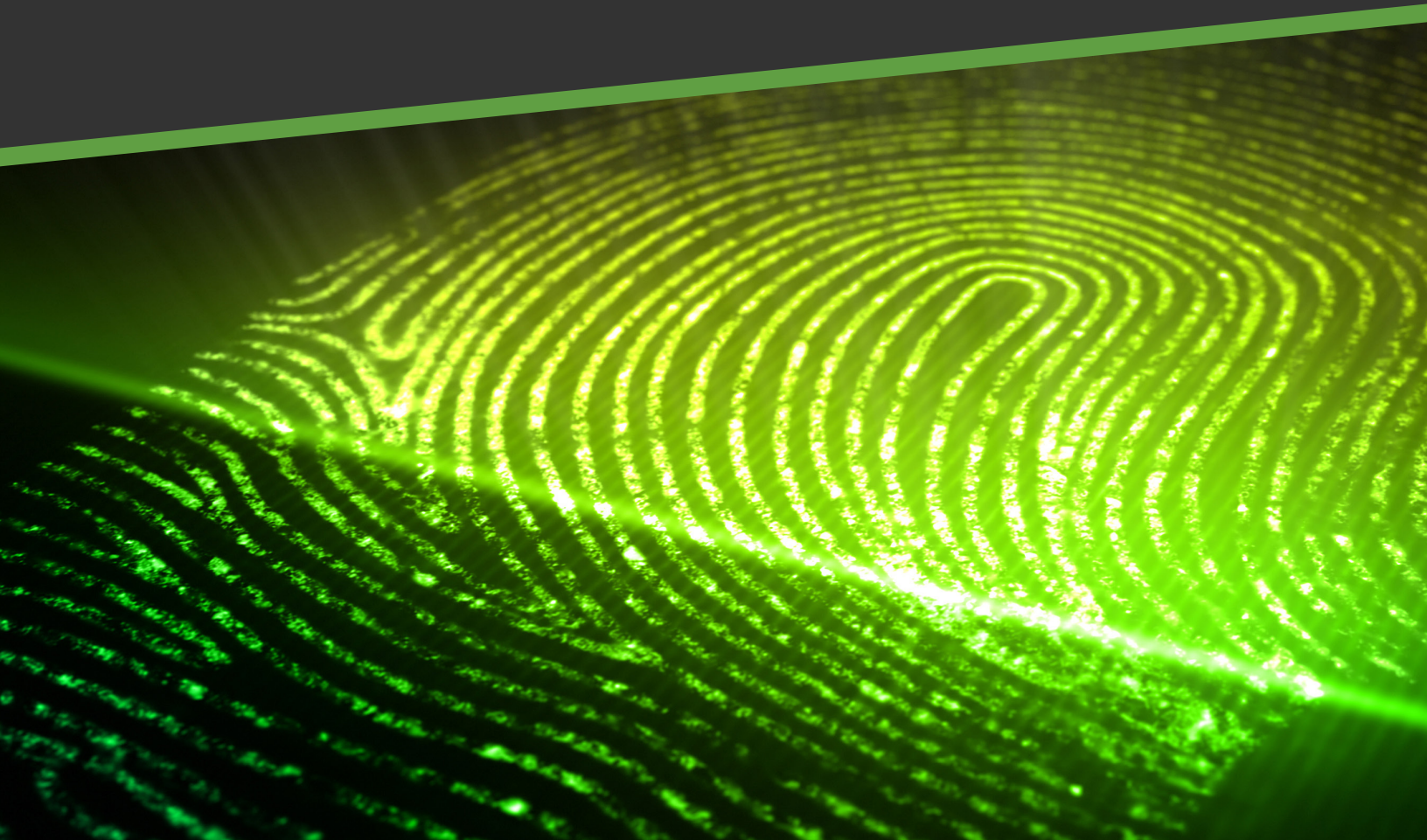
Hacked Website Report 2017

The latest malware and hacking trends in compromised websites.

This report is based on data collected and analyzed by the Sucuri Remediation Group (RG), which includes the Incident Response Team (IRT) and the Malware Research Team (MRT). It analyzes 34,000+ infected websites and shares statistics associated with:

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



Index

Introduction

The Hacked Website Report is a report produced by Sucuri. It summarizes the latest trends by bad actors, identifying the latest tactics, techniques, and procedures (TTPs) seen by the Remediation Group (RG). This report will build on the data from the previous quarters, including updated data for 2017.

The one constant you'll find in this report is the issues pertaining to poorly trained website administrators (i.e., webmasters) and their effect on websites.

This report will provide trends based on the CMS applications most affected by website compromises, the type of malware families being employed, and updates on the state of website blacklisting. It does not consider data related to WordPress plugin configurations.

