



# An E-commerce Guide:

## 12 Ways to Unmask Cyber Threats This Holiday Shopping Season



## This Holiday Shopping Season, Threat Actors Look For a Haul

Every year, bad actors capitalize on holiday shopping e-commerce trends. They use the brand names of leading e-tailers to fool shoppers looking for holiday shopping deals, sales, and coupons, luring them to fake mobile apps and websites.

- A recent consumer survey conducted by RiskIQ found that **83% of people** will spend at least **50% of their budget** online.
- Last year, [RiskIQ observed a 20% increase in total blocklisted apps](#) leading up to Black Friday and Cyber Monday. Of all apps found by searching for terms related to holiday shopping, 951, or 2%, were blocklisted as malicious.
- The top-10 most trafficked sites on Thanksgiving weekend had a total of **6,353 blocklisted mobile apps** containing their branded terms in the title or description.
- All mobile apps for the top-five 'Elite' retailers in the U.K. had a combined total of **24 blocklisted apps** that contained their branded terms in the title or description.
- RiskIQ detected **65 incidents** of domain infringement across the top-10 most trafficked sites on Black Friday weekend.



The holiday shopping season has become a crucial period for e-commerce and a cornerstone of online shops' annual revenue. [Adobe Analytics predicts](#) online holiday shopping to reach a record \$910 billion in 2021, projecting U.S. e-commerce sales to grow 10% year-over-year between November and December. [eMarketer forecasts](#) total U.S. retail sales to rise 9% to \$1.147 trillion this holiday season, with retail e-commerce accounting for 18.4% of total sales, climbing 14.4% to \$211.66 billion.

With online spending this holiday shopping season projected to set yet another record, e-commerce is squarely in the crosshairs of cybercriminals who want a piece of the pie. In our [2020 Holiday Shopping Threat report](#), RiskIQ researchers found hundreds of threats against the 10-most trafficked e-commerce sites via mobile and the web in the U.S. and U.K., including phishing, domain infringement, malicious mobile apps, and scams.

However, despite cybercriminals becoming more numerous and more sophisticated, you don't need a holiday miracle to keep your brand and your organization safe. There are dozens of ways to determine if malicious actors are targeting your brand, helpful to beginners and seasoned cybersecurity pros alike.

Phishing and other malicious sites have distinct characteristics we can use to identify and defeat them. Whether you're a seasoned cybersecurity pro or just a beginner, these twelve red flags can help you determine which sites, apps, and URLs are nice and which may be naughty.

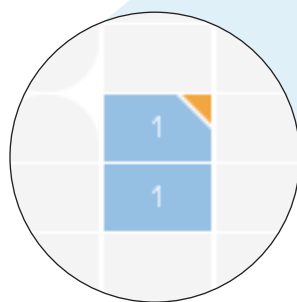
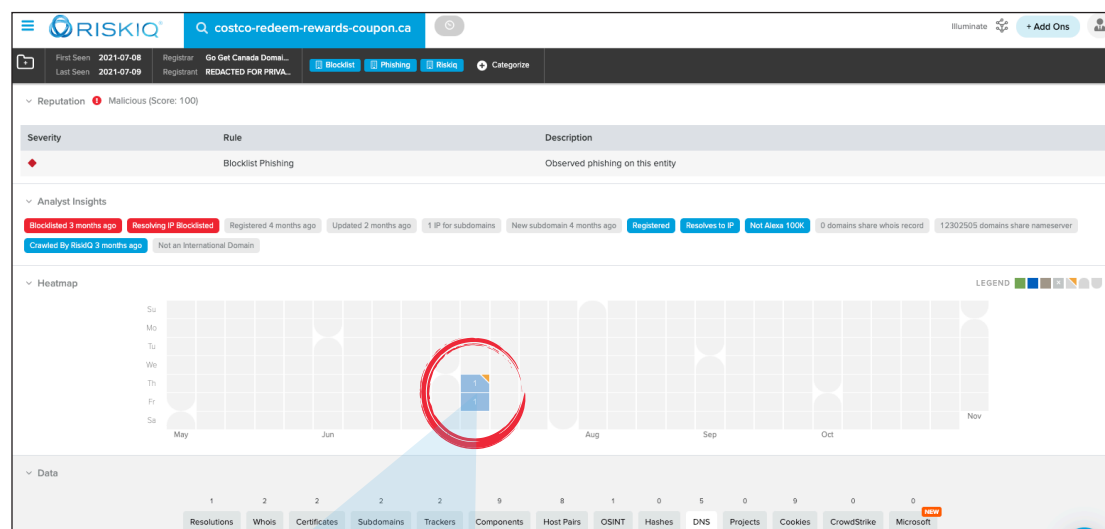
# This Holiday Shopping Season, be Wary of These **12 Red Flags**:

1

## A website has been up for only a short period

Threat actors are standing up new websites every second to fool their victims. When a website's DNS shows that it's only been resolving for a short period, it fits the mold of threat infrastructure.

