10	JavaScript Library	jQuery Migrate (v1.2.1)	
www.awer-center.org	2018-05-10	2018-05-10	JavaScript Library	jQuery (v1.11.1)	
www.awer-center.org	2018-05-06	2018-05-08	JavaScript Library	jQuery (v1.8.2)	
www.awer-center.org	2017-03-20	2018-05-08	JavaScript Library	jQuery (v1.4.2)	
www.awer-center.org	2017-11-21	2017-11-21	CDN	Bootstrap CDN	
www.awer-center.org	2017-11-21	2017-11-21	Web Design	Font Awesome (v4.2.0)	
www.awer-center.org	2017-11-21	2017-11-21	Ad Exchange	Google Ads - DoubleClick	
www.awer-center.org	2015-12-06	2017-08-31	Framework	PHP (v5.3.10)	
www.awer-center.org	2015-12-06	2017-08-31	CMS	WordPress	
www.awer-center.org	2016-01-02	2016-11-18	Tracking Pixel	www.pagaadirect.com	
www.awer-center.org	2016-05-07	2016-05-07	Analytics Service	StatCounter	
www.awer-center.org	2016-05-07	2016-05-07	CMS	Blogger	

PHP and Joomla, the same components as pledgeinsurance.com, are listed.

Open [www.cooperativataulabe.hn](http://www.cooperativataulabe.hn) in another tab and click on the components tab.

[www.cooperativataulabe.hn](http://www.cooperativataulabe.hn) Infrastructure Results | RiskIQ Community Edition

2018-04-29 10:20:11-01

3 2 0 6 2 14 4 6 0 0 0 2

Resolutions WHOS Certificate Subdomains Trackers Components Host Pairs CDNT Hashes DNS Projects Cookies

**FILTERS**

**CATEGORY** (11/16)

- JavaScript Lib... 3
- Server Module 3
- CMS 2
- Ad Network 1
- Analytics Serv... 1

**VALUE** (21/16)

- CentOS 2
- Joomla! 2
- jQuery 2
- PHP 2
- Apache 1

**HOSTNAME** (1/14)

- www.cooper... 14

**TAG**

**SYSTEM TAG**

**COMPONENTS**

Show 25 • 1/14 of 14 • Sort: Last Seen Descending

Hostname	First	Last	Category	Value	Tags
www.cooperativataulabe.hn	2017-02-22	2018-10-31	Server Module	PHP (v5.4.16)	
www.cooperativataulabe.hn	2018-09-05	2018-10-31	Server Module	mod_auth (v2.3.9)	
www.cooperativataulabe.hn	2017-02-22	2018-10-31	Server	Apache (v2.4.6)	
www.cooperativataulabe.hn	2018-09-05	2018-10-31	Server Module	OpenSSL (v1.0.2h-fips)	
www.cooperativataulabe.hn	2017-02-22	2018-10-31	Operating System	CentOS	
www.cooperativataulabe.hn	2018-09-05	2018-10-31	JavaScript Library	jQuery (v3.3.1.slim)	
www.cooperativataulabe.hn	2017-02-22	2018-10-31	Framework	PHP (v5.4.16)	
www.cooperativataulabe.hn	2017-02-22	2018-10-31	JavaScript Library	jQuery	
www.cooperativataulabe.hn	2017-02-22	2018-07-28	CMS	Joomla! (v1.7.2)	
www.cooperativataulabe.hn	2018-07-28	2018-07-28	Cryptocurrency Miner	Coin-How	
www.cooperativataulabe.hn	2017-02-22	2018-07-28	Ad Network	Google	
www.cooperativataulabe.hn	2018-07-28	2018-07-28	JavaScript Library	jQuery (v3.3.1)	
www.cooperativataulabe.hn	2017-02-22	2017-04-27	CMS	Joomla! (v1.7)	
www.cooperativataulabe.hn	2017-02-22	2017-09-29	Analytics Service	Google	

1-14 of 14

PHP and Joomla, the same components as pledgeinsurance.com, are listed.

Open [www.renovacaocarismatica.com.br](http://www.renovacaocarismatica.com.br) in another tab and click on the components tab.

