

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

<u>So Cal Insurance - Auto and Home Insurance in Los Angeles, West Covina, Carson, Huntington</u> <u>Park, Norwalk and Garden Grove</u>



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.

	unity.riskiq.com/search/pledg												• • • • • • • •
	edgeinsurance.com												Upgrade 😯
	ingistrar Network Solutions, L., ingistrant -	• Categorize											
Query Results													
													LEGEND I I I
the car block ship		500W											
	Su 1				1 1						A. A. A. A.		
	Mo												
	Tu 1												
	Th												
	R 1										n n n Nov		
	50 1	1.1	1. 1. 1.		1.1	1.1	1 1 1		1.1	1. 1. 1.	(a) (a) (a)		
	Ma		jun	Ju		Aug		Sep		Oct			
												2018 04-29 to 2018-11-01	
ATA													
ATA		5		0 3	4	68	48	10	0	10 0	2K		
ATA		5 Resolutions		0 3 Subdomains		68 Components	48 Host Pairs	10 OSINT	0 Hashes	10 0 DNS Projects			
	RESOLUTIONS 0												
TERS Ø	RESOLUTIONS 0	Resolutions	WHOIS Cert	ificate Subdomains									Download Cop
TERS 0 ((5/5)		Resolutions	WHOIS Cert	ificate Subdomains	Trackers	Components							Download Cop Tags
15/5) × 162.222.178.143 1 × 209.62.105.19 1	[□ •] Show: 25 • 1	Resolutions	WHOIS Cerr	ificate Subdomains	Tracleers	Components	Host Pairs	OSINT		DNS Projects	Cookies	riskiq	
TERS (0) (3/3) × 1622222,178,143 1 × 209,62,105,19 1 × 216,665,240,49 1	[□•]Show:25 + 1 Resolve	Resolutions 3 of 5 ► Sort :	WHOIS Cen Last Seen Descending Location	oficate Subdomains	Dr24	Components	Host Pairs ASN	OSINT		DNS Projects	Cookies Source	riskiq	
TERS 0 (3/3) × 162,222,178,143 1 × 209,62,105,19 1 × 216,662,249,49 1 × 216,662,249,49 1	Show : 25 1 Resolve 66.146.0.10 162.222.178.1	Resolutions d of 5 + Sort : 43	WHOIS Cent Last Seen Descending Location US	Subdomains	0/24 176.0/21	Components	Host Pairs ASN 11123	05INT First 2015-07-23		DNS Projects	Cookies Source kaspersky, pingly.	riskog	
102222178-143 1 × 102222178-143 1 × 209.62.105.19 1 × 216.66.249.49 1 × 216.66.249.49 1	• Show : 25 • 1 Resolve 66.146.0.10 • • • 162.222.178.1 • • • 216.66.249.93 • •	Resolutions	WHOIS Cent Last Seen Descending Location US US	strate Subdomains	0/24 176.0/21	Components	Host Pairs ASN 11123 15169	05INT First 2015-07-23 2014-04-17		DNS Projects	Cookies Source kospersky, pingly, kuspersky, rinkų	rekiq	
TERS 0 p.19 × 192222178148 1 × 20962.105.19 1 × 21666.249.49 1 × 21666.249.49 1 × 66.160.010 1	• 3how : 25 • 1 Resolve 66.146.0.10 • • • 162.222.178.1 • • • 216.66.249.33 • • • 216.66.249.48 • •	Resolutions -3 of 5 + Sort : 43	WHOIS Cent Last Seen Descending US US US US US	Subdomains * Network 66.146.0. 162.222: 216.66.2. 216.66.2.	0/24 67.24 88.0/21 88.0/21	Components	Hest Pairs ASN 11123 15169 11841 11841	OSINT First 2015-07-23 2014-04-17 2012-02-07 2009-09-02		DNS Projects	Cookies Source kosporsky, pingly, kaspansky, riskiq riskiq riskiq	relikq	
TERS U D/31 V X 102.222.178.143 X 205.62.105.19 X 205.62.203.09 X 216.66.200.400 X 216.66.200.10 X 216.66.200.10 X 216.66.200.20 X 216.66.200.20 X 216.66.200.20	• Show : 25 • 1 Resolve 66.146.0.10 • • • 162.222.178.1 • • • 216.66.249.93 • •	Resolutions -3 of 5 + Sort : 43	WHOIS Cent Last Seen Descending Location US US US	Subdomains (* Network 06.149.0 162.222: 216.65.2	0/24 67.24 88.0/21 88.0/21	Components	Host Pairs ASN 11123 15169 11841	OSINT First 2015-07-23 2014-04-17 2012-02-07		DNS Projects Last 2018-11-01 2015-07-16 2014-04-16	Cookles Source kaspersky, pingly, kaspensky, niską riskią	riską	
TTERS 0 1979 1979 1970 197	• 3how : 25 • 1 Resolve 66.146.0.10 • • • 162.222.178.1 • • • 216.66.249.33 • • • 216.66.249.48 • •	Resolutions -3 of 5 + Sort : 43	WHOIS Cent Last Seen Descending US US US US US	Subdomains * Network 66.146.0. 162.222: 216.66.2. 216.66.2.	0/24 67.24 88.0/21 88.0/21	Components	Hest Pairs ASN 11123 15169 11841 11841	OSINT First 2015-07-23 2014-04-17 2012-02-07 2009-09-02		DNS Projects	Cookies Source kosporsky, pingly, kaspansky, riskiq riskiq riskiq	nską	
TERS 0 10/10 1	Show: 25 1 Resolve 66.146.0.10 142.222.778.1 216.66.249.33 216.66.249.43 216.66.249.43	Resolutions -3 of 5 + Sort : 43	WHOIS Cent Last Seen Descending US US US US US	Subdomains * Network 66.146.0. 162.222: 216.66.2. 216.66.2.	0/24 67.24 88.0/21 88.0/21	Components	Hest Pairs ASN 11123 15169 11841 11841	OSINT First 2015-07-23 2014-04-17 2012-02-07 2009-09-02		DNS Projects	Cookies Source kosporsky, pingly, kaspansky, riskiq riskiq riskiq	riskiq	
TERS 0 10/10 1	Show: 25 1 Resolve 66.146.0.10 142.222.778.1 216.66.249.33 216.66.249.43 216.66.249.43	Resolutions -3 of 5 + Sort : 43	WHOIS Cent Last Seen Descending US US US US US	Subdomains * Network 66.146.0. 162.222: 216.66.2. 216.66.2.	0/24 67.24 88.0/21 88.0/21	Components	Hest Pairs ASN 11123 15169 11841 11841	OSINT First 2015-07-23 2014-04-17 2012-02-07 2009-09-02		DNS Projects	Cookies Source kosporsky, pingly, kaspansky, riskiq riskiq riskiq	riskiq	
eETWORK (4/3) / X 216.66.248.0/21 2 / X 162.222.176.0 1 / X 209.62.0.0/17 1	Show: 25 1 Resolve 66.146.0.10 142.222.778.1 216.66.249.33 216.66.249.43 216.66.249.43	Resolutions -3 of 5 + Sort : 43	WHOIS Cent Last Seen Descending US US US US US	Subdomains * Network 66.146.0. 162.222: 216.66.2. 216.66.2.	0/24 67.24 88.0/21 88.0/21	Components	Hest Pairs ASN 11123 15169 11841 11841	OSINT First 2015-07-23 2014-04-17 2012-02-07 2009-09-02		DNS Projects	Cookies Source kosporsky, pingly, kaspansky, riskiq riskiq riskiq	nską	