In this example, a malicious site was only resolving to an IP address for about a day in July.



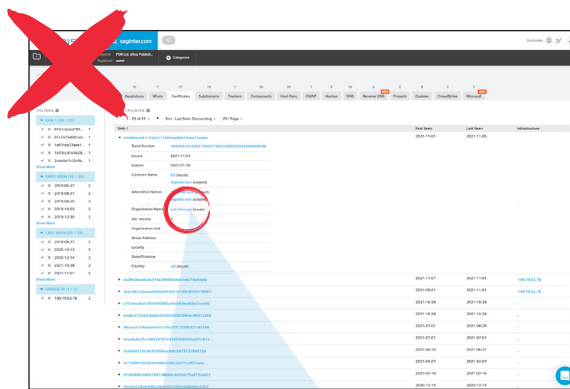
2

## A website has an SSL certificate from a free certificate authority

Threat actors often quickly spin up cheap infrastructure to commit attacks at scale. Free certificate authorities provide SSL certificates that help their malicious sites appear legitimate at a cursory glance. When a site has one of these free certs, it's a good idea to take a closer look.

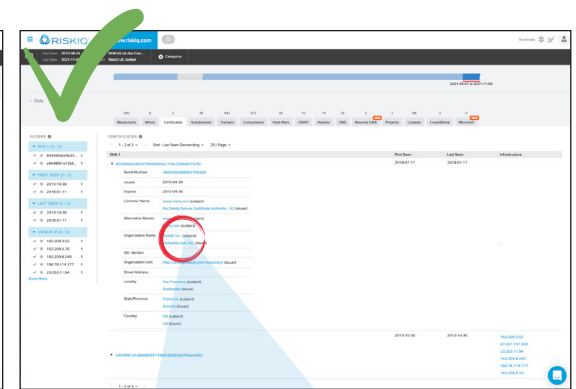
In this example, you can tell which is the legitimate certificate and which is the dubious, self-signed certificate by looking at the issuer. 'Let's Encrypt' is a free resource often abused by cybercriminals to build their infrastructure. GoDaddy Secure Certificate Authority is much more legitimate.

### Free certificate:



Alternative Names	*.saginter.com (subject)
Organization Name	Let's Encrypt (issuer)
SSL Version	3
Organization Unit	
Address	

### Paid certificate:



Alternative Names	www.riskiq.com (subject)
Organization Name	RiskIQ, Inc. (subject)
SSL Version	3
Organization Unit	http://certs.godaddy.com
Address	San Francisco

