HACKED WEBSITE TREND REPORT
2016 - Q3

The latest trends into how websites get hacked, and the malware used

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 over 8k infected websites and shares statistics associated with:

- Affected open-source CMS applications
- Details on the WordPress platform
- Blacklists flagging the compromised sites
- Malware families and their effects

Whats inside this report

Introduction

The Hacked Website Trend 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 2016/Q3.

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

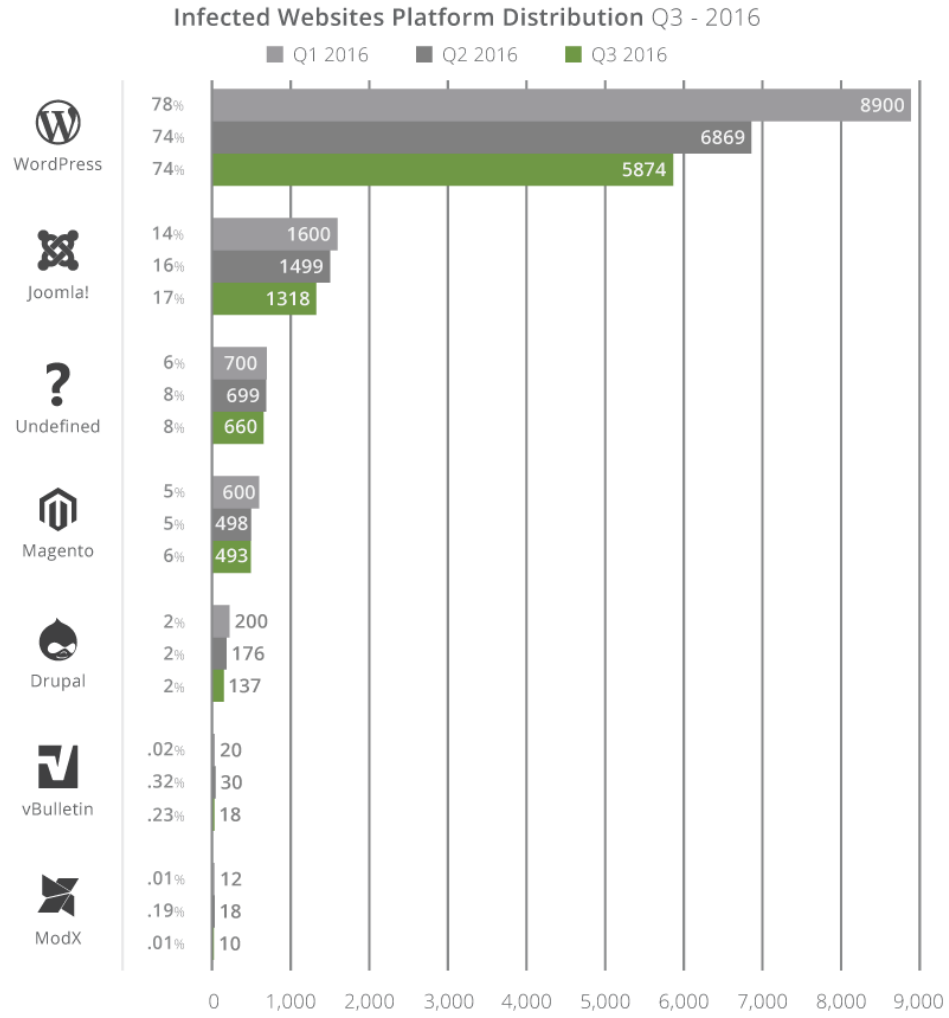
This report will provide trends based on the CMS applications most affected by website compromises, the type of malware families being employed, and updates on the state of website blacklisting. It removes the data pertaining to WordPress plugin configurations.

This report is based on a representative sample of the total number of websites the Sucuri RG performed incident response services on in Calendar Year (CY) 2016 Quarter 3 (CY16-Q3). A total of 7,937 infected websites were analyzed in this report. This sampling was the most accurate representation of the total sites Sucuri worked on this quarter.