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 RisklQ'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.

C A https://community.riskiq.						e a @ ☆ ○ № 4 <u>8</u> ●	
RISKIQ Q ple	dgeinsu	rance.com 💿				Tours Upgrade	0
	gistrar Netv gistrant -	work Solutions, L					
	0	www.ptedgeinsurance.com	2017-09-10	2018-10-08	CMS	Joomia!	
		www.pledgeinsurance.com	2018-07-31	2018-10-08	JavaScript Library	jQuery (v1.11.2)	
		www.pledgeinsurance.com	2016-06-29	2018-10-07	Server Module	PHP (v5.6.22)	
		www.pledgeinsurance.com	2015-12-01	2018-10-07	Operating System	FreeBSD	
		www.pledgeinsurance.com	2016-07-29	2018-10-06	CMS	Joomlal (v-)	
		www.pledgeinsurance.com	2015-12-01	2018-10-06	Tracking Pixel	Facebook	
		www.pledgeinsurance.com	2015-12-01	2018-09-23	CMS	Joomla! (v1.7.3)	
		www.pledgeinsurance.com	2017-10-08	2018-08-14	CMS	Joomlal (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	-

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

RISKIQ Q pled	goingu	irance.com					nten no	Upgr		0 6
							Tours	018	we	
	itrar Nets itrant -	work Solutions, L Categorize								
		www.preagensurance.com	2010-07-29	2010-10-00	CW0	Joomiai (v-)			_	
		www.piedgeinsurance.com	2015-12-01	2018-10-06	Tracking Pixel	Facebook				
		www.pledgeinsurance.com	2015-12-01	2018-09-23	CMS	Joomla! (v1.7.3)				
		www.piedgeinsurance.com	2017-10-08	2018-08-14	CMS	Joomla! (v3.4)				
		www.pledgeinsurance.com	2016-06-29	2018-04-30	Ad Exchange	Google Ads - DoubleClick				
		www.piedgeinsurance.com	2015-12-01	2018-04-30	CDN	YouTube CDN				
		www.pledgeinsurance.com	2015-12-01	2018-04-30	Online Videos	YouTube				
		www.piedgeinsurance.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	twillo-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			-	ſ
				2017-07-10	JavaScript Library					ų.

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. <u>coinhive - Google Search</u>



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

E 🔘 RISKIQ 🤇) pledgeinsurar	ce.com											Tours	Upgrade	0
Rist Seen 2009-09-02 Last Seen 2018-10-10	Registrar Network : Registrant -	iolutions, L.,	Categorize	e		<i>,</i>									
2010	2011			2013		2014	2015		2016			2017		2018 2018-04-08 to	2018-10-
DATA	5 Resolutions	15 WHOIS	0 Certificate	3 Subdomains	6 Trackers	68 Components	45 Host Pairs	10 OSINT	0 Hashes	9 DNS	0 Projects	1K Cookies			
ILTERS 0	TRACKER	5 0													
	()	ow : 100 🔺 '	1-6 of 6 ► Si	ort : Last Seen Des First	cending *	st Ti	vpe			Valu	ie			Download	
		tname w.pledgelnsura w.pledgelnsura	ance.com ance.com	First 2017-12 2017-12	Lan 2-23 20 2-23 20	18-01-09 C	ype oinHiveSiteKey ioogleTagManager			cnp gtm	ufgprubjwuij h-pddl2sh	ipwznq3mt]jgw	wjndl		I Copy Tags
** X GoogleAnalyti 2 ** X GoogleAnalyti 2 ** X CoinHiveSiteKey 1 ** X GoogleTagMa 1 VALUE (4/9) * *	Here www pice pice	itname w.pledgeinsura	ance.com ance.com com	First 2017-12	2-23 20 2-23 20 7-18 20 7-18 20	18-01-09 C 18-01-09 G 14-07-18 G 14-07-18 G	oinHiveSiteKey	countNumber		cnp gtm ua- ua-	ufgprubjwuij	ipwznq3mtjigw	rujndi		
 ✓ X GoogleAnalyti 2 ✓ X CoinHiveSiteKey 1 ✓ X GoogleTagMa 1 VALUE (476) 	Here WWV Place Place Place WWV	tname nv.pledgeinsura nv.pledgeinsura dgeinsurance.c dgeinsurance.c	ance.com ance.com com com ance.com	First 2017-12 2017-12 2014-07 2014-07	Let 2-23 20 2-23 20 7-18 20 7-18 20 6-17 20	18-01-09 C 18-01-09 G 14-07-18 G 14-07-18 G 14-06-17 G	oinHiveSiteKey ioogleTagManager ioogleAnalyticsAco ioogleAnalyticsTran	ckingld		enp gtm ua- ua- ua-	ufgprubjwulj i-pddl2sh 20774683 20774683-1	pwznq3mtjjgw	njndl		