[www.renovacaocarismatica.com.br](http://www.renovacaocarismatica.com.br) Infrastructure Results | RiskIQ Community Edition

2018-04-29 10:20:11-01

2 3 6 4 2 20 5 8 0 9 0 3

Resolutions WHOS Certificate Subdomains Trackers Components Host Pairs CDNT Hashes DNS Projects Cookies

**FILTERS**

**CATEGORY** (11/20)

- Server Module 5
- CMS 2
- JavaScript Lib... 2
- Script 2
- Ad Exchange 1

**VALUE** (18/20)

- Apache 2
- Joomla! 2
- Coin-How 1
- Font Awesome 1
- FontPage 1

**HOSTNAME** (1/20)

- www.renova... 20

**TAG**

**SYSTEM TAG**

**COMPONENTS**

Show 25 • 1/20 of 20 • Sort: Last Seen Descending

Hostname	First	Last	Category	Value	Tags
www.renovacaocarismatica.com.br	2016-06-14	2018-10-31	Server	Apache	
www.renovacaocarismatica.com.br	2018-07-09	2018-10-10	Framework	PHP (v5.3.29)	
www.renovacaocarismatica.com.br	2018-10-08	2018-10-10	CMS	Joomla! (v3.8)	
www.renovacaocarismatica.com.br	2018-07-09	2018-10-10	Ad Network	Google	
www.renovacaocarismatica.com.br	2018-07-09	2018-10-10	JavaScript Library	jQuery	
www.renovacaocarismatica.com.br	2018-07-09	2018-07-09	Online Videos	YouTube	
www.renovacaocarismatica.com.br	2018-07-09	2018-07-09	JavaScript Library	jQuery (v3.3.1)	
www.renovacaocarismatica.com.br	2018-07-09	2018-07-09	CMS	Joomla! (v1.7.3)	
www.renovacaocarismatica.com.br	2018-07-09	2018-07-09	CDN	YouTube CDN	
www.renovacaocarismatica.com.br	2018-07-09	2018-07-09	Search	Google Search	
www.renovacaocarismatica.com.br	2018-07-09	2018-07-09	Cryptocurrency Miner	Coin-How	
www.renovacaocarismatica.com.br	2018-07-09	2018-07-09	Web Design	Font Awesome (v4.3.0)	
www.renovacaocarismatica.com.br	2018-07-09	2018-07-09	Ad Exchange	Google Ads - DoubleClick	
www.renovacaocarismatica.com.br	2012-08-07	2012-08-07	Server Module	mod_auth (v2.3.22)	
www.renovacaocarismatica.com.br	2012-08-07	2012-08-07	Operating System	Ubuntu	
www.renovacaocarismatica.com.br	2012-08-07	2012-08-07	Server Module	mod_auth_passthrough (v2.1)	
www.renovacaocarismatica.com.br	2012-08-07	2012-08-07	Server Module	FontPage (v4.0.2.2835)	
www.renovacaocarismatica.com.br	2012-08-07	2012-08-07	Server Module	mod_auth (v2.3.22)	
www.renovacaocarismatica.com.br	2012-08-07	2012-08-07	Server Module	OpenSSL (v1.0.1g-fips)	
www.renovacaocarismatica.com.br	2012-08-07	2012-08-07	Server	Apache (v2.2.22)	

1-20 of 20

PHP and Joomla, the same components as pledgeinsurance.com, are listed.

Open [www.broadripplelock.com](http://www.broadripplelock.com) in another tab and click on the components tab.

[www.broadripplelock.com](http://www.broadripplelock.com) Infrastructure Results | RiskIQ Community Edition

