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?

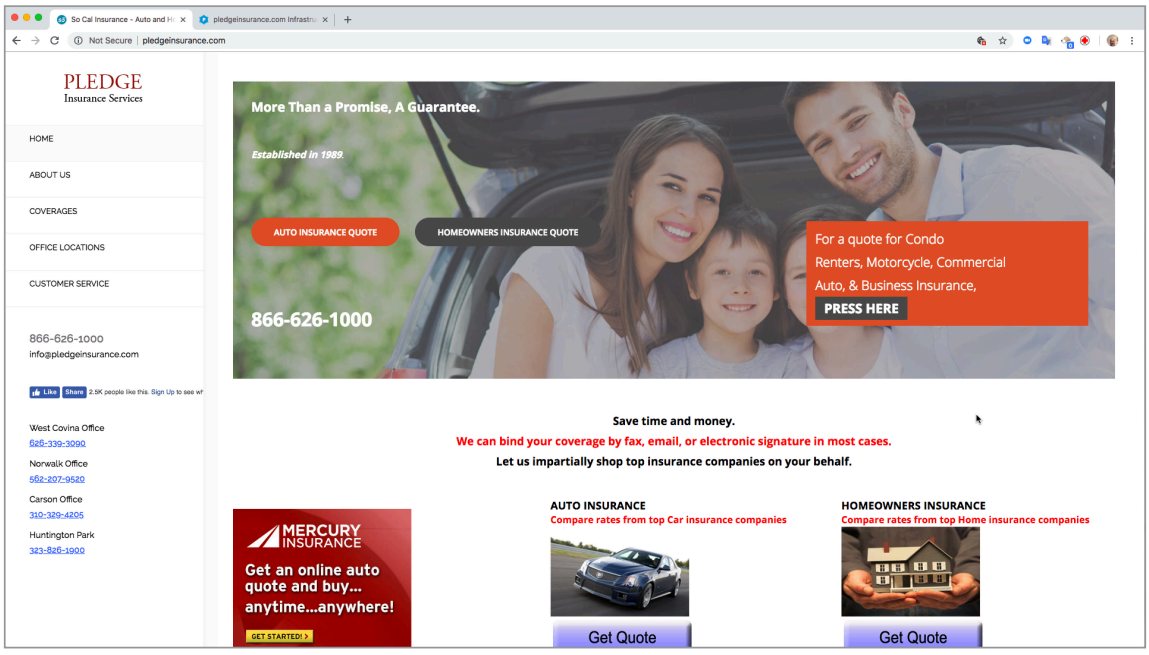
Objective 2: Are there any other websites that may exhibit the same behavior?

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

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

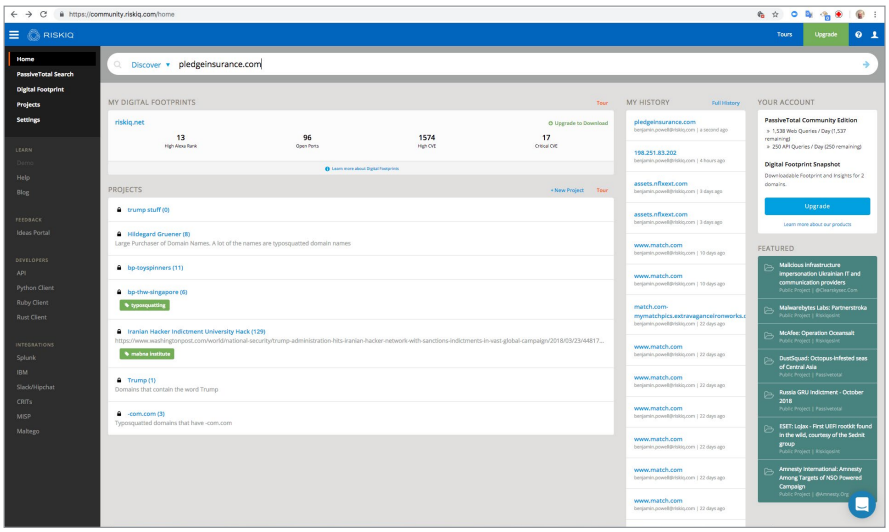


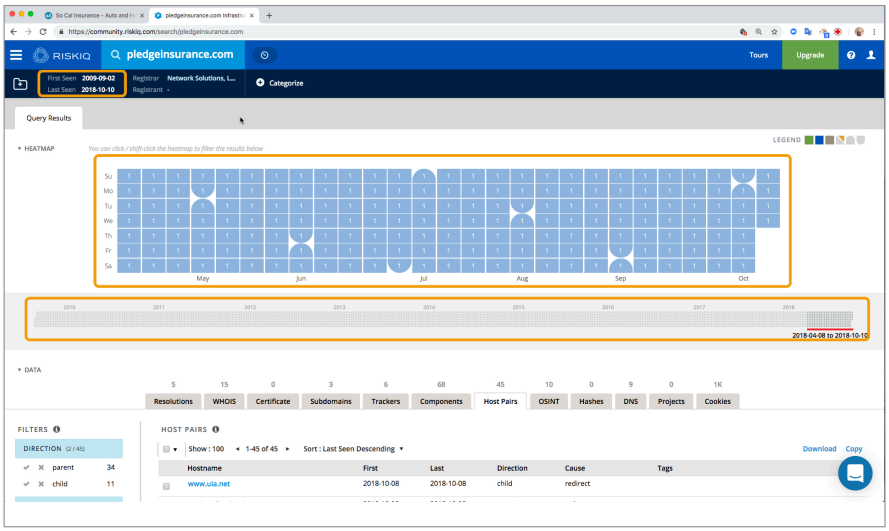
You see your organization's website and everything appears to be normal.