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.

Туре	Value	Ta
CoinHiveSiteKey	cnpufgprubj	Open Link in New Tab
GoogleTagManagerid	gtm-pddl2sł	Open Link in New Window Open Link in Incognito Window
GoogleAnalyticsAccountNumber	ua-2077468:	Save Link As
GoogleAnalyticsTrackingId	ua-2077468:	Copy Link Address
GoogleAnalyticsAccountNumber	ua-2077468:	Copy Search Google for "cnpufgprubjwuijpwznq3mtjjgwujndl"
GoogleAnalyticsTrackingId	ua-2077468:	Print
		Inspect
		Speech Services

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

🔘 RISKIQ 🔍 CNPU	fgprubjwuijpwznq3mtjjgwujndl	pledgeinsurance.com	0		Tours			•
W RISKIQ Q CIPU	ightanjwajpwzndpindjgwajna	pieogensurance.com	•		Tours	Upgrade	, v	1
cnpufgprubiwuiipwz	nq3mtjjgwujndl (CoinHiveSiteK							
	nqsmijjgwujnui (coinnivesiteki	ey)						
Tracker Search: Hosts Tracker S	Search: IP Addresses							
* DATA								
FILTERS Ø	TRACKER SEARCH							
HOSTNAME (9/9)		: Last Seen Descending 🔻	Total Records : 9			Download	Сору	
✓ X awer-center.org 1	Hostname			First Seen	Last Seen	Tags		
✓ X mastercardco 1	www.conalvias.com			2018-04-05	2018-09-28			
✓ X www.awer-cen 1	www.dscsc.lk			2018-04-04	2018-08-30			
✓ X www.broadrip 1	www.awer-center.org			2018-05-06	2018-08-13			
✓ X www.conalvia 1 Show More	www.cooperativataulabe.hn			2018-07-28	2018-07-28			
TAG	www.renovacaocarismatica.com	n.br		2018-07-09	2018-07-09			
				2017-12-26	2018-04-22			
SYSTEM TAG				2018-03-22				
	awer-center.org			2018-03-22	2018-03-22			
	mastercardconcierge.globalairp	ortconcierge.com		2018-03-03	2018-03-03			
	www.pledgeinsurance.com			2017-12-23	2018-01-09			
	1-9 of 9						-	
	1.5415							J

Tracker Search for cnpufgprubjwujpwznq3mtjjgwujndl (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.

🔘 RISKIQ 🔍 Cnpul	fgprubjwuijpwz	Indoundiewolu	di cnpufgprubjwuijpwzną	3mtjjgwujndl pledgeinsurance.com	0	Tours Upgra	sde 🕻
cnpufgprubjwuijpwzi	กกริตามีเดิงแม่ก	dl (CoinHiveSi	teKev)				
	indonud)Produ		(center)				
Tracker Search: Hosts Tracker S	Search: IP Addresses						
* DATA							
FILTERS 0	TRACKER SEAF	RCH ()					
HOSTNAME (87/8)	Show: 2	15 ≺ 1-8 of 8 ►	Sort : Last Seen Descending 🔻	Total Records : 8		Downlo	oad Copy
✓ × 181.189.235.2 1		Hostname		First Seen	Last Seen	Tags	
✓ × 184.107.167.170 1		200.31.14.89		2018-04-05	2018-10-09		
✓ ※ 200.31.14.89 1		222.165.133.145		2018-04-04	2018-10-08		
✓ × 209.43.112.33 1	0	89.107.229.16		2018-03-22	2018-08-13		
✓ × 222.165.133.145 1 Show More		181,189,235,2		2018-07-28	2018-07-28		
	-	184.107.167.170		2018-07-09	2018-07-09		
TAG	8						
SYSTEM TAG		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						
	1.0 01 8						
							-

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

← → C (iii https://transparencyreport.google	com/safe-browsing/search?N=en	* • • • • •
Google		
Transparency Report Reports	✓ About FAQ	
Safe Browsing: malware and phishing	Direview Malware Site status	
	Cofo Broweing oito status	
	Safe Browsing site status	
	Google's Safe Browsing technology examines billions of URLs per day loaking 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 dargeous to visit.	
	Check site status	
	Search by URL Q	
	Working for a safer web	
	We hope that sharing information will encourage cooperation among everyone who battles malware across the web.	

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

Check www.dscsc.lk

ogle's Safe Browsing technology examines billions of URLs per day looking for un	ng site status safe websites. Every day, we discover thousands of new unsafe sites, many of sites, we show warnings on Google Search and in web browsers. You can search
neck site status	
www.dscsc.lk	Q
Current status	

www.dscsc.lk is Not malicious.