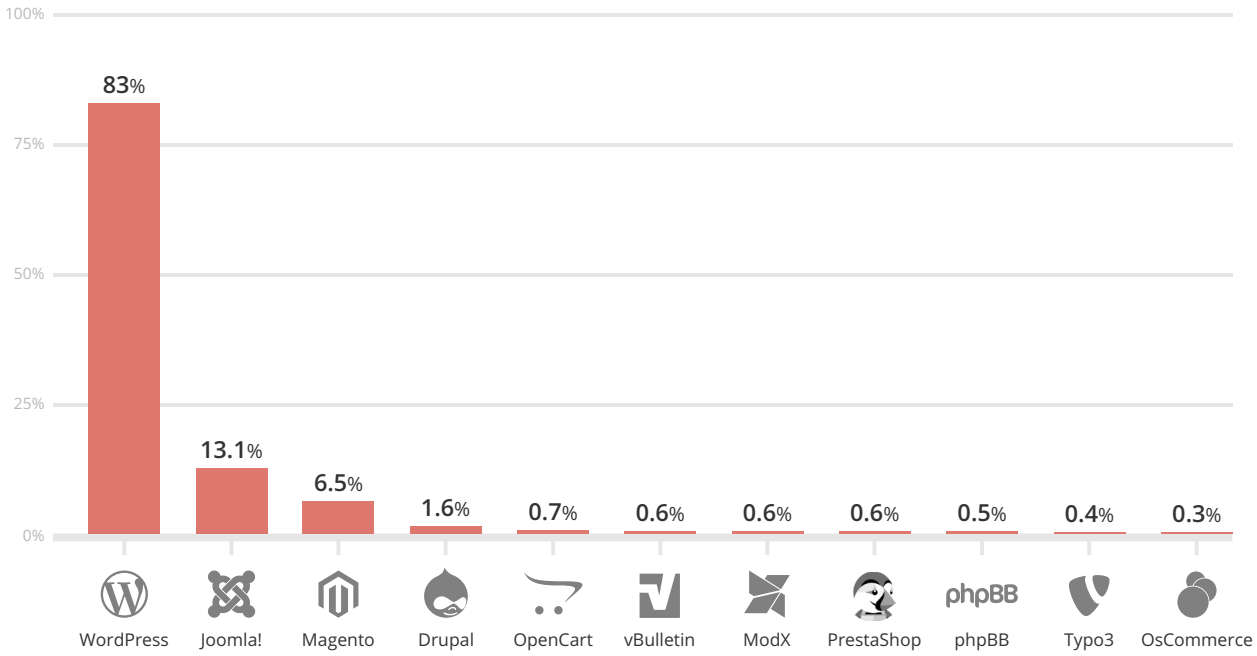
This report is based on a representative sample of the total number of websites the Sucuri RG performed incident response services in the Calendar Year (CY) 2017. A total of **34,371 infected websites** were analyzed in this report. This sample provided an accurate representation of the infected websites worked on by the remediation group in 2017.

CMS Analysis

Based on our data, the three most commonly infected CMS platforms were **WordPress, Joomla!** and **Magento**. This data does not imply these platforms are more or less secure than others.

In most instances, the compromises which were analyzed had little, if anything, to do with the core of the CMS application itself but more with its improper deployment, configuration and overall maintenance by the webmasters.

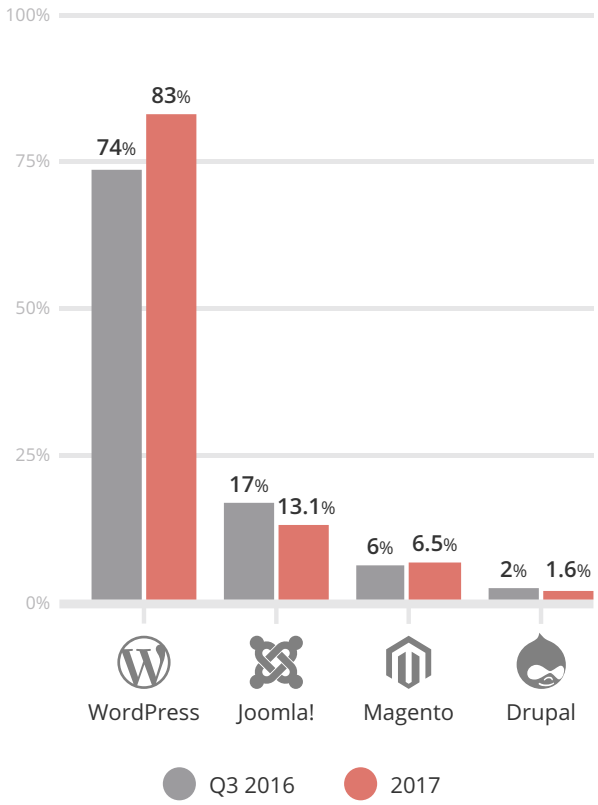
Infected Websites Platform Distribution - 2017



The 2017 telemetry indicates a shift in CMS infections:

- WordPress infections rose from 74% in 2016 Q3 to 83% in 2017.
- Joomla infection rates have dropped from 17% in 2016 Q3 to 13.1% in 2017.
- Magento infection rates rose marginally from 6% in Q3 2016 to 6.5% in 2017.
- Drupal infections dropped slightly from 2% in Q3 2016 to 1.6% in 2017.