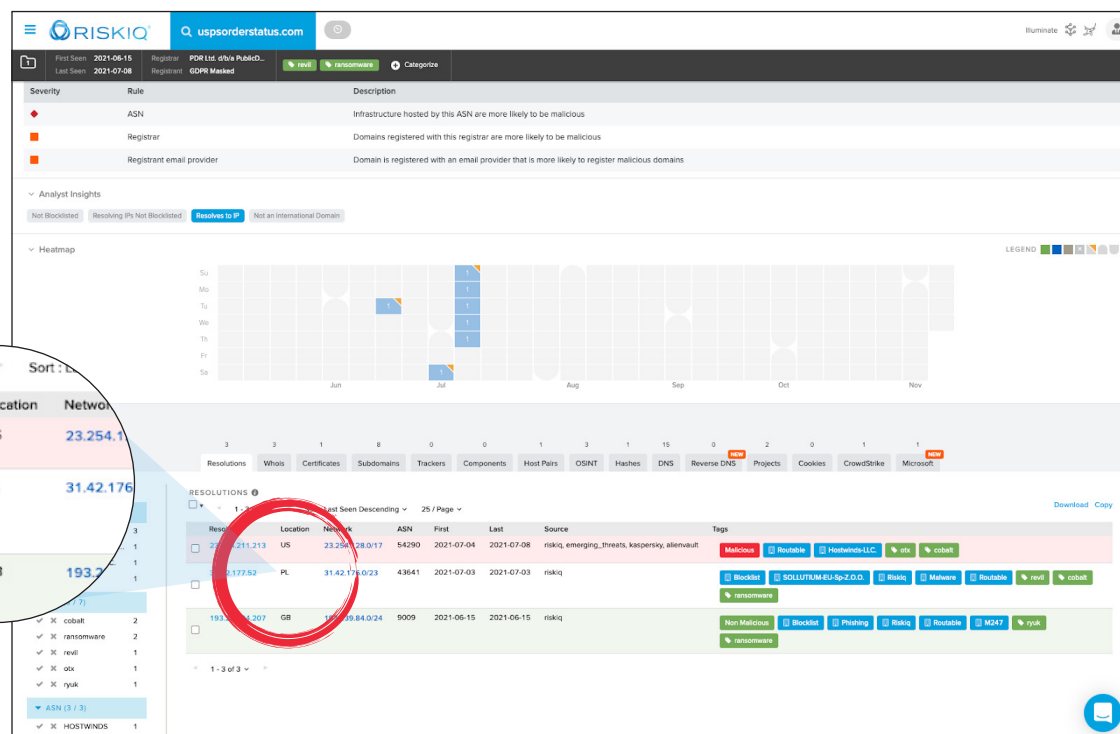


3

## A domain is hosted in a country you're not expecting

Check the domain registration of a website. If it's registered in a country you wouldn't expect, it's likely a malicious site. For example, if a supposed American e-commerce site was stood up in Russia, that's a major red flag.

We should expect a domain from the United States Postal Service to originate in the United States. However, historical records of `uspsorderstatus[.]com`, a malicious domain imitating the USPS, shows it coming from Poland and Great Britain IP addresses.



## 4

## The site is a copy from elsewhere

Threat actors copy legitimate sites component-for-component to make their phishing sites look as authentic as possible. Often, they'll use free software like HTTrack to make these duplicates. If a site has an HTTrack or [mark of the web](#), proceed with caution.

In this example, inside RiskIQ PassiveTotal, we see this malicious site has trackers denoting it was copied from the genuine site via HTTrack.

The screenshot shows the RiskIQ PassiveTotal interface for the domain 'costco-redeem-rewards-coupon.ca'. The 'Trackers' tab is selected, displaying a table of trackers. A red circle highlights the 'HTTrackSourceHost' and 'HTTrackSourceWebsite' trackers, which are circled in white. The interface includes filters, a table of trackers, and a sidebar with navigation options.

Hostname	First	Last	Type	Value	Tags
costco-redeem-rewards-coupon.ca	2021-07-09	2021-07-09	HTTrackSourceHost	www1.royalbank.com	Blocklist, Phishing, RiskIQ
costco-redeem-rewards-coupon.ca	2021-07-09	2021-07-09	HTTrackSourceWebsite	www1.royalbank.com/cgi-bin/ibaccess/ibcg3m01	Blocklist, Phishing, RiskIQ

5

## Open-source intelligence (OSINT) says it's bad

Threat researchers worldwide work around the clock hunting threats and identifying threat actors and their tools. A plethora of open-source intelligence is available that could offer valuable insight into a site's reputation or associations with threat infrastructure, e.g., if it's been put on a blocklist.

**RiskIQ's Threat Intelligence Portal (TIP) curates intelligence from around the world and adds context from its global collection network. This example shows intelligence articles and indicators of compromised (IOCs) related to Kaseya ransomware.**

The screenshot shows the RiskIQ Threat Intelligence Portal (TIP) interface. At the top, there is a search bar with the query 'kaseya' and a 'Search Options' link. Below the search bar, the results are categorized under 'PassiveTotal Intelligence'. The main section is titled 'kaseya' and includes several expandable sections: 'Cyber Threat Intelligence (0)', 'Organizations (1)', 'Whois Organization (0)', 'Certificates (64)', 'Tags (0)', 'Components on Hosts (208)', 'Components on IPs (938)', and 'Deep & Dark Web (20)'. The 'Organizations (1)' section is expanded, showing a table with the following data:

Focus	Industry	Total Assets	Actions
Kaseya Limited	Software	62.5K	<a href="#">View Details</a>

Below the table, there is a 'View Record' button. At the bottom of the 'Organizations (1)' section, there is a link to 'Less Common Searches' with sub-links for 'Tags', 'Cert Issuer', 'Whois Address', and 'Whois Name'.