Check 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 www.conalvias.com Q
Current status
No available data

Check 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 www.awer-center.org Q
Current status No available data

Check 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
www.cooperativataulabe.hnj Q
Current status
No available data

9

Check www.renovacaocarismatica.com.br

Saf	e Browsing site status
	f URLs per day looking for unsafe websites. Every day, we discover thousands of new unsafe sites, many of nised. When we detect unsafe sites, we show warnings on Google Search and in web browsers. You can search
Check site status	
www.renovacaocarismatica.com.br	۹
Current status	
No available data	

Check 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
www.broadripptelock.com
Current status
No available data

Check mastercardconcierge.globalairportconcierge.com

Socgle'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 vhich are legitimate websites that have been compromised. When we detect unsafe sites, we show warnings on Google Search and in web browsers. You can sear o see whether a website is currently dangerous to visit.	ch
Check site status	
mastercardconcierge.globalairportconcierge.com	Q
Current status	
No available data	

Check www.pledgeinsurance.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 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 a to see whether a website is currently dangerous to visit.	
Check site status	
www.pledgeinsurance.com	Q
Current status	
No available data	

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

	unity.riskiq.com/search/www	W.dscsc.ik												9 6 ×	• • •	• •
🔘 RISKIQ 🔍 V	ww.dscsc.lk														ours Upgrad	³⁰
	Registrar Registrart - Categorize															
- Cast Seen 2018-11-01	argootat 1													2018/01/2010/2018/	1-01	
DATA		2 3		6	4	18	4	10	0		0					
		Resolutions WHOIS				ponents	Host Pairs	OSINT	Hashes	DNS	Projects	Cookies				
LTERS O	COMPONENTS Ø															
ATEGORY (9/18)		1-18 of 18 Sort : Last See														nload Co
✓ X JavaScript Libr 6 ✓ X Server Module 3	Hostname		First 2016-03-20	Last 2018-	10-31		Category Server					Value			Tags	
 x Server Module 3 x Framework 2 			2018-04-04	2018-			Cryptocurrency 1	1 fines				Coin Hive				
X Server 2																
× CDN 1	www.dsc		2016-03-20	2018-			JavaScript Librar	y .				JQuery UI				
w More	u www.dsc	scik	2016-03-20	2018-			Framework					PHP (v5.3.3)				
ALUE (947.10)	O www.dsc	sc.lk	2013-01-20	2018-	10-31		JavaScript Librar	У				JQuery				
× Query 3	www.dsc	scik	2018-04-04	2018-	10-31		JavaScript Librar	y				twilio-js (vNA)				
X Apache 2	C www.dsc	sc.lk	2018-04-04	2018-	04-04		JavaScript Librar	У				JQuery Migrate				
r x PHP 2	www.dsc	scik	2017-01-20	2017-	03-21		JavaScript Librar	y				jQuery (v1.9.1)				
× glyphicons 1	u www.dsc	sc.lk	2017-01-20	2017-	03-21		CDN					JQuery CDN				
w More	o www.dsc	scik	2017-01-20	2017-	03-21		Web Design					glyphicons				
OSTNAME (1718)	www.dsc	scik	2016-03-20	2017-	01-11		JavaScript Librar	y				JQuery (v1.7.2)				
/ X www.dscsc.ik 18	www.dsc	scik	2013-01-08	2013-	01-29		Server Module					mod_bwlimited	(v1.4)			
NG	www.dsc	nr. lk	2013-01-08	2013-	01-29		Operating System	m				Unix				
YSTEM TAG			2013-01-08	2013-	01-29		Server Module					mod_ssl (v2.2.2				
			2013-01-06	2013-			Server					Apeche (v2.2.23				
			2013-01-08	2013-			Server Module									
	www.dsc											OpenSSL (v1.0.0	-fips)			
	www.dsc		2013-01-08	2013-			Framework					PHP (v5.2.17)				
	www.dsc	ac.lk	2013-01-20	2013-	01-20		CMS					Joomlal (v1.5)				
	1-18 of 18															-