Hostname	First	Last	Category	Value	Tags
www.broadripplack.com	2018-04-22	2018-10-31	Content Management	Pluck	
www.broadripplack.com	2016-10-12	2018-10-31	Server	Apache (v2.2.3)	
www.broadripplack.com	2016-10-12	2018-10-31	Operating System	CentOS	
www.broadripplack.com	2017-12-26	2018-10-31	Framework	PHP (v5.6.40)	
www.broadripplack.com	2016-10-28	2018-10-31	CMS	Joomla (v3)	
www.broadripplack.com	2016-10-28	2018-10-31	Ad Network	Google	
www.broadripplack.com	2015-11-27	2018-10-31	Tracking Pixel	www.broadripplack.com	
www.broadripplack.com	2016-10-28	2018-10-31	JavaScript Library	jQuery	
www.broadripplack.com	2017-10-16	2018-10-31	Web Design	Font Awesome (v4.2.1)	
www.broadripplack.com	2016-10-28	2018-10-31	Analytics Service	Google Analytics	
www.broadripplack.com	2017-03-30	2018-10-31	JavaScript Library	jQuery Migrate	
www.broadripplack.com	2018-08-02	2018-10-31	CMS	Joomla (v3.8)	
www.broadripplack.com	2016-10-28	2018-10-31	Tracking Pixel	Google Analytics	
www.broadripplack.com	2016-10-28	2018-10-31	CMS	Joomla (v3.7.5)	
www.broadripplack.com	2018-07-12	2018-09-28	Advertising	AdSense	
www.broadripplack.com	2018-07-12	2018-09-28	DCO	Phorms	
www.broadripplack.com	2018-08-02	2018-08-29	Search	Google Maps	
www.broadripplack.com	2018-08-02	2018-08-29	Search	Google Search	
www.broadripplack.com	2017-10-16	2018-04-22	JavaScript Library	twilio.js (v0.4)	
www.broadripplack.com	2017-10-16	2018-04-22	Cryptocurrency Miner	Coin Hive	
www.broadripplack.com	2016-10-12	2017-10-24	Framework	PHP (v5.6.38)	
www.broadripplack.com	2016-10-12	2017-04-05	Analytics Service	CentOS	
www.broadripplack.com	2015-07-09	2016-09-25	Framework	ASP.NET	
www.broadripplack.com	2015-07-09	2016-09-25	Server	Microsoft-MS (v6.0)	
www.broadripplack.com	2015-11-27	2016-09-25	Tracking Pixel	counters.tricklabs.com	

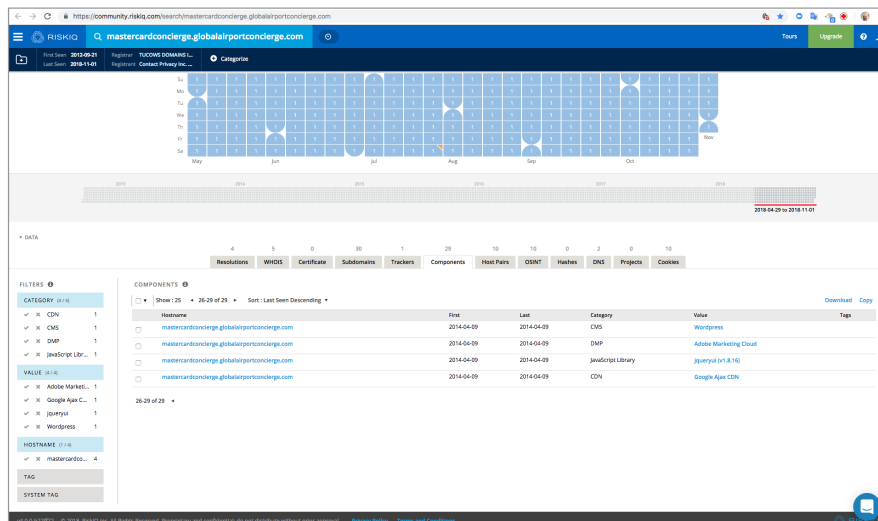
PHP and Joomla, the same components as pledgeinsurance.com, are listed.

Open mastercardconcierge.globalairportconcierge.com in another tab and click on the components tab.