The screenshot shows the 'RiskIQ Articles (3)' section. Three articles are listed, each with a title, a brief description, and a set of tags. Red arrows point to the first three articles:

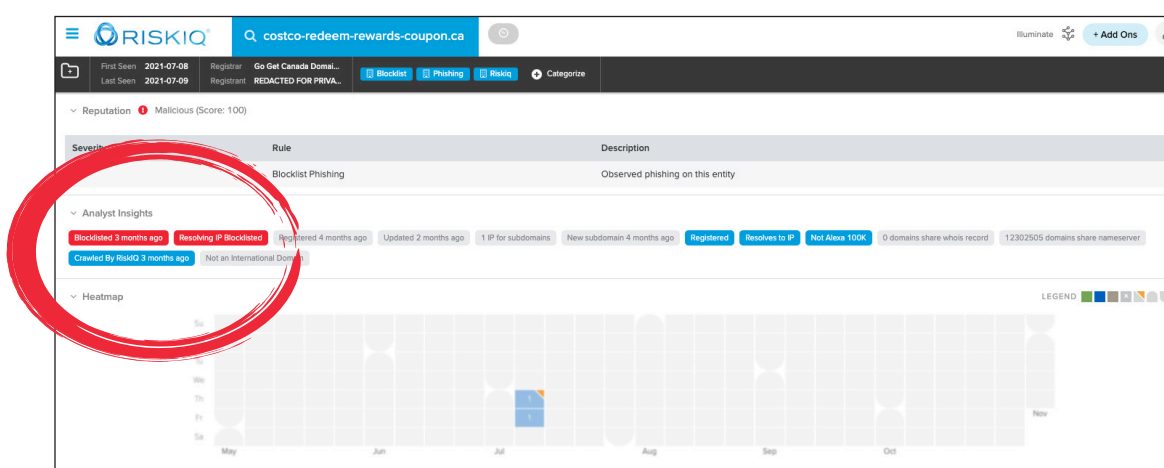
- Diving Deeper into the Kaseya VSA Attack: REvil Returns and Other Hackers Are Riding Their Coattails** (14 Indicators: 8 Public, 6 RiskIQ). On July 28th, a massive ransomware attack was launched against roughly 50 managed services providers by criminals associated with the REvil ransomware-as-a-service group. The attack leveraged the on-premises servers deployed by IT Management Software vendor Kaseya. The attackers found an...  
Created 4 Months Ago  
Tags: REvil, Kaseya, CVE-2021-30116, TrustWave, Ransomware
- Fake Kaseya VSA Security Update Drops Cobalt Strike** (26 Indicators: 9 Public, 17 RiskIQ). Threat actors are planting Cobalt Strike backdoors by masquerading a bogus Microsoft update along with a SecurityUpdates.exe. A malware spam campaign is milking the Kaseya ransomware attacks against its Virtual System/Server Administrator (VSA) platform to spread a link pretending to be a Micro...  
Created 4 Months Ago  
Tags: Phishing, CobaltStrike, Malwarebytes, Kaseya, Microsoft, ThreatPost, Ordris
- CISA-FBI Guidance for MSPs and their Customers Affected by the Kaseya VSA Supply-Chain Ransomware Attack** (0 Indicators: 0 Public). CISA and the FBI continue to respond to the recent supply-chain ransomware attack leveraging a vulnerability in Kaseya VSA software against multiple managed service providers (MSPs) and their customers. CISA and FBI strongly urge affected MSPs and their customers to follow the guidance in this ar...  
Created 4 Months Ago  
Tags: SupplyChain, Kaseya, MSP, CISA, Ransomware

## 6

## A site is known, and it has a bad reputation

Cybersleuths wanting to go beyond OSINT can use tools that curate threat intelligence and other data to develop a reputation for malicious sites and apps that have been seen in the wild. By looking up a suspicious URL, you may be able to instantly know if the site in question has a good or bad reputation.

**In this example, we see a phishing page that's shown to have been blocklisted three months ago.**





## 7

## The site associates with known bad actors

Some say a person is judged by the company they keep. Websites and apps are no different. Even if nothing is known about a particular site or app, there may be a rap sheet about its associated web infrastructure, like a domain or IP. Free tools that map the web's infrastructure can show if a site links to IPs, domains, or another piece of web infrastructure that is known to be linked to a threat actor group.