CMS Infection Comparison - 2017



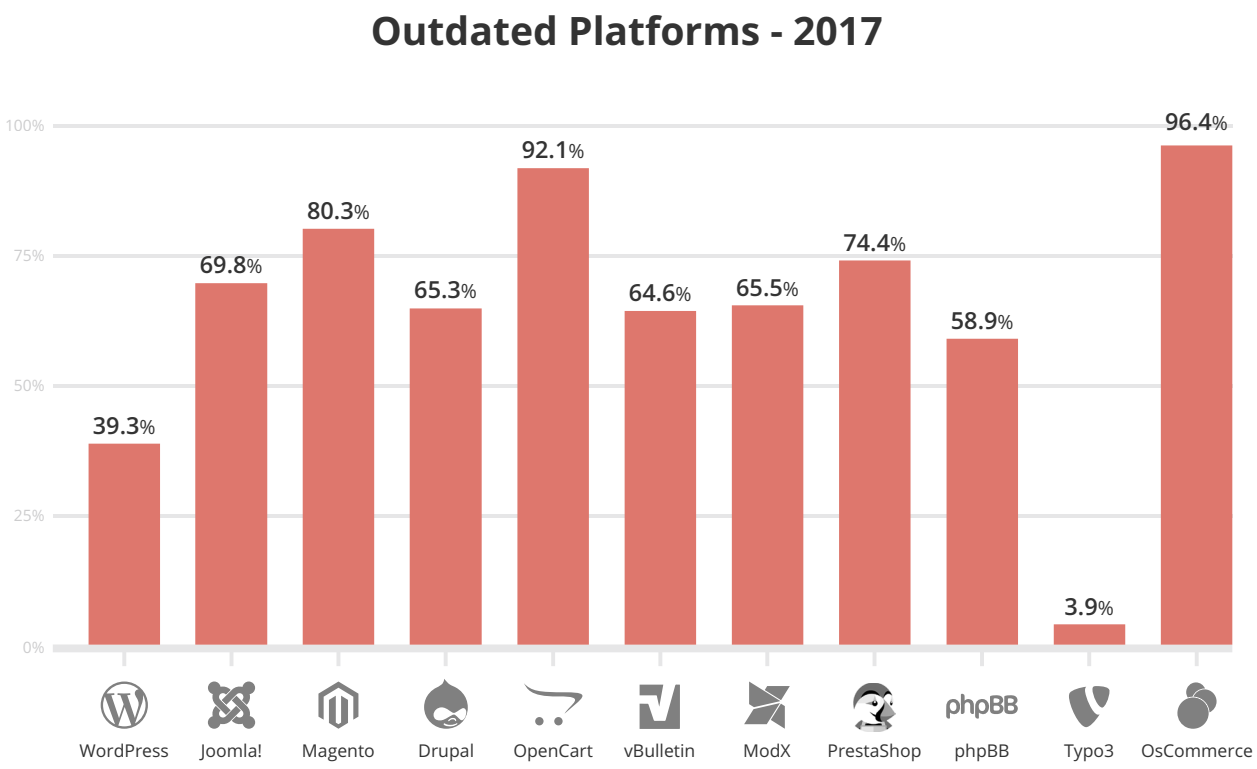
The above chart provides a comparison from our previous report in Q3 2016 to 2017 of the platform distribution for the top four CMS applications we monitor.

Outdated CMS Analysis

While the leading cause of infections stemmed from vulnerabilities found in the extensible components of the CMS applications (i.e., extensions, plugins, modules), it is also important to analyze and understand the state of the CMSs we worked on.

- Updated CMS
- Outdated CMS

A CMS was considered out of date if it was not on the latest recommended security version or if it had not patched the environment with available security updates (as is the case in Magento deployments) at the time Sucuri performed the incident response services.



We are seeing an interesting shift in the number of out of date, vulnerable versions of WordPress at the point of infection. At the end of Q3 2016, 61% of hacked WordPress sites recorded outdated installations, however, this has since decreased. In 2017, only **39.3% of clean up requests for WordPress had an outdated version.**

Joomla and Drupal saw more than a **15% decrease in outdated versions** from the previous year, down to 69.8% and 65.3% respectively.

Similar to previous years, Magento websites (80.3%) were mostly out of date and vulnerable at the point of infection; though this number has declined over 13% since Q3 2016.

We believe that this issue is stemming from three main areas: highly customized deployments, issues with backward compatibility, and lack of staff available to assist with the migration to newer CMS versions within the respective organizations. These areas tend to foster upgrading and patching issues for the organizations that leverage popular CMSs for their websites, also resulting in potential incompatibility issues and impacts to the website's availability.

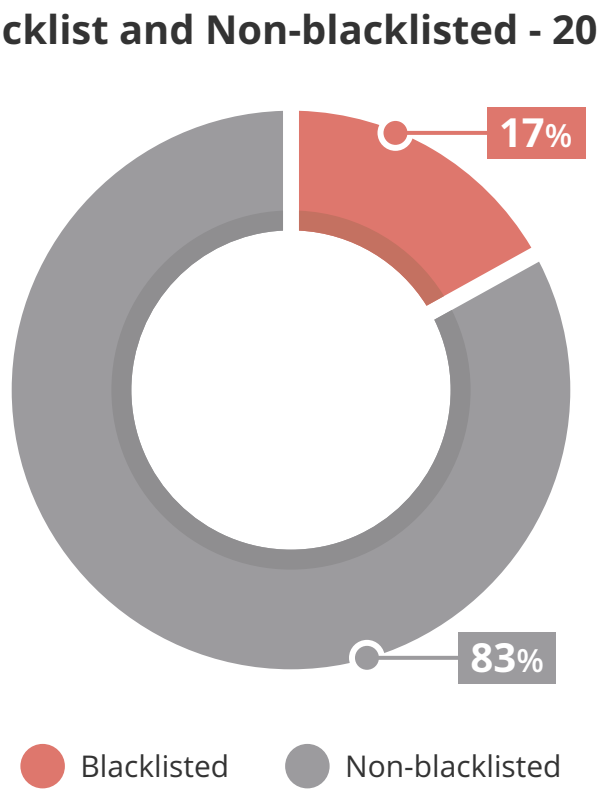
One of the more concerning trends we have identified is with Magento, a leading platform for online commerce by large organizations. Due to its rich data environment, attackers have a high interest in targeting cardholder data (i.e., credit card information and PAN information).