Step 2: **Perform a search for pledgeinsurance.com**

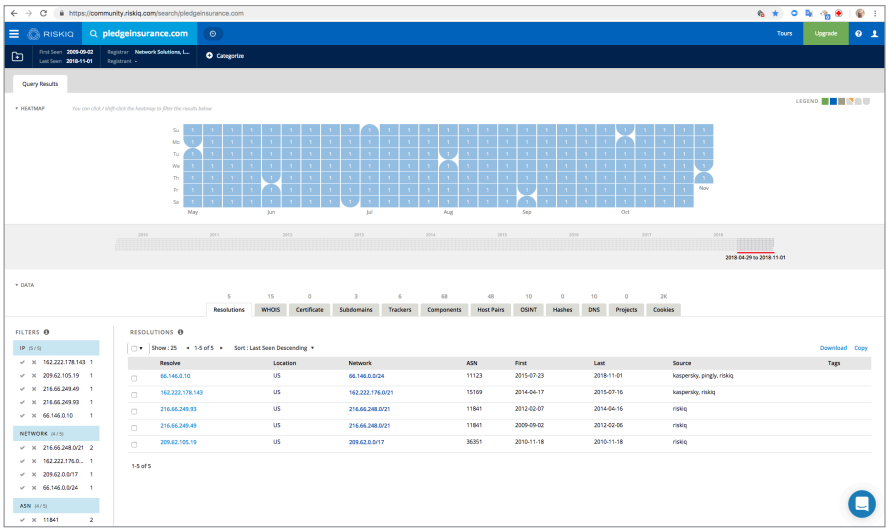
Log into https://community.riskiq.com with your web browser.

Search for pledgeinsurance.com
https://community.riskiq.com/search/pledgeinsurance.com





By examining the "First Seen" and "Last Seen," we can learn that pledgeinsurance.com has been around since 9-2-2009. Looking at the heatmap, we can see that the website has only had one IP address that has always been routable. The data bar shows continuous data for the entire time.

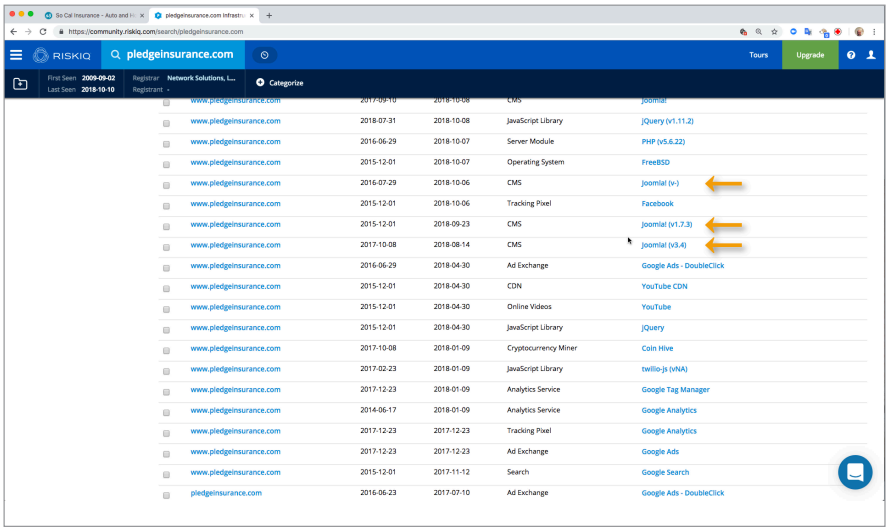


Pledge insurance has had five different IP addresses since 2009 — all have been in the US.

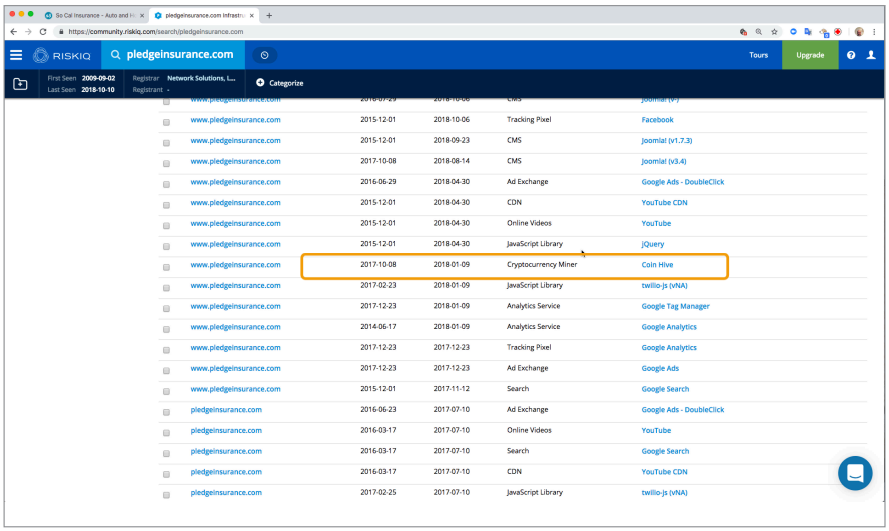
In order to determine if the website has been compromised, we will have to examine the advanced crawled data sets. These are dynamic data sets that are created when RiskIQ's virtual user interact with the websites. The crawl data sets we will be looking at are tracker, components, and host pairs.

Step 3: **Components**

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



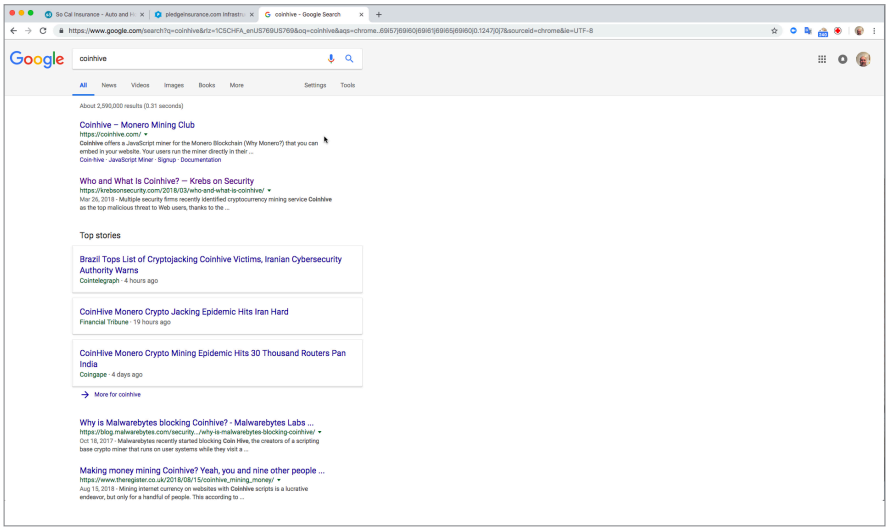
The components that tend to be compromised will be PHP, CMS (like Joomla), Word Press, and Drupal.