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

> C i https://commu	nity.riskiq.com/search/www.conalvias.com					& * O & & & @
	ww.conalvias.com					Tours Upgrade 😯
	rgistrent -					
✓ X JavaScript Lib., 10	Hostname	First	Last	Category	Value	Tags
✓ × CDN 3	www.conalvias.com	2015-02-27	2018-10-31	Operating System	Red Hat	
✓ × Analytics Servi., 2 ✓ × Framework 2	www.conalvias.com	2015-02-27	2018-10-31	Server	Apache (v2.2.15)	
V X Tracking Pixel 2	www.conalvias.com	2015-02-27	2018-10-31	JavaScript Library	jqueryul (v1.9.2)	
how More	www.conalvias.com	2018-04-05	2018-10-31	Web Design	Font Awesome (v3.2.1)	
VALUE (01739)	www.conalvias.com	2015-11-30	2018-10-31	Tracking Pixel	Google Analytics	
√ × jQuery 3	www.conalvias.com	2018-10-31	2018-10-31	JavaScript Library	jQuery (vul)	
✓ X Google Analyti 2	www.conalvias.com	2017-03-12	2018-10-31	JavaScript Library	jquery.caroufredsel (v6.2.1)	
✓ X PHP 2 ✓ X Apache 1	www.conalvias.com	2018-09-28	2018-10-31	JavaScript Library	jQuery carouFredSel (v6.2.1)	
 X BootStrap CDN 1 	www.conalvias.com	2015-02-27	2018-10-31	CDN	Google Ajax CDN	
w More	www.conalvias.com	2017-03-12	2018-10-31	Tracking Pixel	www.conalvlas.com	
IOSTNAME (1725)	www.conalvias.com	2018-04-05	2018-10-31	CDN	Google Hosted Libraries	
 X www.conalvi 25 	www.conalvias.com	2015-02-27	2018-10-31	Ad Network	Google	
TAG	www.conalvias.com	2015-02-27	2018-10-31	CDN	BootStrap CDN	
SYSTEM TAG	www.conalvias.com	2015-02-27	2018-10-31	Analytics Service	Google Analytics (deprecated)	
	www.conalvias.com	2018-10-51	2018-10-31	Framework	PHP (V5.6.38)	
		2017-03-12	2018-10-31	lavaScript Library	PrettyPhoto	
		2015-02-27	2018-10-31	JavaScript Library	jQuery UI (v1.9.2)	
		2015-02-27	2018-10-31	Analytics Service	Google Analytics	
		2015-02-27	2018-10-10	Framework	PHP (v5.3.3)	
		2018-04-05	2018-10-10			
	www.conalvias.com			JavaScript Library	Dean Edwards Packer	
	www.conabilas.com	2018-04-05	2018-10-10	Cryptocurrency Miner	Coin Hive	
	www.conalvias.com	2018-04-05	2018-10-10	JavaScript Library	jQuery	
	www.conalvlas.com	2018-04-05	2018-10-10	JavaScript Library	twilio-js (vNA)	
	www.conalvias.com	2017-03-12	2018-10-10	CMS	Joomlal (v-)	
	www.conalvlas.com	2015-02-27	2017-04-28	JavaScript Library	JQuery (v1.11.0)	C
	1-25 of 26 >					

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

	nity.riskiq.com/search/www.awer-center.org					*o × •	ی 🍋 😫	-
	w.awer-center.org						Upgrade	0
	pitrar PDR Ltd. d/b/a Publ Categorize pitrant							
 × JavaScript Libr 6 	Hostname	First	Last	Category	Value		Тар	p.
/ X CM5 3	www.awer-center.org	2015-12-06	2018-10-31	Server	Apache (v2)			
× Wordpress Plu 3	www.awer-center.org	2018-05-06	2018-10-31	Framework	PHP (VS.3.25)			
× Publisher 2 × Tracking Pixel 2	www.awer-center.org	2016-08-10	2018-10-31	Search	Google Search			
v More	O www.awer-center.org	2018-06-03	2018-10-31	Social Network	Google+			
NLUE (21 / 25)	www.awer-center.org	2016-08-10	2018-10-31	Social Media	Twitter Widgets			
× WordPress 3	www.awer-center.org	2016-08-10	2018-10-31	Ad Exchange	Facebook			
X Query 2	www.awer-center.org	2018-06-03	2018-10-31	Wordpress Plugin	T(-) Countdown			
× jQuery Migrate 2 × Apache 1	www.awer-center.org	2015-12-06	2018-10-31	Tracking Pixel	www.awer-center.org			
× Contact Form 7 1	www.awer-center.org	2015-12-06	2018-10-31	JavaScript Ubrary	jQuery			
More	www.awer-center.org	2018-07-02	2018-10-31	JavaScript Library	(Query Migrate (v1.4.1)			
DSTNAME (1725)	O www.awer-center.org	2016-08-10	2018-10-31	Publisher	Pinterest			
X www.awer-ce., 25	www.awen-center.org	2018-07-02	2018-10-31	CVIS	WordPress (v4.5.3)			
us	O www.awer-center.org	2018-06-03	2018-10-31	Wordpress Plugin	Social Media Share Buttons & amp; Social Sharing Icons (Ultimate Sharing)			
STEM TAG	www.awer-center.org	2016-08-10	2018-10-31	Publisher	Twitter Ads			
	· www.awer-center.org	2016-08-03	2018-10-31	CVIS	WordPress (v6.3.1)			
	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	(Query Migrate (v1.2.1)			
	www.awer-center.org	2015-12-06	2018-10-07	CMS	WordPress (v3.9.1)			
	www.awer-center.org	2018-07-15	2018-10-07	Tracking Pixel	Facebook Pixel			
	www.awer-center.org	2018-05-06	2018-08-13	Web Design	Fort Awesome (v4.1.0)			
	www.awer-center.org	2018-05-06	2018-08-13	JavaScript Library	jQuery UI			
	O www.awer-center.org	2016-05-07	2018-08-13	Ad Network	Google			
	www.awer-center.org	2018-05-06	2018-08-13	JavaGcript Library	Owl Carousel			
	o 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)			
								6