Here, in RiskIQ PassiveTotal, we're looking at an IP address that a phishing page resolved to. Exploring that IP, we see several other domains resolving to it, including a page that's been blocklisted for phishing.

Filters: RECORD TYPE (3 / 5): SOA (2), NS (2), MX (1). VALUE (4 / 5): dns1.registranse... (2), dns2.registranse... (1), hostmaster@regl... (1), costco-redeem-r... (1).

Value	First	Last	Type	Tags
<input type="checkbox"/> dns2.registrar-servers.com	2021-07-08	2021-07-08	NS	
<input type="checkbox"/> dns1.registrar-servers.com	2021-07-08	2021-07-08	SOA	
<input type="checkbox"/> dns1.registrar-servers.com	2021-07-08	2021-07-08	NS	
<input type="checkbox"/> hostmaster@registrar-servers.com	2021-07-08	2021-07-08	SOA	
<input type="checkbox"/> costco-redeem-rewards-coupon.ca	2021-07-08	2021-07-08	MX	

Buttons: Blocklist, Phishing, Risks.

## A site is registered to a person and not a company

Check the WHOIS information of a website. If the registrant isn't the company you're expecting, e.g., Walmart, it should be viewed with suspicion. It's especially suspicious when the registrant is an individual with a private email address, e.g., hotmail.com.

Here, we're looking at a phishing page purporting to be from NBC. However, the registrant isn't NBC, but rather something called 'Wuxi Tillian LLC.' This site is almost guaranteed to be bad news.

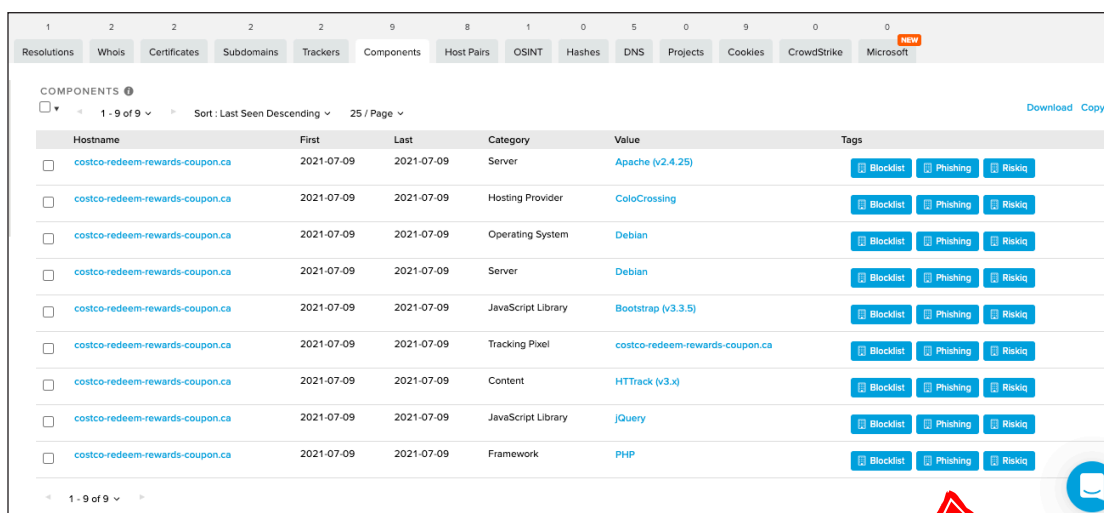
The screenshot shows the RiskIQ rsn.bcpost.com interface. At the top, there's a navigation bar with the RiskIQ logo and a search bar. Below the navigation bar, there's a calendar view showing the domain's registration history. The main content area displays the domain details for Wuxi Yilian LLC, including its status, contact information, and a list of records. A red circle highlights the 'Name' field in the 'Registrant' section, which is 'Wuxi Yilian LLC (registrant, admin, tech)'. The page also displays a detailed view of the domain status and contact information.

## 9

## A site shares components with known threat infrastructure

Threat actors are efficient and reuse their tooling to spin up malicious sites and apps as quickly and prolifically as possible. As a result, websites targeting your brand this holiday shopping season will likely share web components like tracking pixels with other malicious sites. Tools that map the infrastructure of the web will show you which other sites share these components. You can then check the reputation of these sites that share components with the site in question.