[mastercardconcierge.globalairportconcierge.com Infrastructure Results | RiskIQ Community Edition](https://community.riskiq.com/search/mastercardconcierge.globalairportconcierge.com)

Hostname	First	Last	Category	Value	Tags
mastercardconcierge.globalairportconcierge.com	2015-11-21	2018-10-31	Framework	ASP.NET	
mastercardconcierge.globalairportconcierge.com	2018-10-10	2018-10-31	Server	Microsoft-MS (v10.0)	
mastercardconcierge.globalairportconcierge.com	2018-06-27	2018-10-31	JavaScript Library	jQuery	
mastercardconcierge.globalairportconcierge.com	2015-11-21	2018-10-31	JavaScript Library	jQuery UI	
mastercardconcierge.globalairportconcierge.com	2015-12-09	2018-10-31	Framework	PHP (v5.3.28)	
mastercardconcierge.globalairportconcierge.com	2014-04-09	2018-10-31	JavaScript Library	jQuery UI (v1.8.16)	
mastercardconcierge.globalairportconcierge.com	2018-10-10	2018-10-31	Hosting Provider	Microsoft Azure	
mastercardconcierge.globalairportconcierge.com	2017-05-20	2018-10-31	JavaScript Library	jQuery Migrate	
mastercardconcierge.globalairportconcierge.com	2018-03-19	2018-10-31	JavaScript Library	SWFObject	
mastercardconcierge.globalairportconcierge.com	2015-12-09	2018-06-28	Server	Microsoft-MS (v8.5)	
mastercardconcierge.globalairportconcierge.com	2018-06-27	2018-06-28	Ad Exchange	Facebook	
mastercardconcierge.globalairportconcierge.com	2018-03-03	2018-03-03	Cryptocurrency Miner	Coin Hive	
mastercardconcierge.globalairportconcierge.com	2016-01-21	2017-06-20	CDN	jQuery CDN	
mastercardconcierge.globalairportconcierge.com	2017-06-20	2017-06-20	JavaScript Library	jQuery (v1.11.1)	
mastercardconcierge.globalairportconcierge.com	2016-06-22	2017-06-20	Analytics Service	DoubleClick Floodlight	
mastercardconcierge.globalairportconcierge.com	2016-01-21	2017-06-20	JavaScript Library	jQuery (v1.11.1)	
mastercardconcierge.globalairportconcierge.com	2015-11-24	2017-03-30	Ad Network	Google	
mastercardconcierge.globalairportconcierge.com	2015-11-24	2017-03-30	JavaScript Library	jQuery (v1.11.0)	
mastercardconcierge.globalairportconcierge.com	2015-11-21	2015-12-02	Server	Microsoft-MS (v7.5)	
mastercardconcierge.globalairportconcierge.com	2015-11-21	2015-12-02	Framework	PHP (v5.6.20)	
mastercardconcierge.globalairportconcierge.com	2014-04-09	2014-04-09	Server	Apache (v2.2.15)	
mastercardconcierge.globalairportconcierge.com	2014-04-09	2014-04-09	Operating System	CentOS	
mastercardconcierge.globalairportconcierge.com	2014-04-09	2014-04-09	Framework	PHP (v5.3.2)	
mastercardconcierge.globalairportconcierge.com	2014-04-09	2014-04-09	CMS	ExpressionEngine	
mastercardconcierge.globalairportconcierge.com	2014-04-09	2014-04-09	JavaScript Library	jQuery (v1.4.4)	

PHP but no Joomla this time.



**Objective 3 completed:** What does the infrastructure look like and does it appear malicious?

We did not find any malicious infrastructure, but we did determine that all of the compromised web sites used PHP and 7, and 8 also used Joomla.

## Conclusion:

When investigating performance or availability issues it is a good idea to also investigate it as a potential security incident.

By removing the coinhive application user will no longer experience performance issues with the pledgeinsurance.com website.

Pledge Insurance and seven other domains were most likely compromised by a vulnerability in PHP and potentially Joomla. It is important to keep all of your infrastructure patched and have mitigating controls and layer security defences in place to prevent exploitation in network infrastructure, operating systems, and applications.



**RiskIQ, Inc.**  
22 Battery Street, 10th Floor  
San Francisco, CA. 94111

✉ sales@riskiq.net

☎ 1 888.415.4447

**Learn more at riskiq.com**

Copyright © 2020 RiskIQ, Inc. RiskIQ, the RiskIQ logo and RiskIQ family of marks are registered trademarks or trademarks of RiskIQ, Inc. in the United States and other countries. Other trademarks mentioned herein may be trademarks of RiskIQ or other companies.01\_20