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

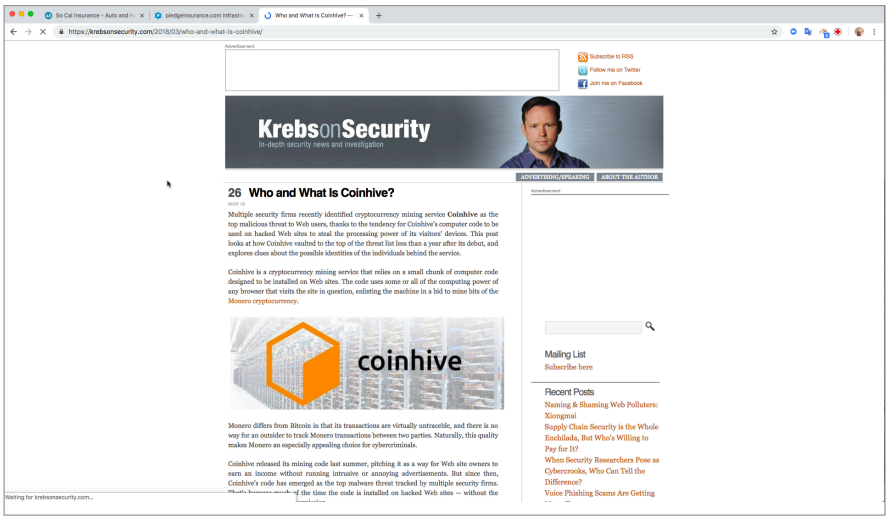
Step 4: **Research what is coinhive**

Now open a new tab and search for Coinhive.
coinhive - Google Search



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.

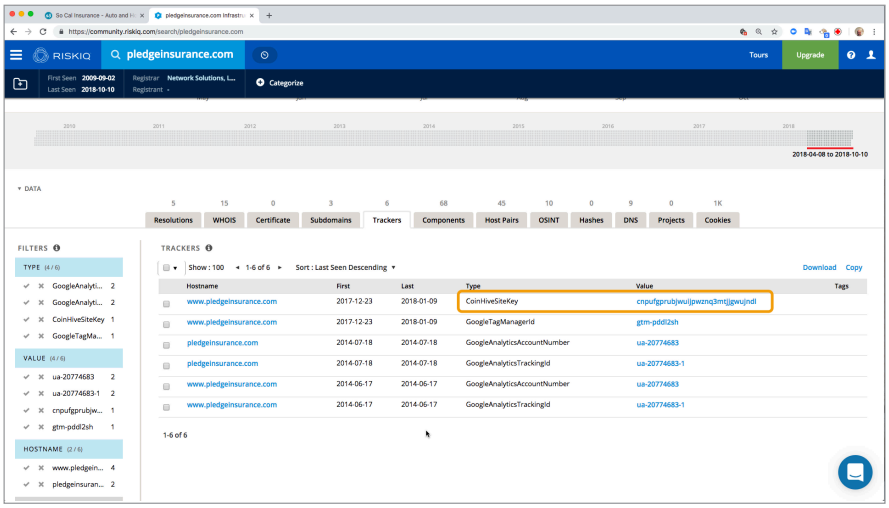
Objective 1 completed: Is the website compromised? If so, how and why?

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 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**

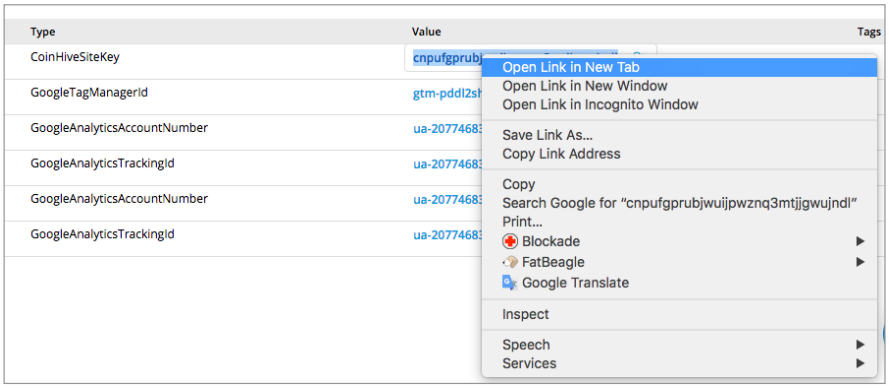


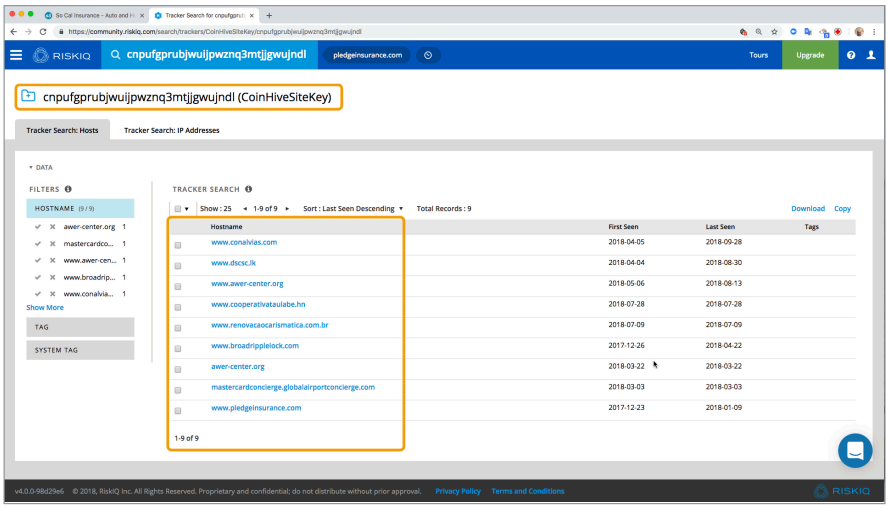
RiskIQ identified the CoinHiveSiteKey associated with this particular instance running on pledgeinsurance.com.

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 the the same threat actor or group.