In this example, we're taking a closer look at a phishing page and can see that many of the components that comprise it are part of other phishing pages. We can see in RiskIQ PassiveTotal that they've been tagged as phishing infrastructure.



1	2	2	2	2	9	8	1	0	5	0	9	0	0	new
Resolutions	Whois	Certificates	Subdomains	Trackers	Components	Host Pairs	OSINT	Hashes	DNS	Projects	Cookies	CrowdStrike	Microsoft	
COMPONENTS														
1 - 9 of 9														
Sort: Last Seen Descending														
25 / Page														
Download Copy														
Hostname	First	Last	Category	Value	Tags									
costco-redeem-rewards-coupon.ca	2021-07-09	2021-07-09	Server	Apache (v2.4.25)	Blocklist Phishing RiskIQ									
costco-redeem-rewards-coupon.ca	2021-07-09	2021-07-09	Hosting Provider	ColoCrossing	Blocklist Phishing RiskIQ									
costco-redeem-rewards-coupon.ca	2021-07-09	2021-07-09	Operating System	Debian	Blocklist Phishing RiskIQ									
costco-redeem-rewards-coupon.ca	2021-07-09	2021-07-09	Server	Debian	Blocklist Phishing RiskIQ									
costco-redeem-rewards-coupon.ca	2021-07-09	2021-07-09	JavaScript Library	Bootstrap (v3.3.5)	Blocklist Phishing RiskIQ									
costco-redeem-rewards-coupon.ca	2021-07-09	2021-07-09	Tracking Pixel	costco-redeem-rewards-coupon.ca	Blocklist Phishing RiskIQ									
costco-redeem-rewards-coupon.ca	2021-07-09	2021-07-09	Content	HTTrack (v3.x)	Blocklist Phishing RiskIQ									
costco-redeem-rewards-coupon.ca	2021-07-09	2021-07-09	JavaScript Library	jQuery	Blocklist Phishing RiskIQ									
costco-redeem-rewards-coupon.ca	2021-07-09	2021-07-09	Framework	PHP	Blocklist Phishing RiskIQ									
1 - 9 of 9														



10

## A site doesn't have much attached to it

As we've mentioned, threat actors move quickly and don't like to spend much time on an individual malicious site. As a result, many sites spun up to phish users or fool them into downloading malware will be spartan, with very few components attached to them compared to typical, reputable websites. For example, if a site you think is reputable lacks tracking pixels or plug-ins, it is likely not what it appears to be.



In the examples below, we see the same phishing page as in red flag number 9 next to a legitimate site, ours. You can see all the components that come together to make a legitimate business site and how many of them are conspicuously absent in the phishing page.

Phishing page:

Item	File	Last	Category	Value	Type
<input type="checkbox"/>	cdn.cloudflare.com	2021-07-09	2021-07-09	Server	cdn.cloudflare.com
<input type="checkbox"/>	cdn.cloudflare.com	2021-07-09	2021-07-09	Hosting Provider	cdn.cloudflare.com
<input type="checkbox"/>	cdn.cloudflare.com	2021-07-09	2021-07-09	Operating System	cdn.cloudflare.com
<input type="checkbox"/>	cdn.cloudflare.com	2021-07-09	2021-07-09	Server	cdn.cloudflare.com
<input type="checkbox"/>	cdn.cloudflare.com	2021-07-09	2021-07-09	JavaScript Library	cdn.cloudflare.com
<input type="checkbox"/>	cdn.cloudflare.com	2021-07-09	2021-07-09	Tracking Pixel	cdn.cloudflare.com
<input type="checkbox"/>	cdn.cloudflare.com	2021-07-09	2021-07-09	Content	cdn.cloudflare.com
<input type="checkbox"/>	cdn.cloudflare.com	2021-07-09	2021-07-09	JavaScript Library	cdn.cloudflare.com
<input type="checkbox"/>	cdn.cloudflare.com	2021-07-09	2021-07-09	Font	cdn.cloudflare.com

Legitimate page:

Item	File	Last	Category	Value	Type
<input type="checkbox"/>	cdn.cloudflare.com	2021-07-09	2021-07-09	Server	cdn.cloudflare.com
<input type="checkbox"/>	cdn.cloudflare.com	2021-07-09	2021-07-09	Hosting Provider	cdn.cloudflare.com
<input type="checkbox"/>	cdn.cloudflare.com	2021-07-09	2021-07-09	Operating System	cdn.cloudflare.com
<input type="checkbox"/>	cdn.cloudflare.com	2021-07-09	2021-07-09	Server	cdn.cloudflare.com
<input type="checkbox"/>	cdn.cloudflare.com	2021-07-09	2021-07-09	JavaScript Library	cdn.cloudflare.com
<input type="checkbox"/>	cdn.cloudflare.com	2021-07-09	2021-07-09	Tracking Pixel	cdn.cloudflare.com
<input type="checkbox"/>	cdn.cloudflare.com	2021-07-09	2021-07-09	Content	cdn.cloudflare.com
<input type="checkbox"/>	cdn.cloudflare.com	2021-07-09	2021-07-09	JavaScript Library	cdn.cloudflare.com
<input type="checkbox"/>	cdn.cloudflare.com	2021-07-09	2021-07-09	Font	cdn.cloudflare.com

## 11

## A website shares things with other sites

In their eternal quest to make their malicious pages look legit, threat actors will often borrow elements from other pages, such as images, iframes, or redirects. Host pairs, two domains (a parent and a child) that share a connection, can show what a site is pulling from other sites. Host pairs can go both ways - you can see what a malicious page is pulling from a legitimate one and what malicious pages may be pulling from your e-commerce site.

In the example below, we see a phishing page borrowing elements — in this case, links and images — from a legitimate page. We can see the relationship between the two pages via the parent and child hostnames below.

The screenshot shows the RiskIQ interface with a search for 'costco-redeem-rewards-coupon.ca'. The 'HOST PAIRS' section displays a table of relationships between the legitimate site and a phishing page.

Parent Hostname	Child Hostname	First	Last	Cause	Tags
costco-redeem-rewards-coupon.ca	costco-redeem-rewards-coupon.ca	2021-07-10	2021-07-10	parentPage	Blocklist, Phishing, Riskiq
costco-redeem-rewards-coupon.ca	www1.royalbank.com	2021-07-09	2021-07-09	img.src	Blocklist, Phishing, Riskiq
costco-redeem-rewards-coupon.ca	www1.royalbank.com	2021-07-09	2021-07-09	link.href	Blocklist, Phishing, Riskiq
costco-redeem-rewards-coupon.ca	www1.royalbank.com	2021-07-09	2021-07-09	css.import	Blocklist, Phishing, Riskiq
costco-redeem-rewards-coupon.ca	www1.royalbank.com	2021-07-09	2021-07-09	xmlHttpRequest	Blocklist, Phishing, Riskiq
costco-redeem-rewards-coupon.ca	www1.royalbank.com	2021-07-09	2021-07-09	script.src	Blocklist, Phishing, Riskiq
costco-redeem-rewards-coupon.ca	www1.royalbank.com	2021-07-09	2021-07-09	script.src	Blocklist, Phishing, Riskiq
costco-redeem-rewards-coupon.ca	meet.google.com	2021-07-09	2021-07-09	redirect	Blocklist, Phishing, Riskiq

## 12

## A website shares things with your site

More advanced cybersleuths can check which elements of their e-commerce sites are being used by threat actors across the web. With a Jupyter Notebook from RiskIQ, you can enter your domain to see which reputable sites may be stealing images, stylesheets, or other elements from your site to create fake pages.

Below, we can see an example of a site that's been copied by threat actors to use in various threat campaigns.

Jupyter Who Is Phishing www1.royalbank.com Last Checkpoint: 10/28/2021 (autosaved)

File Edit View Insert Cell Kernel Widgets Help Trusted Python 3

```
In [15]: hostpairs_df = foreign_hostpairs.filter_in(cause=redirect_causes).as_df

# Remove some extra columns
del(hostpairs_df['query'])
del(hostpairs_df['direction'])
del(hostpairs_df['child'])

# Create a parent_domain column with just the registered domain
hostpairs_df['parent_domain'] = hostpairs_df.apply(lambda r: str(analyzer.Hostname(r['parent']).registered_domain), axis=1)

# Create a reputation dataframe
reputation_df = pd.concat([analyzer.Hostname(h).reputation.as_df for h in suspect_domains])

# Join the reputation dataframe to the hostpairs dataframe and cleanup extra columns
hostpairs_df = hostpairs_df.merge(reputation_df, left_on='parent_domain', right_on='query')
del(hostpairs_df['query'])
del(hostpairs_df['rules'])
hostpairs_df.sort_values('score', ascending=False, inplace=True)
hostpairs_df
```