Blacklist Analysis

In 2017, we continued our analysis of blacklists. Website blacklists have the ability to adversely affect website owners, so it's important to understand how to remove a blacklist warning.

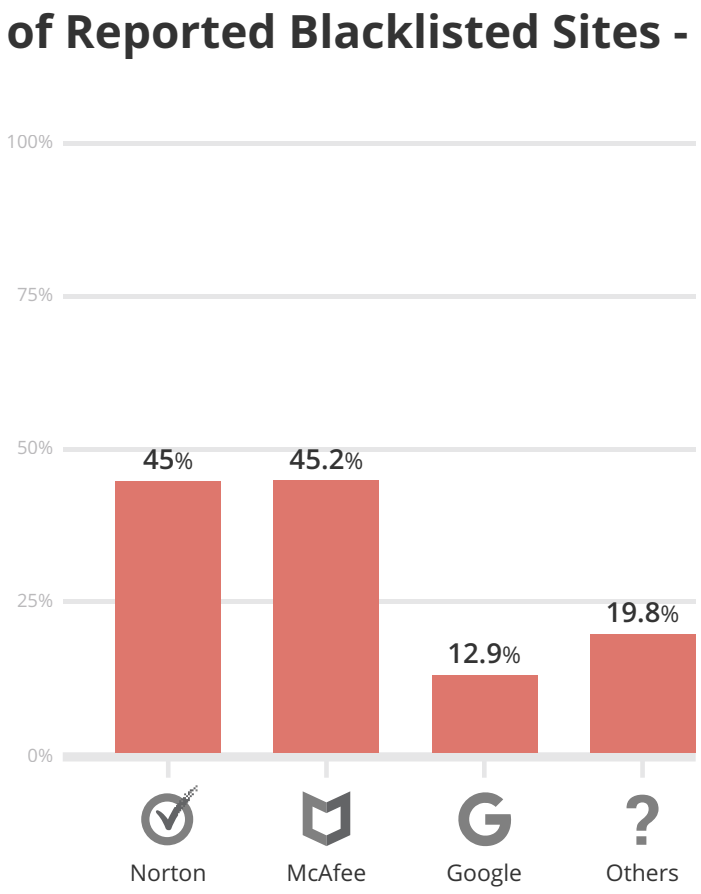
When a website has been flagged by a blacklist authority (such as Google), the results are devastating. Blacklisting can affect how visitors access a website, how it ranks in Search Engine Result Pages (SERP) and how adversely it can affect communication mediums like email.

Per our analysis, approximately **17% of the infected websites were blacklisted** (a 2% increase from 15% in Q3 - 2016).



This highlights the importance of continuous monitoring of web properties beyond the traditional means like Google and Bing webmaster tools. It also indicates that blacklist monitoring is not enough to detect whether a site has been compromised.

In our scans, we leverage a number of different blacklists. During 2017, the two most prominent blacklists were **Norton Safe Web** and **McAfee SiteAdvisor**; both of these groups accounted for **45% of blacklisted websites.**



Google Safe Browsing captured only 12.9% of the blacklists, which is a decline from previous years.

Several other blacklisting authorities flagged 19.8% of websites. Unnamed in the graph above, these blacklists include PhishTank, Spamhaus, and a couple of smaller groups.