	www.awer-center.org					🗞 ★ O	Upgrade	0
Rest Seen 2014-07-26	Registrar POR Lod. d'Ara Publi Registrant							
ATEGORY (10/23)	[Seen Descending *					Download	d Copy
 X JavaScript Libr 7 	Hostname	fint	Last	Category	Value		Tega	
/ × CMS 5	 www.awer-center.org 	2018-05-06	2018-08-13	Cryptocurrency Miner	Coin Hive			
r X Tracking Pixel 3	www.awer-center.org	2017-03-20	2018-08-13	Online Videos	YouTube			
/ X CDN 2	 www.awer-center.org 	2017-03-20	2018-08-13	CDN	YouTube CDN			
w More	www.awer-center.org	2017-03-20	2018-08-13	JavaScript Library	(Query (v1.11.1)			
ALUE (197.20	www.awer-center.org	2018-05-06	2018-08-13	JavaScript Library	twilio-js (vNA)			
r x joomial 3	www.awer-center.org	2017-06-01	2018-08-13	JavaScript Library	jQuery Migrate			
r X jQuery 3	www.awer-center.org	2018-06-23	2018-08-12	Tracking Posel	Twitter Ads			
/ X Blogger 1	www.awer-center.org	2016-08-03	2018-07-28	Tracking Pixel	Facebook			
 × BootStrap CDN 1 × Coin Hive 1 	www.awer-center.org	2017-03-20	2018-05-16	CVIS	joomial (v1.7.3)			
w More	O www.awer-center.org	2018-05-10	2018-05-16	OVS	joomlat (v3.3)			
OSTNAME (1723)	o www.awer-center.org	2017-03-20	2018-05-13	OVS	joornial (v-)			
/ × www.awer-ce 23	www.awer-center.org	2018-05-10	2018-05-10	lavaScript Library	(Query (vm)grate-1.2.1)			
AG		2018-05-10	2018-05-10	JavaScript Library	(Query (v2.1.1)			
YSTEM TAG		2018-05-05	2018-05-08	JavaScript Library	selectiviar (v1.0.2)			
	www.awer-center.org	2017-03-20	2018-05-08	JavaScript Library	Respond (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 - Double Click			
	 www.awer-center.org 	2015-12-06	2017-08-31	Framework	PHP (v5.3.19)			
	 www.awer-center.org 	2015-12-06	2017-08-31	CVIS	WordPress			
	o www.awer-center.org	2016-01-02	2016-11-18	Tracking Pixel	www.paypalobjects.com			
	www.awer-center.org	2016-05-07	2016-05-07	Analytics Service	StatCounter			
	www.awer-center.org	2016-05-07	2016-05-07	OVS	Blogger			

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

🔘 RISKIQ 🔍 🛛	ww.cooperativataulabe.hn				Tours Upgrade 🕢
	ngistrar Baro Internacional d				
	Si 1 1 1 1 1 1 Nay Jun		Aug	Sep Oct	
					2018 2018-04-23 to 2018-11-01
ата	3 2 0 Resolutions WH0KS Certificate	6 2 Subdomains Trackers	14 4 Components Host Pairs	6 0 0 0 2 DSINT Hashes DNS Projects Cookles	
LTERS 0	COMPONENTS () . Show : 25 < 1-14 of 14 > Sort : Last Seen Descending *				Download Copy
 × JavaScriptLibr 3 	Hostname	First	Last	Category Value	Tags
 X Server Module 3 	 www.cooperativataulabe.hn 	2017-02-22	2018-10-31	Server Module PHP (v	5.4.16)
√ × CMS 2	www.cooperativataulabe.hn	2018-09-05	2018-10-31	Server Module mod_6	rgid (v2.3.9)
Ad Network 1	www.cooperativataulabe.hn	2017-02-22	2018-10-31	Server Apach	t (v2.4.6)
X Analytics Seni 1 ow More	www.cooperativataulabe.hn	2018-09-05	2018-10-31	Server Module OpenS	SL (v1.0.2k-fips)
VALUE (00/14)	www.cooperativataulabe.hn	2017-02-22	2018-10-31	Operating System ContO	5
 X CentOS 2 	www.cooperativataulabe.hn	2018-09-05	2018-10-31	JavaScript Library IQuery	(v3.3.1.slim)
√ × joomiał 2	www.cooperativataulabe.hn	2017-02-22	2018-10-31	Framework PHP (v	
r ≍ jQuery 2	www.cooperativataulabe.hn	2017-02-22	2018-10-31	JavaScript Library IQuery	
✓ X PHP 2 ✓ X Apache 1	www.cooperativataulabe.hn	2017-02-22	2018-07-28		e (v1.7.3)
w More 1		2018-07-28	2018-07-28	Cryptocurrency Miner Cole H	
HOSTNAME (1714)		2017-02-22	2018-07-28	Ad Network Google	
✓ X www.cooper 14		2018-07-28	2018-07-28	JavaScript Library twilio-	
TAG		2017-02-22	2017-04-27	CVS Joomia	
SYSTEM TAG	www.cooperativataulabe.hn	2017-02-22	2017-03-29	Analytics Service Centrol	
	1-14 of 14				C