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





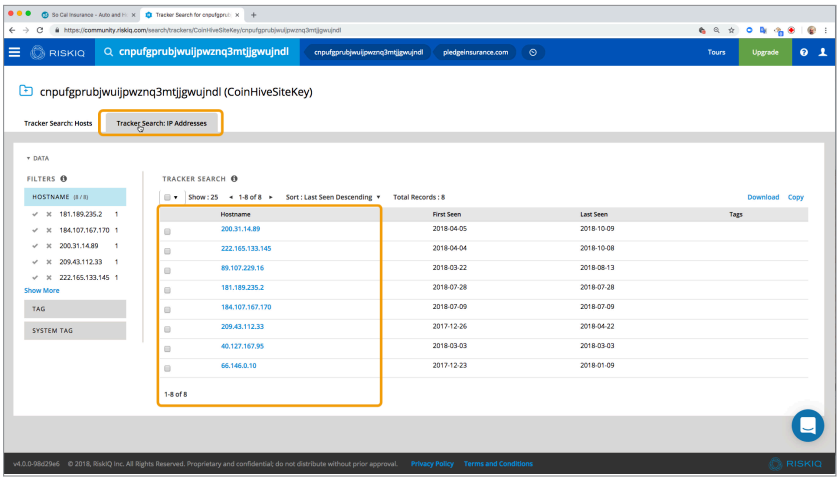
[Tracker Search for cnpufgprubjwuijpwznq3mtjjgwujndl (CoinHiveSiteKey) | RiskIQ Community Edition]

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.



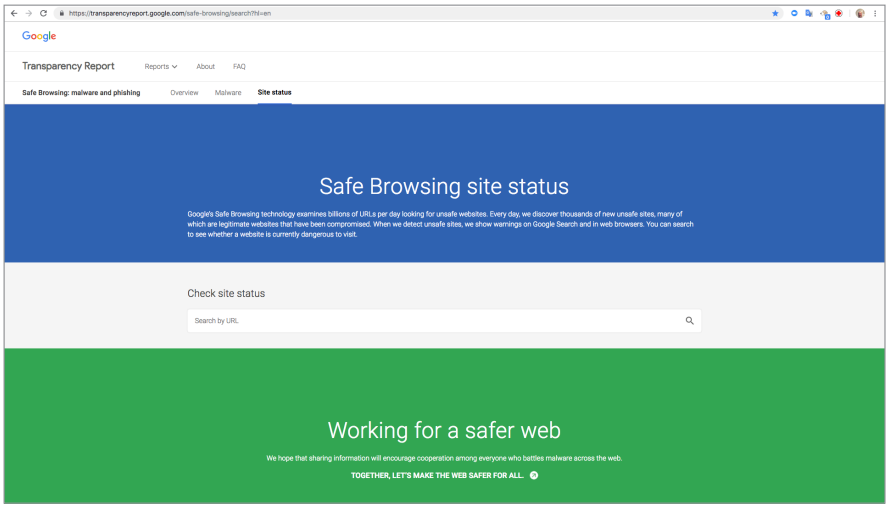
We can determine that all of the website are not on the same IP address. It appears that the websites might have been compromised the same way as pledgeinsurance.com, most likely by compromising the same web components to gain access and install Coinhive.

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.**

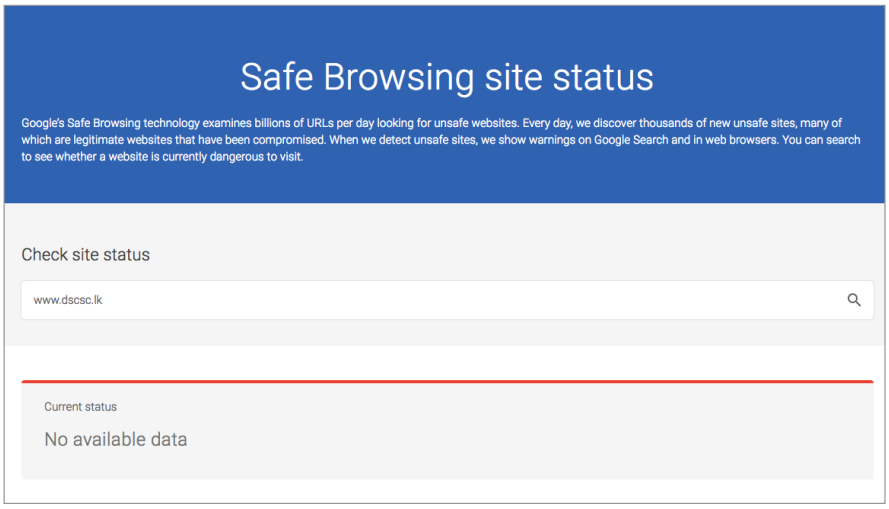
One way to determine if a website is malicious is to check it against the google safe browsing list.

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



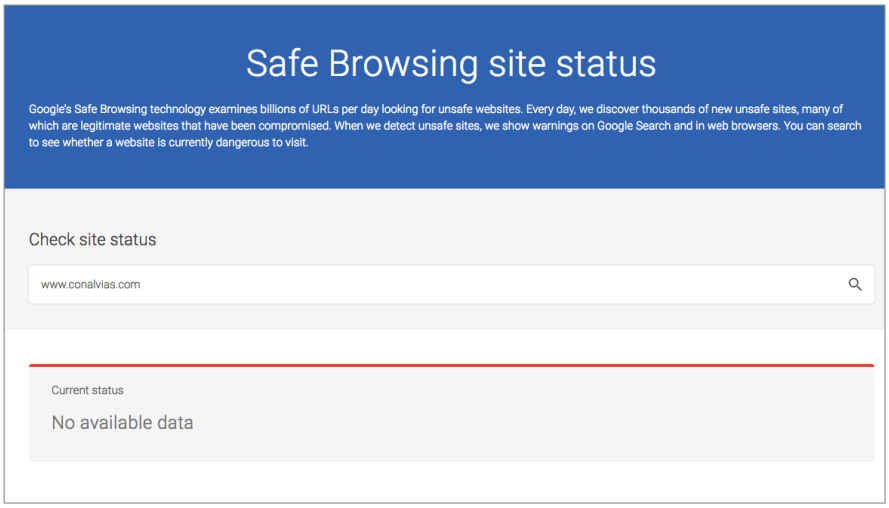
Now copy and paste each domain name into the check site status and press the return key on your keyboard.