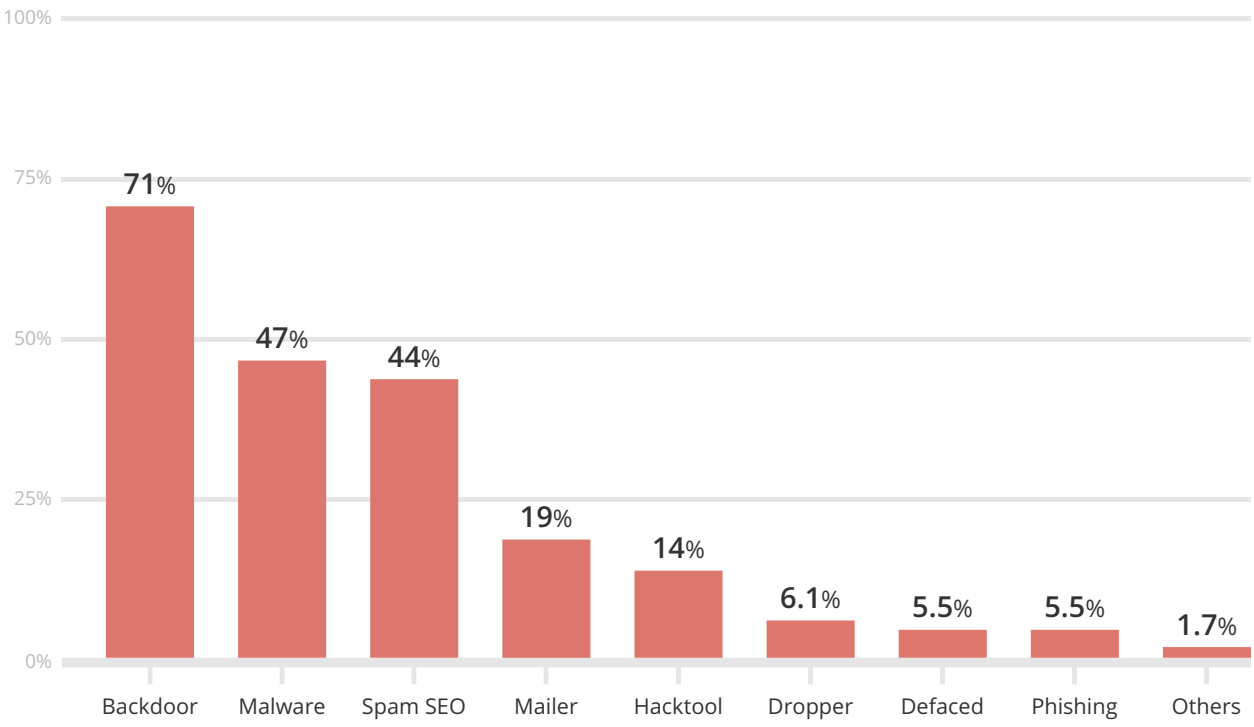
Note: An overlap in reported percentages is often due to more than one blacklisting authority flagging a single website. When analyzing these data sets, our sample size was smaller due to upgrades to our blacklist reporting. This may have impacted our results.

Malware Families

Part of our 2017 research included analyzing the various infection trends, specifically how they correlate to our malware families. Malware families allow our team to better assess and understand the attacker's tactics, techniques, and procedures (TTP), which inevitably leads us to their intentions.

A hacked site can have multiple files modified with different families of malware in them (a many-to-many relationship). It depends on the attacker's intent (i.e., action on objective) in how they plan to leverage their new asset (ie. the website that is now part of their network).

Malware Family Distribution - 2017



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.)

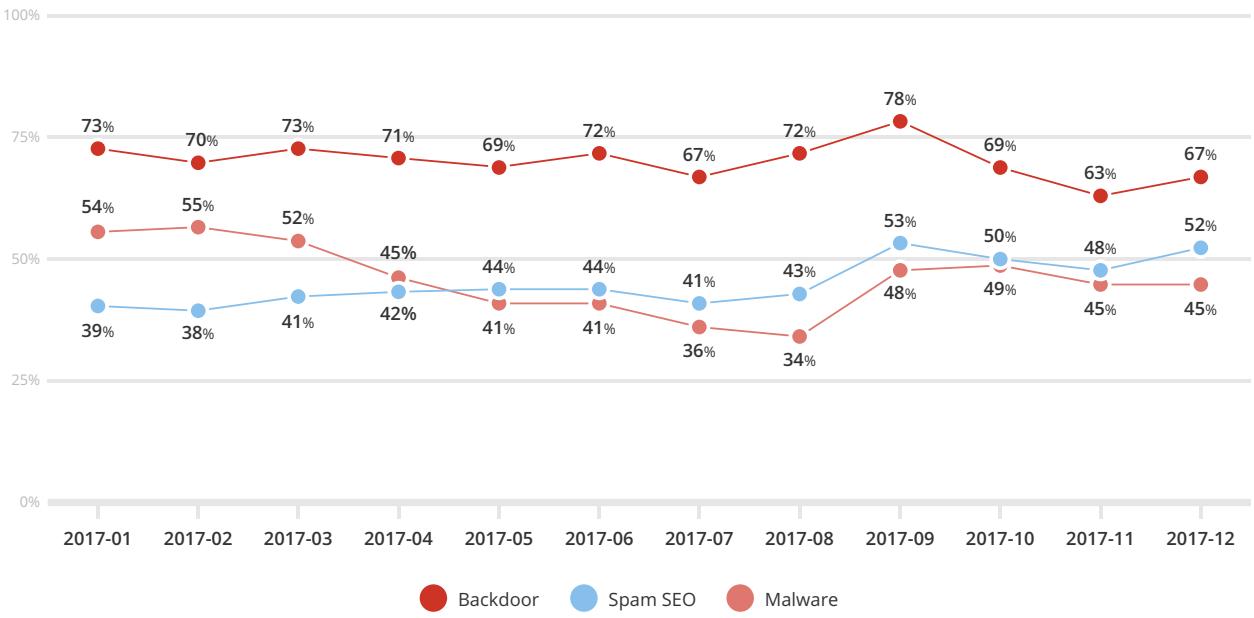
Over the course of the previous year, 71% of all compromises had a PHP-based backdoor hidden within the site. These backdoors allow an attacker to retain access to the environment long after they have successfully infected the website and performed their nefarious acts. This gives attackers the opportunity to bypass any existing access controls into the web server environment. The effectiveness of these backdoors comes from their elusiveness to most website scanning technologies.