CMS Analysis

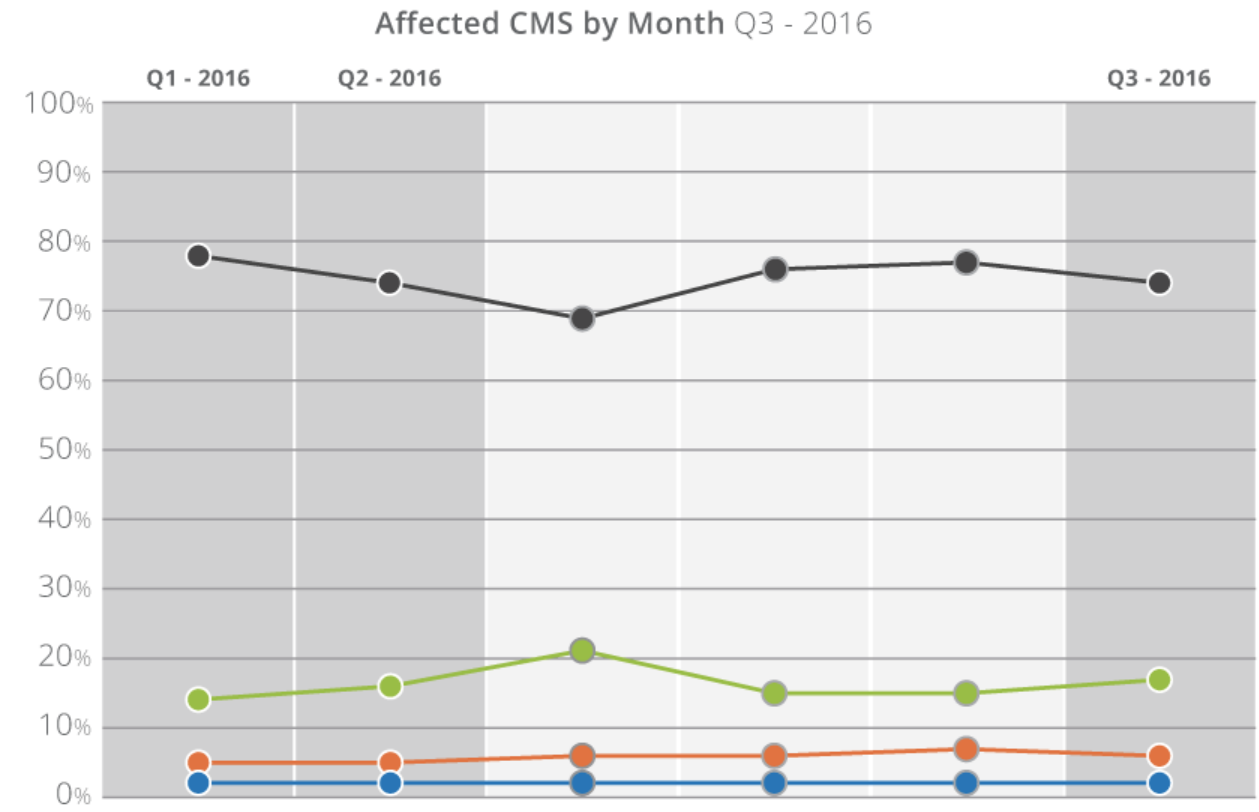
Based on our data, similar to 2016 - Q1 / Q2, the three leading CMS platforms were WordPress, Joomla! and Magento. Again, this does not imply these platforms are more or less secure than others.

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



The Q3 telemetry shows things were relatively stable across all platforms. The overall changes seemed marginal, with both Joomla! And Magento both experiencing a 1% increase. The modest increase in Magento is not a surprise, taking into consideration the trend this year of attackers shifting their focus to platforms used for online commerce (i.e., e-commerce)..