Check www.dscsc.lk

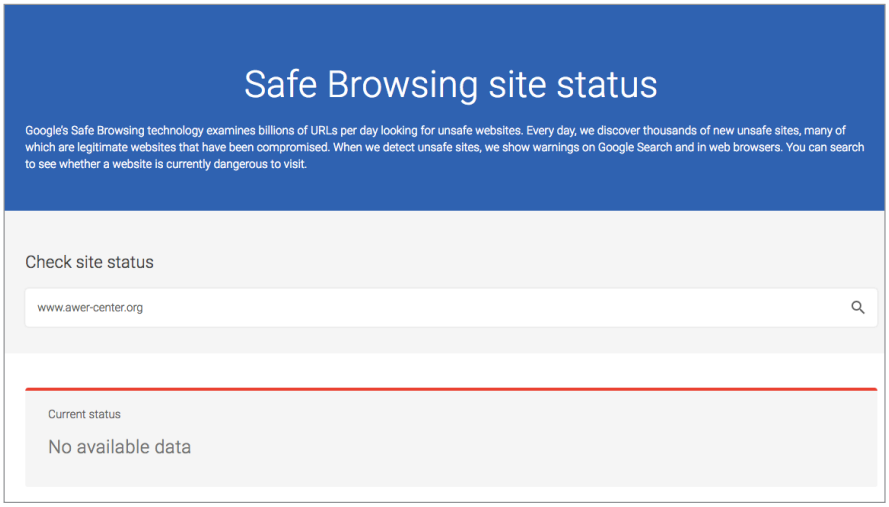


www.dscsc.lk is Not malicious.

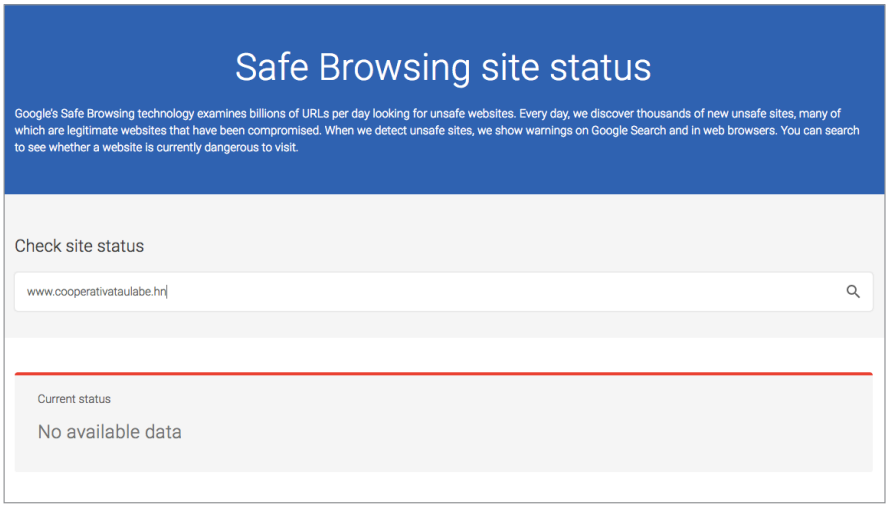
Check www.conalvias.com



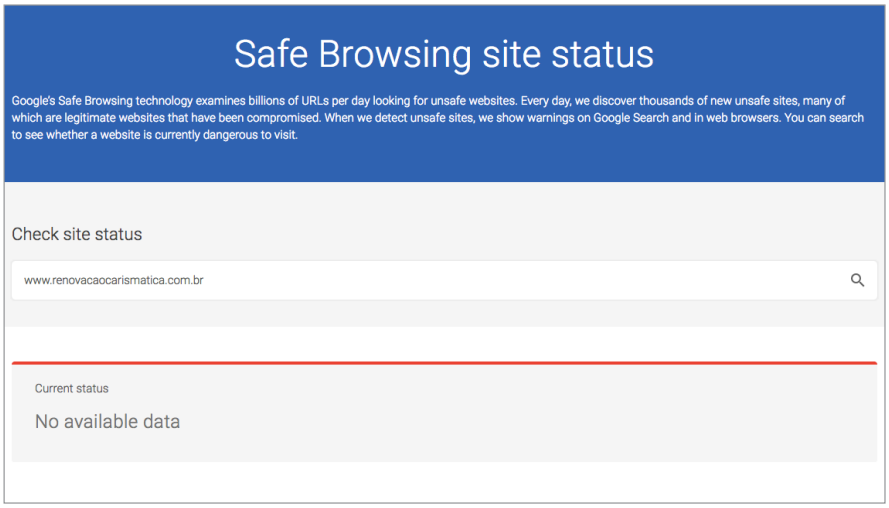
Check www.awer-center.org, this domain appears twice in the list.