Out[15]:

	firstseen	lastseen	parent	cause	parent_domain	score	classification
117	2021-10-04 06:32:02	2021-10-04 13:19:19	citizendonation.xyz	script.src	citizendonation.xyz	100	MALICIOUS
82	2021-10-18 19:17:46	2021-10-19 00:11:33	xcvbji.info	unknown	xcvbjl.info	100	MALICIOUS
90	2021-10-13 12:11:00	2021-10-14 03:55:08	www.rbc-bnk.com	css.import	rbc-bnk.com	100	MALICIOUS
89	2021-10-13 12:11:30	2021-10-14 03:55:10	www.rbc-bnk.com	img.src	rbc-bnk.com	100	MALICIOUS
48	2021-10-28 15:47:49	2021-10-28 15:47:49	diaryport.com	topLevelRedirect	diaryport.com	100	MALICIOUS
85	2021-10-18 19:53:39	2021-10-18 21:05:38	belicapayreturn.com	script.src	belicapayreturn.com	100	MALICIOUS
84	2021-10-18 19:53:47	2021-10-18 21:06:35	belicapayreturn.com	css.import	belicapayreturn.com	100	MALICIOUS
83	2021-10-18 19:53:43	2021-10-18 21:06:36	belicapayreturn.com	img.src	belicapayreturn.com	100	MALICIOUS
81	2021-10-18 18:34:16	2021-10-19 01:59:19	xcvbjl.info	script.src	xcvbjl.info	100	MALICIOUS
92	2021-10-13 06:33:35	2021-10-13 23:27:51	interac.lcu	css.import	interac.lcu	100	MALICIOUS
80	2021-10-18 20:07:27	2021-10-19 01:59:47	xcvbjl.info	img.src	xcvbjl.info	100	MALICIOUS

In [16]: analyzer.Hostname('belicapayreturn.com').hostpair\_children.as\_df

Out[16]:

	query	direction	firstseen	lastseen	child	parent	cause
0	belicapayreturn.com	children	2021-10-18 19:53:43	2021-10-18 21:06:36	www1.royalbank.com	belicapayreturn.com	img.src
1	belicapayreturn.com	children	2021-10-18 19:54:24	2021-10-18 21:06:35	www1.royalbank.com	belicapayreturn.com	link.href
2	belicapayreturn.com	children	2021-10-18 19:53:47	2021-10-18 21:06:35	www1.royalbank.com	belicapayreturn.com	css.import
3	belicapayreturn.com	children	2021-10-18 19:53:42	2021-10-18 21:05:42	www1.royalbank.com	belicapayreturn.com	xmlhttprequest
4	belicapayreturn.com	children	2021-10-18 19:53:41	2021-10-18 21:05:41	www1.royalbank.com	belicapayreturn.com	script.src
5	belicapayreturn.com	children	2021-10-18 19:53:39	2021-10-18 21:05:38	www1.royalbank.com	belicapayreturn.com	script.src
6	belicapayreturn.com	children	2021-10-18 15:00:45	2021-10-18 15:00:45	meet.google.com	belicapayreturn.com	redirect



## Get a Head Start on Threat Actors this Holiday Shopping Season

These 12 red flags will be an easy, useful way for anyone looking after an e-commerce shop to identify cyber threats that are now endemic to the holiday shopping season. In the 12 examples above, we used RiskIQ Community Edition to highlight each example ([register here for free](#)). RiskIQ users will find several upgrades to the platform, including a new UI and layered Threat Intelligence that Illuminates Threat Actors and their tools.

However, while RiskIQ Community Edition is a great one-stop shop to spot these red flags, a wide selection of free, open-source tools are available to e-commerce defenders.

When you identify threats this holiday shopping season, pat yourself on the back to making the internet a safer place. Then, be sure to submit the URL to Google Safe Browsing to be blocked so it can no longer do harm.

Anyone with questions about combating cyber threats this holiday shopping season [can contact RiskIQ today](#).



**RiskIQ, Inc.**

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

✉ [sales@riskiq.net](mailto:sales@riskiq.net)

☎ 1 888.415.4447

**Learn more at [riskiq.com](https://riskiq.com)**

Copyright © 2021 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. 11\_21