Backdoors often function as the point of entry into the environment, post-successful compromise (i.e., the ability to continue to compromise). Backdoors themselves are not often the intent of the attacker. The intent is in the attack itself, found in the form of conditional SEO spam, malicious redirects, or drive-by-download infections.

We also saw a **marginal decline in malware distribution** – from 50% in Q3 2016 to 47% in 2017. **Mailer script infections held steady at 19%** from the previous report.

Approximately **44% of all infection cases in 2017 were misused for SEO spam campaigns**; up 7% from our last report. These campaigns often occur through PHP, database injections, or .htaccess redirects where the site was infected with spam content or the site redirected visitors to spam-specific pages. The content used is often in the form of pharmaceutical ad placements (i.e., erectile dysfunction, Viagra, Cialis, etc.) and includes other injections for industries like fashion and entertainment (i.e. cheap Ray-Bans, gambling, pornography).

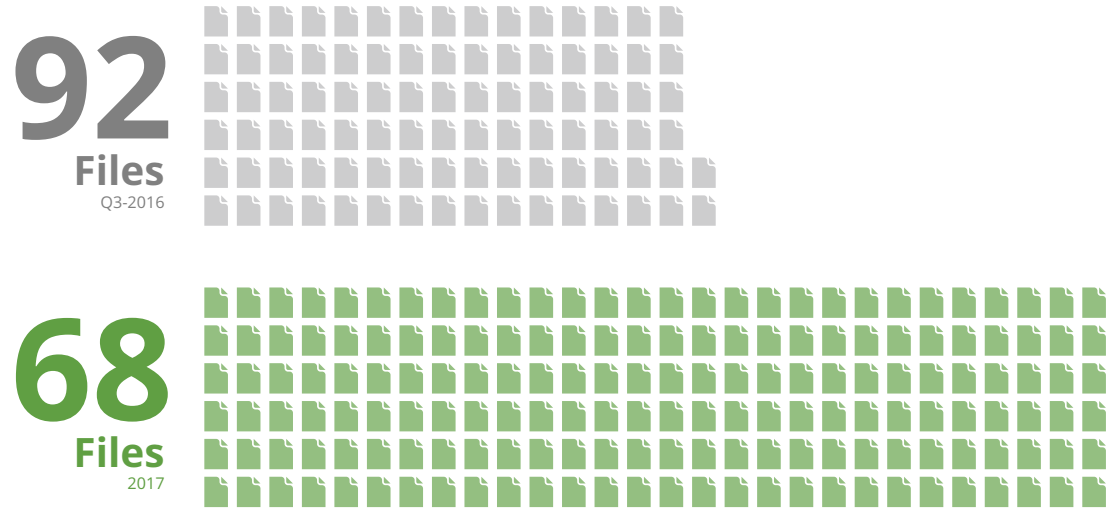
Annual Trends for the Top 3 Malware Families - 2017



According to the annual trends shown above for the top three threats, we can see a gradual increase in Spam SEO in contrast to a slight decline in Malware. In general, the Malware family represents a more generic family of attacks, whereas Spam SEO are more specific attacks that aim the manipulation of search engine optimization. The most interesting aspect of this trend increase is that it suggests attackers are now finding SEO spam a more lucrative attack vector compared to malware.

Our incident response service cleaned approximately **168 files during each malware removal request**, which was a **82% increase in the total number of files from our last report for Q3 2016.**

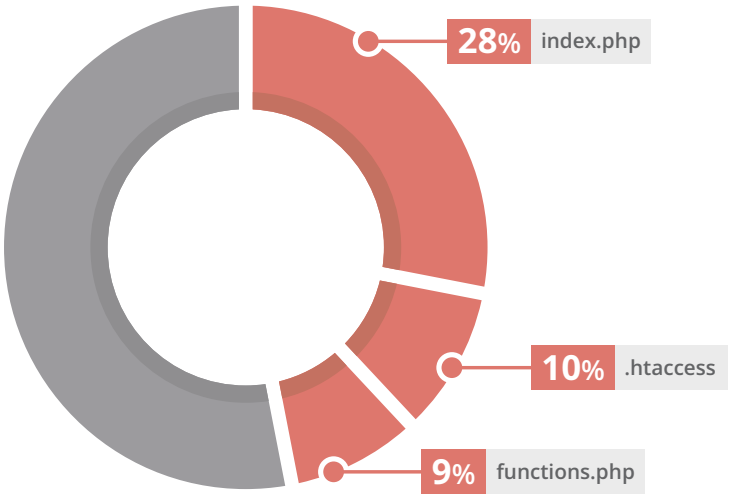
Files Cleaned Per Compromised Site - 2017



This doesn't necessarily speak to more complex hacks but does speak to an increase in the depth of files being affected with each hack. It also indicates that **cleaning the symptom from one file is often not enough** to remove an infection completely.