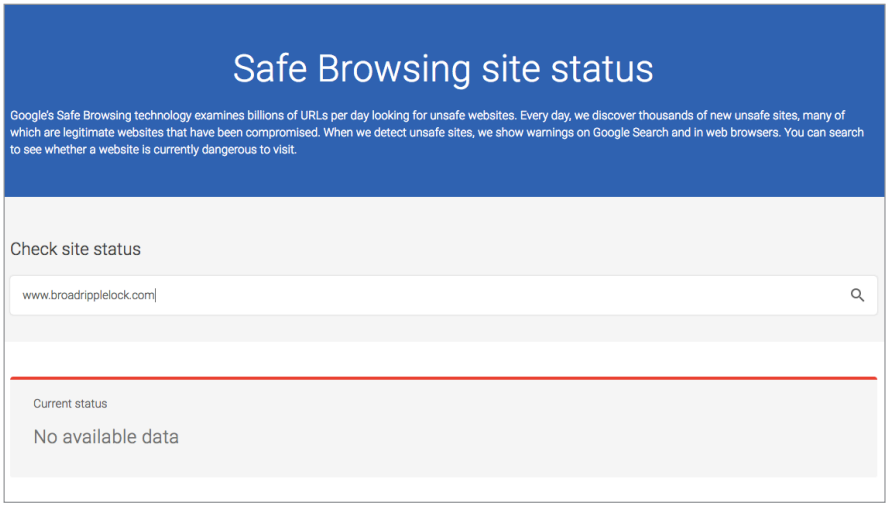
Check www.cooperativataulabe.hn



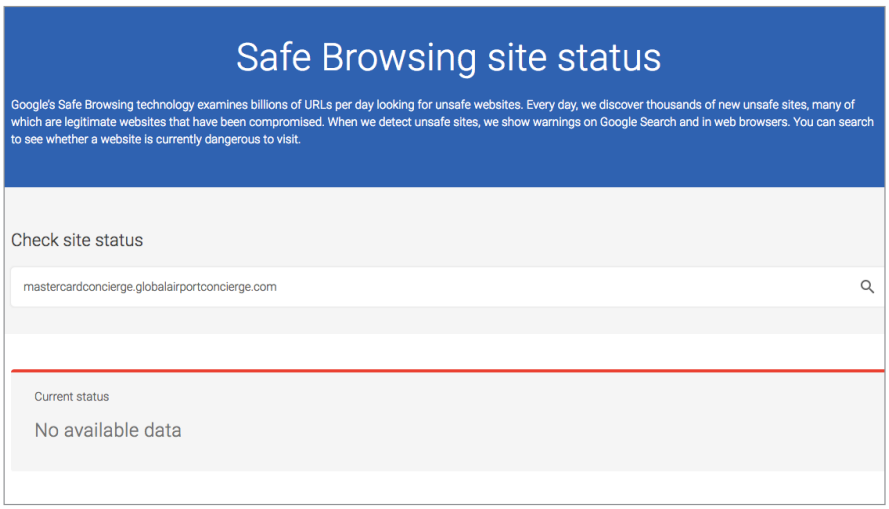
Check www.renovacaocarismatica.com.br



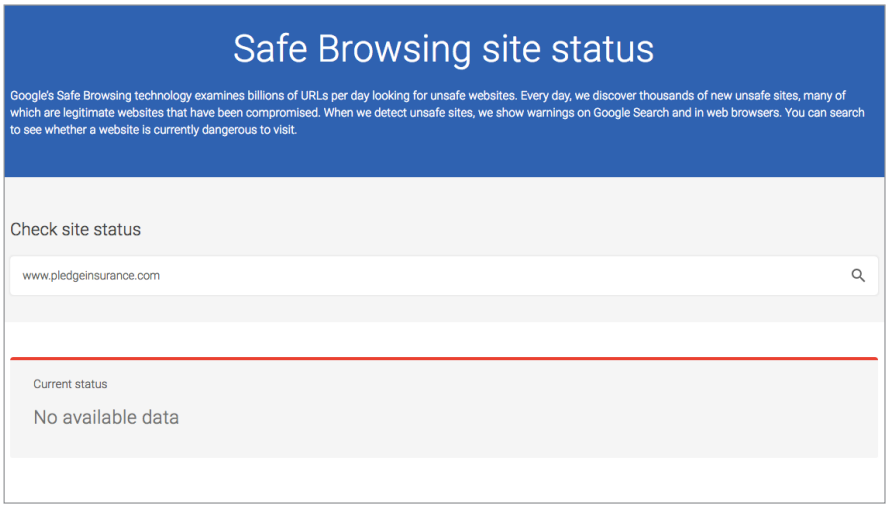
Check www.broadripplelock.com



Check mastercardconcierge.globalairportconcierge.com



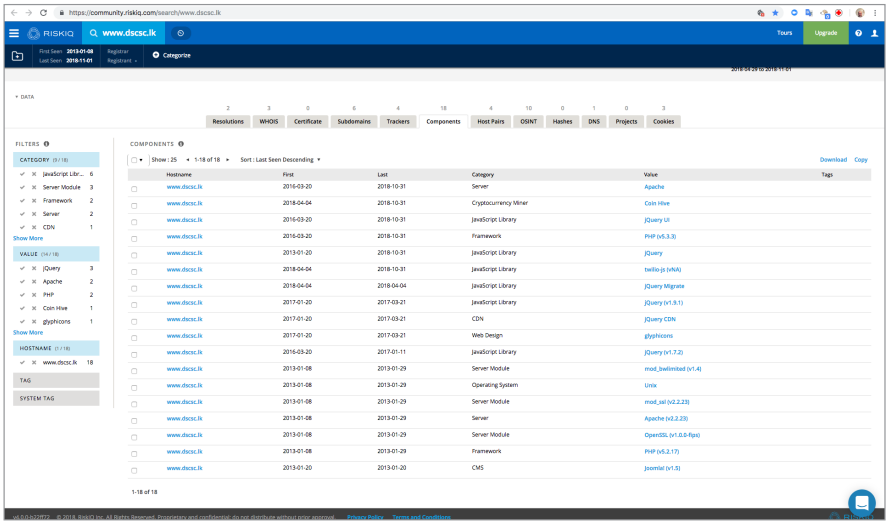
Check www.pledgeinsurance.com



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.

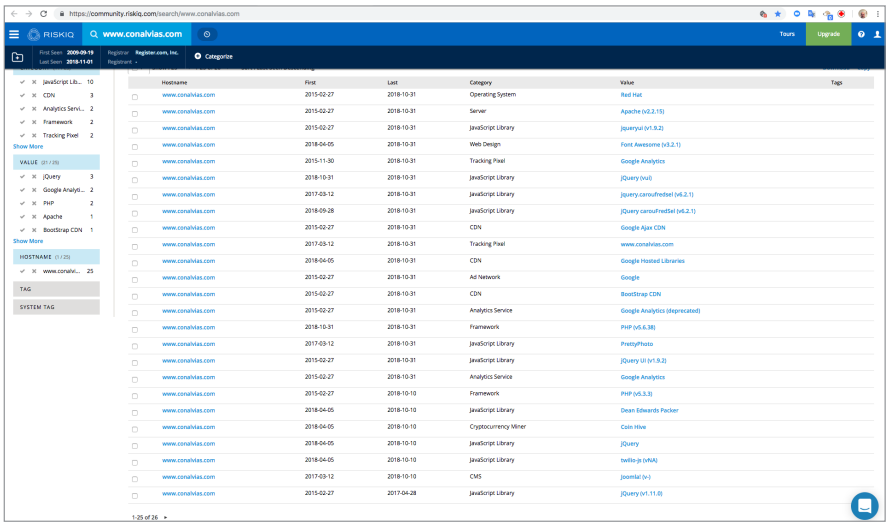
Step 7: Review the components tab for CoinHiveSiteKey domains