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

	w.renovacaocari	smatica.com.br	0											Upgrade	0
	jstrar jstrant - Catego														
		2 Resolutions	WHOIS	6 Certificate	4 Subdomains	2 Trackers	20 Components	5 Host Pairs	OSINT	0 Hashes	DNS	0 Projects	3 Cookies		
TERS O	COMPONENTS (,													
ATEGORY (13/20)	. • Show: 25	+ 1-20 of 20 ► Sor	t : Last Seen D	escending *										Downloa	d Cog
× Server Module 5	Hestname					Box	Last		Category				Value	Tag	s
× CMS 2	www.ren	ovacaocarismatica.com.b				2016-06-14	2018-1	ka1	Server				Apache		
× JavaScript Libr 2	· www.ren	ovacaocarismatica.com.b				2018-07-09	2018-1	1-10	Framework	k			PHP (v5.3.29)		
X Server 2	O www.ren	ovacaocarismatica.com.b				2018-10-08	2018-1	>10	CMS				Joomial (v3)		
× Ad Exchange 1	· www.ren	ovacaocarismatica.com.b				2018-07-09	2018-1	-10	Ad Networ	k			Google		
ALUE (18/20)		ovacaocarismatica.com.b				2018-07-09	2018-1	F10	JavaScript I	Ubrary			jQuery		
X Apache 2		ovacaocarismatica.com.b				2018-07-09	2018-0	-09	Online Vide	eos			YouTube		
× joomlel 2		oveceocerismetice.com.b				2018-07-09	2018-0	149	JavaScript I	Library			twilio-js (vNA)		
X Coin Hive 1		oveceocarismatice.com.b				2018-07-09	2018-0	-09	CNS				joomlal (v1.7.3)		
X Fort Awesome 1		ovacaocarismatica.com.b				2018-07-09	2018-0		CDN				YouTube CDN		
× FrontPage 1		ovacaocarismatica.com.b				2018-07-09	2018-0		Search				Google Search		
OSTNAME (1720)						2018-07-09	2018-0								
× www.renova 20		ovacaocarismatica.com.b							Cryptocum				Coin Hive		
AG		ovacaocarismatica.com.b				2018-07-09	2018-0		Web Desig				Fort Awesome (v3.1.0)		
	· · · · · · · · · · · · · · · · · · ·	ovacaocarismatica.com.b				2018-07-09	2018-0	-09	Ad Exchang	80			Google Ads - DoubleClick		
YSTEM TAG	C www.ren	ovacaocarismatica.com.b				2012-08-07	2012-0	1-07	Server Mor	dule			mod_ssl (v2.2.22)		
	· www.ren	ovacaocarismatica.com.b				2012-08-07	2012-0	1-07	Operating	System			Unix		
	0 www.ren	ovacaocarismatica.com.b				2012-08-07	2012-0	1-07	Server Mor	dule			mod_auth_passthrough (v2.1)		
	· www.ren	ovacaocarismatica.com.b				2012-08-07	2012-0	1-07	Server Mor	dule			FrontPage (v5.0.2.2635)		
		ovacaocarismatica.com.b				2012-08-07	2012-0	147	Server Mor	dule			mod_bwlimited (v1.4)		
	www.ren	ovacaocarismatica.com.b				2012-08-07	2012-0	1-07	Server Mor	dule			OpenSSL (v1.0.0 fips)		
		ovacaocarismatica.com.b				2012-08-07	2012-0	1-07	Server				Apache (v2.2.22)		
	1-20 of 20														-

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

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

> C iii https://commu	unity.riskiq.com/search/www.broadripplelock.com					<u></u> ★ ○ № -% ● @
	ww.broadripplelock.com					Teurs Upgrade 🕑
	Registrant GODADDV.COM, LLC Categorize Registrant Broad Ripple Lock					
CATEGORY (14725)	[□•] Show: 25 • 1-25 of 27 • Sort: Last Seen Desce	nding *				Download Copy
√ × CM5 3	Hestname	First	Last	Category	Value	Tags
✓ X Framework 3	 www.broadrippielock.com 	2018-04-22	2018-10-31	Content Management	Plesk	
✓ X JavaScript Libr 3	www.broadrippielock.com	2016-10-12	2018-10-31	Server	Apache (v2.2.3)	
✓ X Tracking Pixel 3 ✓ X Analytics Servi., 2	www.broadripplelock.com	2016-10-12	2018-10-31	Operating System	CentOS	
how More	www.broadrippielock.com	2017-12-26	2018-10-31	Framework	PHP (v5.4.45)	
VALUE (20/25)	 www.broadrippielock.com 	2016-10-28	2018-10-31	CVIS	joomlal (v-)	
✓ X Joomial 3	www.broadripplelock.com	2016-10-28	2018-10-31	Ad Network	Google	
✓ X CentOS 2	www.broadripplelock.com	2015-11-27	2018-10-31	Tracking Pixel	www.broadripplelock.com	
✓ × Google Analyti 2 ✓ × PHP 2	www.broadripplelock.com	2016-10-28	2018-10-31	JavaScript Library	JQuery	
v × Apache 1	www.broadripplelock.com	2017-10-16	2018-10-31	Web Design	Fort Awesome (v3.2.1)	
how More	www.broadripplelock.com	2016-10-28	2018-10-31	Analytics Service	Google Analytics	
HOSTNAME (1725)	www.broadripplelock.com	2017-05-20	2018-10-31	JavaScript Library	Query Migrate	
✓ X www.broadri 25	www.broadripplelock.com	2018-08-02	2018-10-31	OVS	joomlal (v3.4)	
TAG	www.broadripplelock.com	2016-10-28	2018-10-31	Tracking Pixel	Google Analytics	
SYSTEM TAG	www.broadripplelock.com	2016-10-28	2018-10-10	CVIS	joomla! (v1.7.3)	
		2018-07-12	2018-09-28	Advertising	AppNexus	
		2018-07-12	2018-09-28	000	Promote	
		2018-08-02	2018-08-29	Search		
					Google Maps	
	www.broadripplelock.com	2018-08-02	2018-08-29	Search	Google Search	
	www.broadripplelock.com	2017-10-16	2018-04-22	JavaScript Library	twillo-js (vNA)	
	 www.broadripplelock.com 	2017-10-16	2018-04-22	Cryptocurrency Miner	Coin Hive	
	www.broadripplelock.com	2016-10-12	2017-10-24	Framework	PHP (v5.4.20)	
	www.broadrippielock.com	2016-10-12	2017-04-05	Analytics Service	CentOS	
	www.broadripplelock.com	2015-07-09	2016-09-25	Framework	ASP.NET	
	 www.broadrippielock.com 	2015-07-09	2016-09-25	Server	Microsoft-IIS (v6.0)	
	www.broadripplelock.com	2015-11-27	2016-09-25	Tracking Pixel	counter.hitslink.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