Additionally, we analyzed what attackers modified once a compromise was successful and were able to attribute them to the following three files:

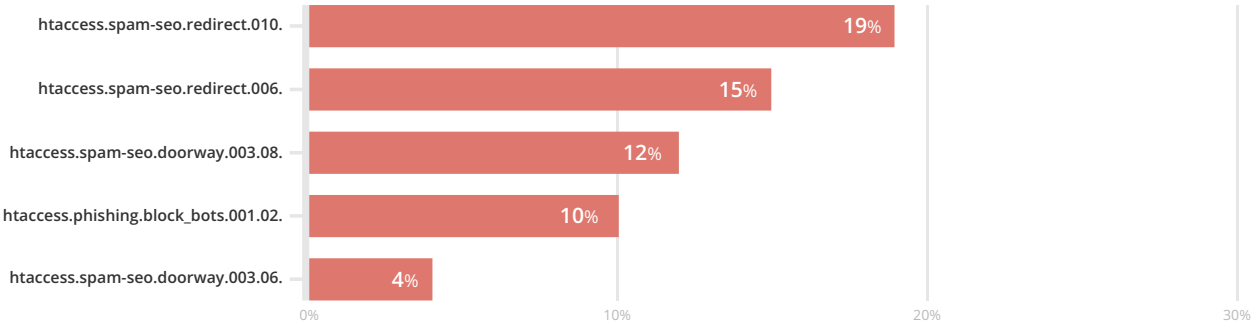
Top 3 Modified Files Post-Hack - 2017



Our data analysts and researchers identified which malware signatures were most commonly associated with these modified files.

Nineteen percent of .htaccess files were associated with the malware signature **htaccess.spam-seo.redirect.010**, also related to **htaccess.spam-seo.redirect.006** (15%). Used in Blackhat SEO/spam campaigns, the payload for these signatures are based on .htaccess rules and executed directly on the server before the site is rendered. Only the payload result, which can include spam content or redirects, is visible in the browser, not the malicious code itself.

Malware Signatures Associated with .htaccess Files - 2017

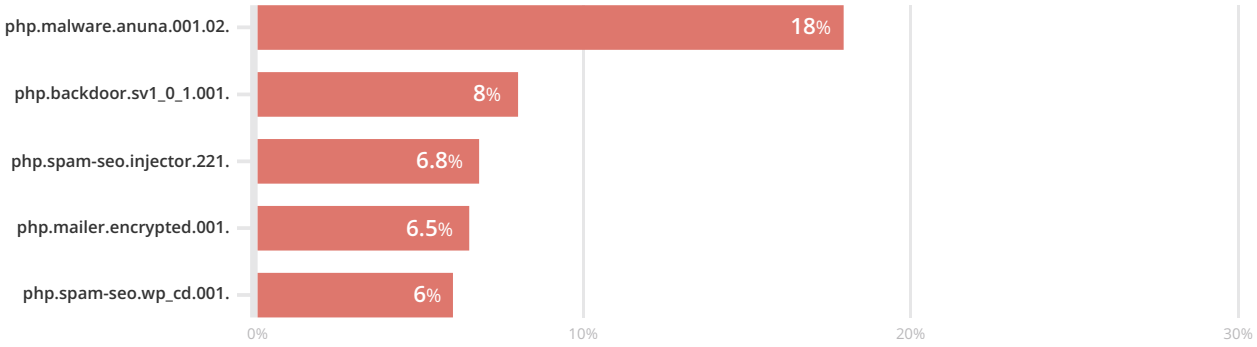


We also noticed two doorways that were commonly associated with modified .htaccess files: **htaccess.spam-seo.doorway.003.08** (12%) and **htaccess.spam-seo.doorway.003.06** (4%). These signatures trigger malicious code responsible for serving pages created to rank highly for specific search queries, which then redirects traffic to a different page. The redirections are often conditional and triggered based on user-agent, referrers, or IP addresses.

Ten percent of the .htaccess files we reviewed were also linked to the signature **htaccess.phishing.block_bots.001.02.** Malware authors used these to block bots and prevent indexing and automated detection of their phishing files.

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

Malware Signatures Associated with functions.php Files - 2017

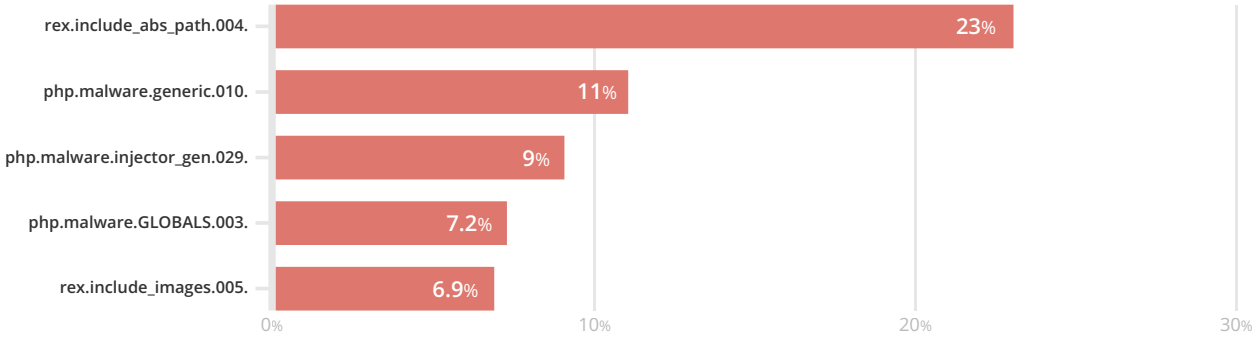


We also saw the signature **php.backdoor.sv1_0_1.001** associated with 8% of modified .htaccess files, which perpetrates malicious access to server environments. With this particular signature, the payload is PHP based and executed directly on the server while the site is loaded. Server-level analysis is necessary for these types of infections – only the payload result is visible in the browser, which is very common for backdoors and makes them impossible to detect them at the site level.