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



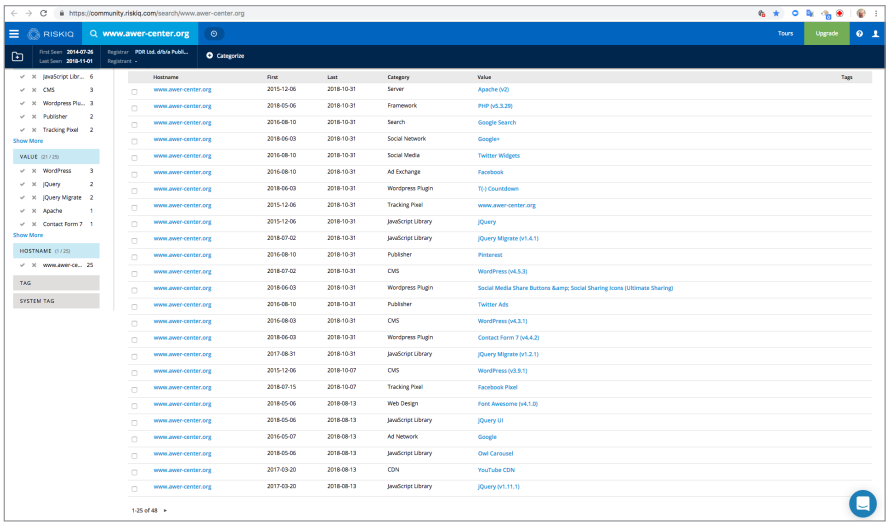
PHP and Joomla, the same components as pledgeinsurance.com, are listed.

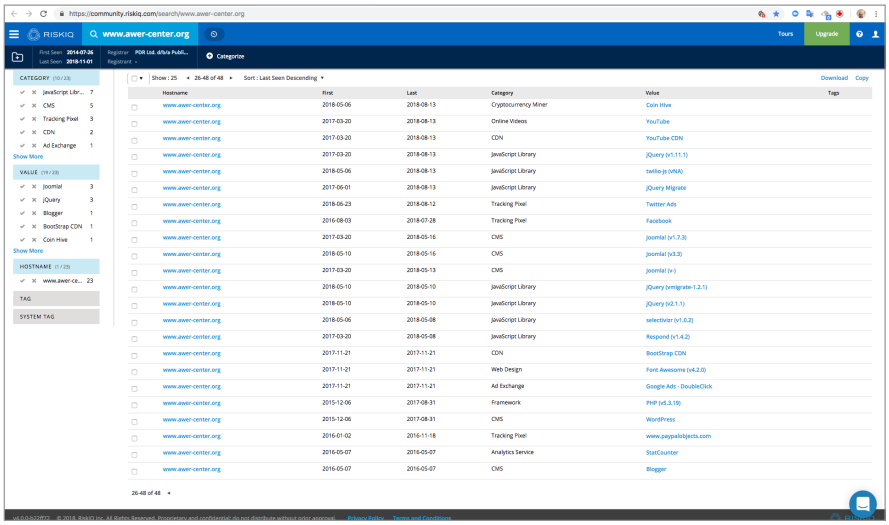
Open www.conalvias.com in another tab and click on the components tab.
[www.conalvias.com Infrastructure Results | RiskIQ Community Edition]



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

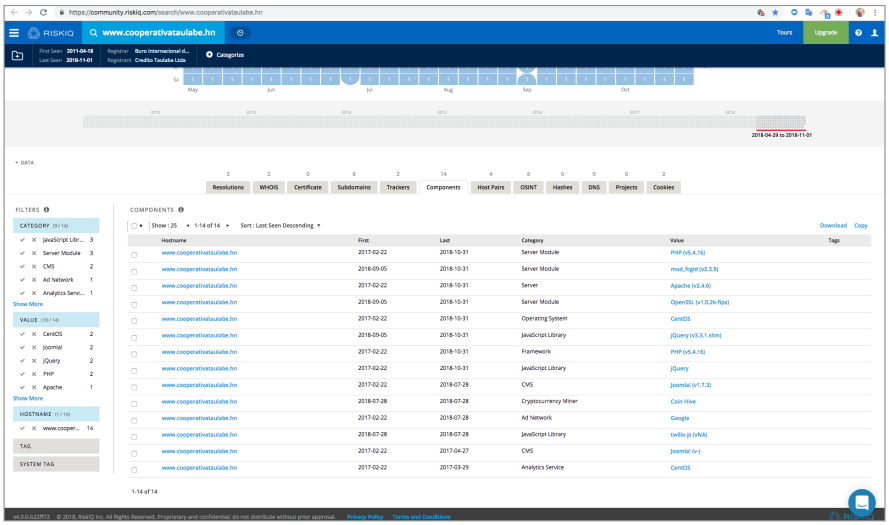
Open www.awer-center.org in another tab and click on the components tab.
[www.awer-center.org Infrastructure Results | RiskIQ Community Edition]





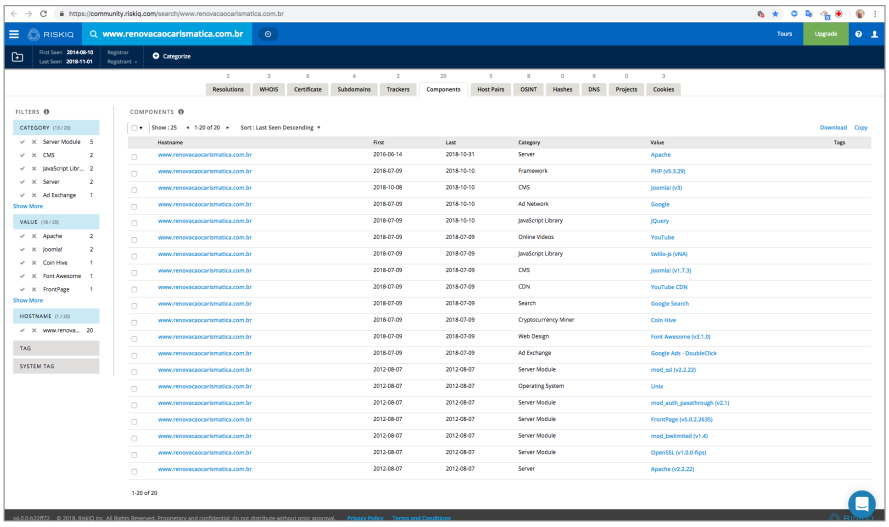
PHP and Joomla, the same components as pledgeinsurance.com, are listed.