	astercardconclerge.globalairportconclerge.com				Tours	Upgrade 🕤
First Seen 2012-09-21 Re	gitarar TuCows DoMAINS I gitarar: Centest Hivey Inc □ Stream 25 - 125 of 42 - Sort Last Seen Descending -					Download Coy.
✓ X JavaScript Libr 9 ✓ X Framework 4 ✓ X Server 4	Hostnome mastercardconcierge.globalairportconcierge.com	Regt 2015-11-21	Last 2018-10-31	Category Framework	Volue ASP.NET	Tags
✓ X Ad Exchange 1 ✓ X Ad Network 1	mastercardconcierge.globalairportconcierge.com mastercardconcierge.globalairportconcierge.com	2018-10-10 2018-06-27	2018-10-31	Server JavaScript Library	Microsoft-IIS (v10.0) jQuery	
VALUE (167.25)	mastercardconcierge.globalairportconcierge.com mastercardconcierge.globalairportconcierge.com	2015-11-21 2015-12-09	2018-10-31	JavaScript Library Framework	JQuery UI PHP (v5.3.28)	
✓ X Query 5 ✓ X Microsoft+IS 3	mastercardconcierge.globalairportconcierge.com mastercardconcierge.globalairportconcierge.com	2014-04-09 2018-10-10	2018-10-31	JavaScript Library Hosting Provider	JQuery UI (v1.8.16) Microsoft Azure	
✓ X PHP 3 ✓ X QueryUI 2 ✓ X Apache 1	mastercardconcierge.globalairportconcierge.com mastercardconcierge.globalairportconcierge.com	2017-05-20 2018-03-19	2018-10-31 2018-10-31	JavaScript Library JavaScript Library	jQuery Migrate SWFObject	
ow More	mastercandconcierge.globala/rportconcierge.com mastercandconcierge.globala/rportconcierge.com	2015-12-09	2018-06-28	Server Ad Exchange	Microsoft-IIS (v8.5) Facebook	
✓ X mastercardc 25 TAG	mastercardconcierge.globalairportconcierge.com	2018-03-03	2018-03-03	Cryptocurrency Miner	Coin Hive	
SYSTEM TAG	mastercardconcierge.globalairportconcierge.com mastercardconcierge.globalairportconcierge.com	2017-06-20	2017-06-20	JavaScript Library	jQuery CDN jQuery (vlatest)	
	mastercardconcierge.globalairportconcierge.com mastercardconcierge.globalairportconcierge.com	2016-06-22 2016-01-21	2017-06-20	Analytics Service JavaScript Library	DoubleClick Roodlight	
	mastercardconcierge globala/portconcierge.com mastercardconcierge.globala/portconcierge.com	2015-11-24 2015-11-24	2017-02-20 2017-02-20	Ad Network JavaScript Library	Geogle (Query (v1.11.0)	
	mastercardconcierge.globalairportconcierge.com mastercardconcierge.globalairportconcierge.com	2015-11-21 2015-11-21	2015-12-02	Server Framework	Microsoft-IS (v7.5) PHP (v5.4.24)	
	mastercardconcierge.globalairportconcierge.com	2014-04-09	2014-04-09	Server Operating System	Apache (v2.2.15) CentOS	
	mastercardconcierge_globalis/rportconcierge.com mastercardconcierge_globalis/rportconcierge.com	2014-04-09	2014-04-09	Framework	PHP (v5.3.3)	
	mastercardconcierge.globalairportconcierge.com mastercardconcierge.globalairportconcierge.com	2014-04-09	2014-04-09	CMS JavaScript Library	ExpressionEngine (Query (v1.6.4)	6

PHP but no Joomla this time.

	astercardconcierge.glob		lairportconcierge.com											🗞 ★ O	Upgrade	0
	ginur Tuccus Soukuns L. ginur Causa Hway Na															
	50 3 60 5 70 7 70 3 77 3 7 7 4 7 7 7 8 7 8 7 8 8 7 8 8 7 8 7 8 7 8 7	1 1 5 1 1 5 2 3 5 3 3 5 4 5 5 5 5 5 6 5 5 7 5 5 6 5 5 7 5 5			5 4 5 4 5 4 5 4 5 4 5 4 5 4 5 4 5 4 5 4 5 4 5 4 5 4 5 4	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 Xet 1 1 1 1 1 1		1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 3 5 p	- -			1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Nov			
														2018-04-29 to 2018-11	01	
ATA		4 Resolutions	S 0 WHOIS Certificate	30 Subdomains	1 Trackers	29 Components	10 Host Pairs	10 OSINT	0 Hashes	2 DNS	0 Projects	10 Cookles				
TERS θ	COMPONENTS 0 [19 of 29 + Sort : 1	ast Seen Descending												Download	d Copy
× CDN 1	Hostname					First		Last		Category			Value		Taga	
* X CMS 1	mastercardconcie	erge.globalairportcon	clerge.com			2014-04-0	0	2014-04-09		OVS			Wordpress			
× DMP 1	mastercardconcierge.globalairportconcierge.com					2014-04-0	2014-04-09 2014-04-09			DMP			Adobe Marketing	loud		
× JavaScript Libr 1	mastercardconcierge.globala/rportconcierge.com					2014-04-0	2014-04-09 2014-04-09			JavaScript Library			jqueryul (v1.8.16)			
ALUE (474)	mastercardconcie	irge.globalairportcom	lerge.com			2014-04-0	9	2014-04-09		CDN			Google Ajax CDN			
× X Adobe Market 1 × X Googla Ajax C 1 × X jouennum × X jouennum × Vordgress 1 × X Wordgress 1 × X Wordgress 4 × X maskerCandoo 4 rag v X maskerCandoo 4	26-22 of 23 +															

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.



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

- ✓ sales@riskiq.net
- **L** 1888.415.4447

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