Other common signatures associated with functions.php files include **php.spam-seo.injector.221** (6.8%), **php.spam-seo.wp_cd.001** (6.5%), and **php.mailer.encrypted.001** (6.0%).

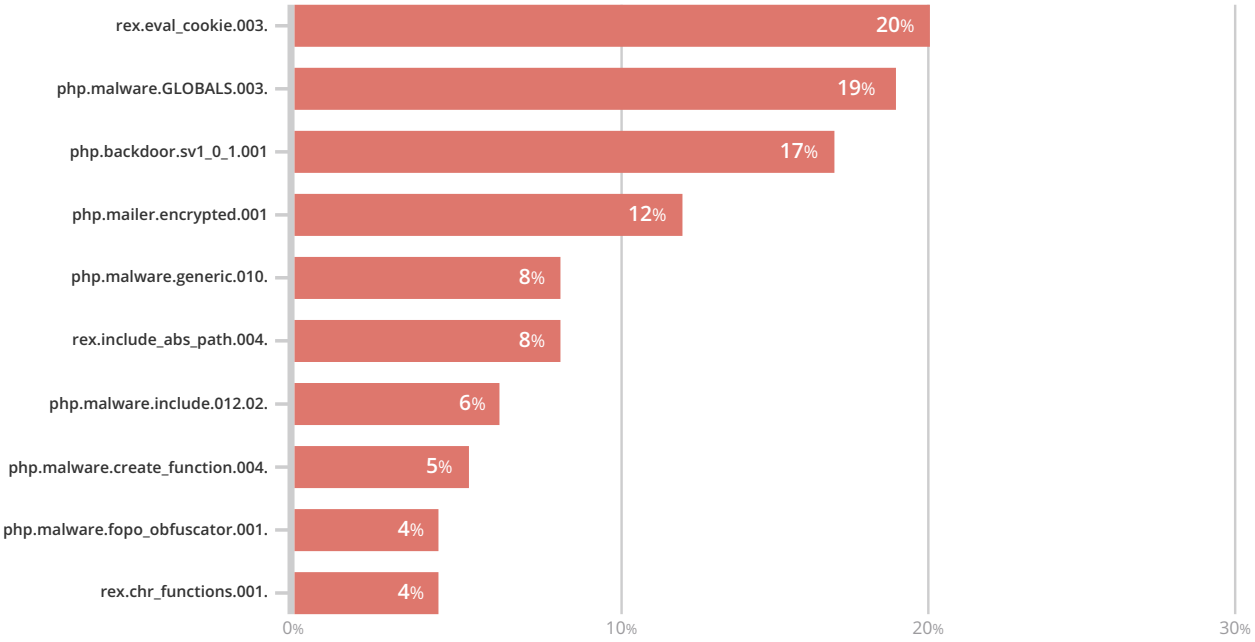
Twenty-three percent of index.php files were associated with the malware signature **rex.include_abs_path.004.** This signature looks for files called by PHP scripts using absolute paths and obfuscated characters within seemingly innocent files.

Malware Signatures Associated with index.php Files - 2017



The remaining malware signatures associated with index.php on our chart are for generic malware signatures and PHP malware.

Top 10 Malware Signatures in 2017



You can find more information about specific malware signatures in our Knowledge Base.

Conclusion

This report confirms what is already known. Vulnerable software continues to be a problem and is one of the primary causes of today's websites hacks.

A few takeaways from this report include:

- WordPress continues to be the leading infected website CMS (**83% of all websites** cleaned in 2017).
- There was a **notable decrease in out-of-date WordPress, Joomla, and Drupal installations** at the point of infection. Magento continues to lead the pack for number of out-of-date vulnerable installations at the point of infection.
- The blacklist telemetry showed a 1% reduction in sites being blacklisted (only 14%), **increasing the number of infected websites that are going undetected by blacklist engines** to 86%.
- The malware families analysis showed that SEO spam has risen to 62.8% (up 25.8% from Q3 2016). It also showed a decrease in mailer scripts, from 19% to 15.1%, and a **sharp decline in malware distribution** to 35% in 2017, down from 50% in Q3 2016.

There is little found in the data to indicate any significant difference between what is disseminated by information security (InfoSec) professionals and the actions taken by website administrators.

Similar to prior reports, we can expect that as open-source technologies continue to develop, the website industry will continue to see evolutions in the way they are compromised. There is a reduction in the knowledge required to create and own a website, which is breeding the wrong mindset with website owners and service providers alike.

Thank you for taking the time to read our report. We hope you found it engaging and thoughtful. If there is any additional information you think we should be tracking and reporting on, please let us know.

Website Security Platform

SucuriSecurity | sucuri.net

For more information

sucuri.net sales@sucuri.net 1–888-873-0817

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.