Open www.cooperativataulabe.hn in another tab and click on the components tab.
[www.cooperativataulabe.hn Infrastructure Results | RiskIQ Community Edition]



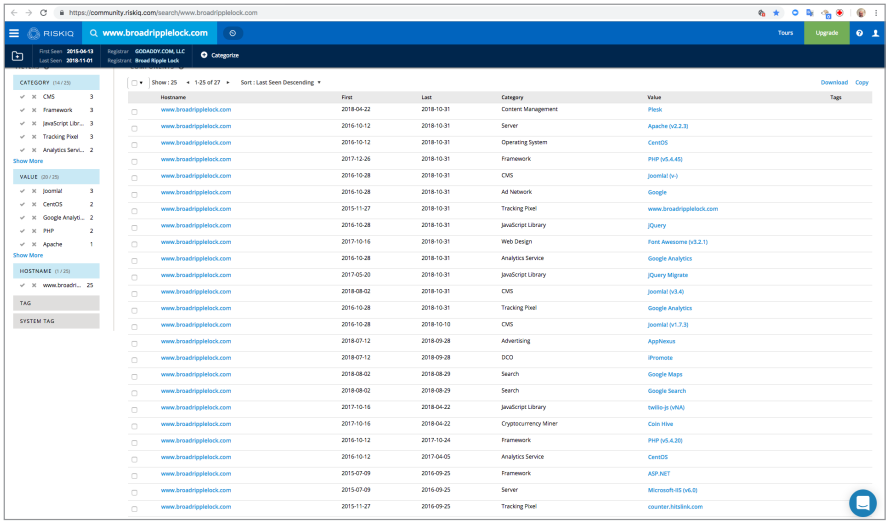
PHP and Joomla, the same components as pledgeinsurance.com, are listed.

Open www.renovacaocarismatica.com in another tab and click on the components tab.
[www.renovacaocarismatica.com.br Infrastructure Results | RiskIQ Community Edition]



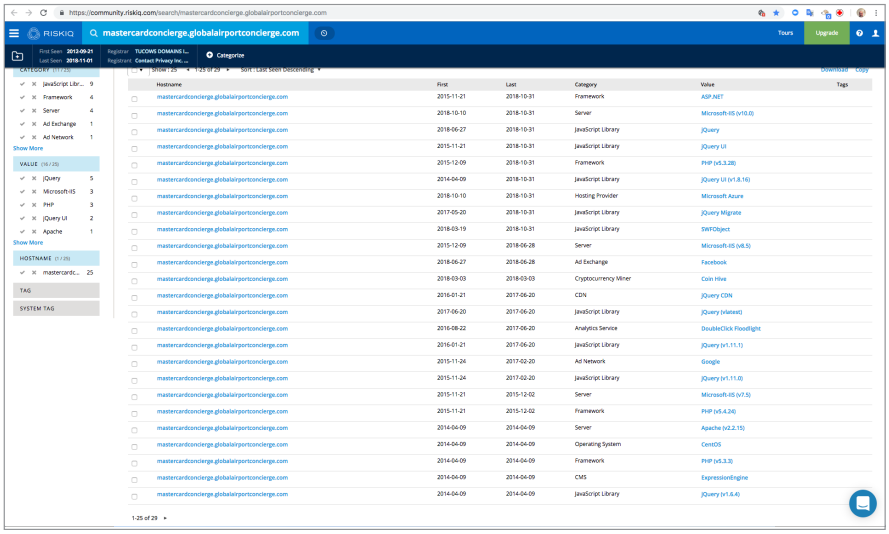
PHP and Joomla, the same components as pledgeinsurance.com, are listed.

Open www.broadripplelock.com in another tab and click on the components tab.
[www.broadripplelock.com Infrastructure Results | RiskIQ Community Edition]

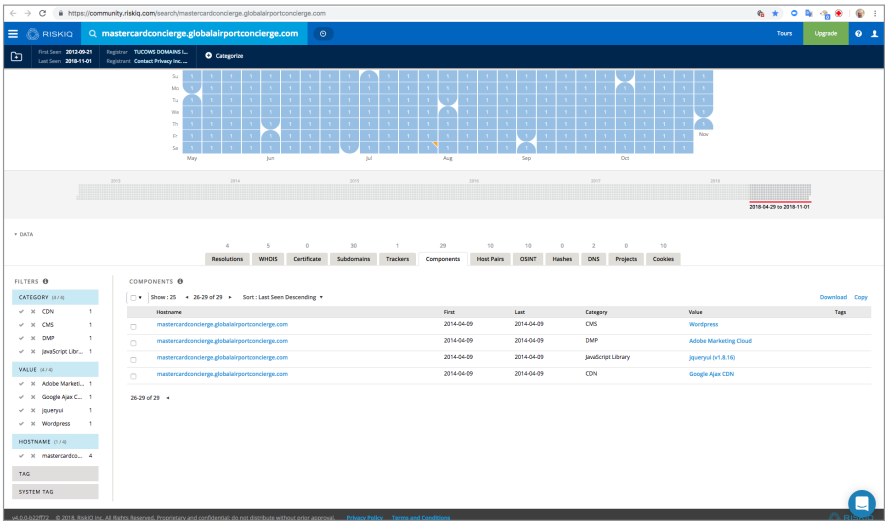


PHP and Joomla, the same components as pledgeinsurance.com, are listed.

Open mastercardconcierge.globalairportconcierge.com in another tab and click on the components tab.
[mastercardconcierge.globalairportconcierge.com Infrastructure Results | RiskIQ Community Edition]



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®

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

sales@riskiq.net
1 888.415.4447

Learn more at riskiq.com