CMS Analysis (Continued)



	Q1 2016	Q2 2016	July 2016	August 2016	September 2016	Q3 2016
	78%	74%	69%	76%	77%	74%
	14%	16%	21%	15%	15%	17%
	5%	5%	6%	6%	7%	6%
	2%	2%	2%	2%	2%	2%

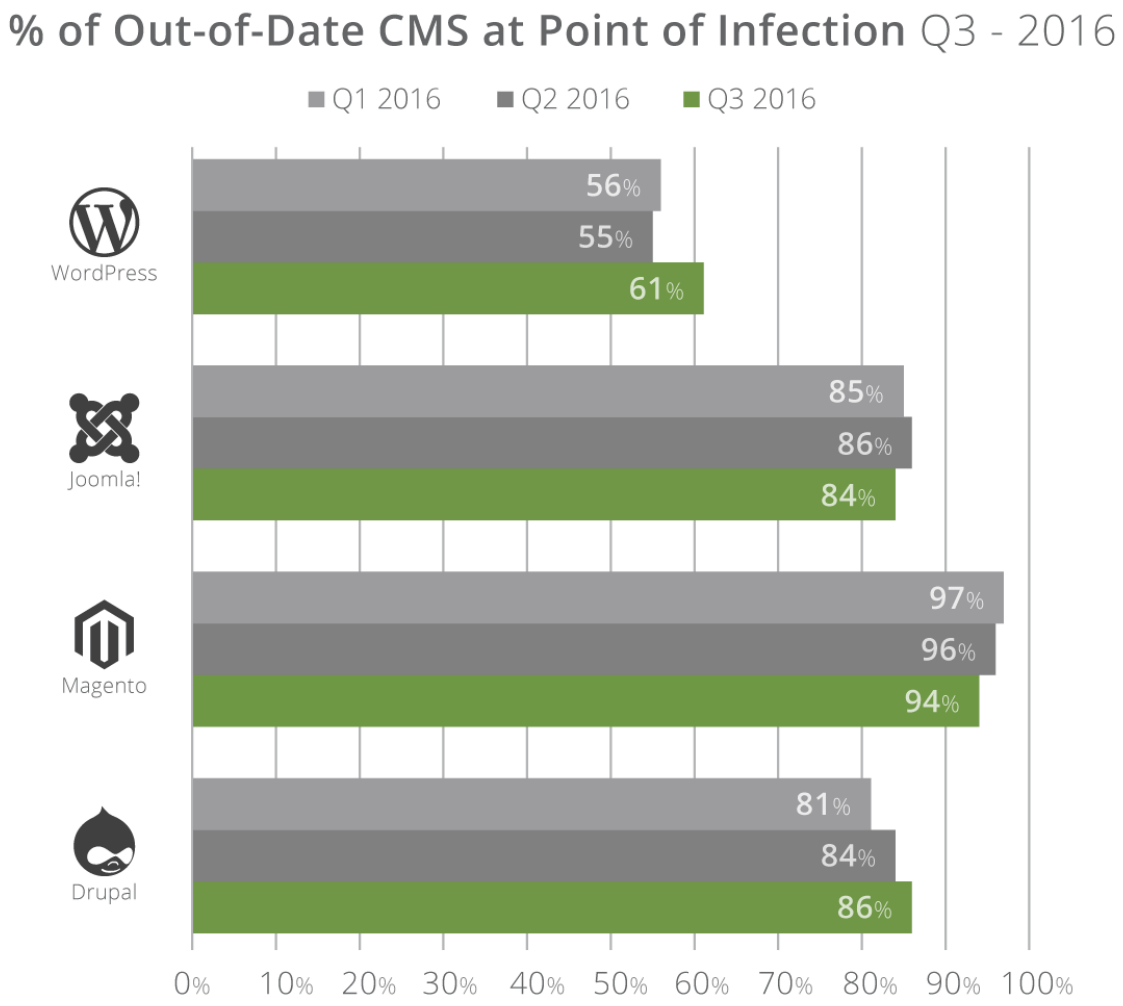
The above chart provides a monthly illustration of the platform distribution for the top four CMS applications we monitor.

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's also important to analyze and understand the state of the CMS's 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 had not patched the environment with available security updates (as is the case in Magento deployments) at the time Sucuri was engaged to perform **incident response services**.



Outdated CMS Analysis (Continued)

The most surprising change this quarter was the 6% increase in out of date, vulnerable versions of WordPress installations at the point of infection. In Q1 / Q2, **hacked WordPress sites** recorded outdated installations at 56% and 55% respectively.

Drupal also experienced a 2% increase from Q2 to Q3.

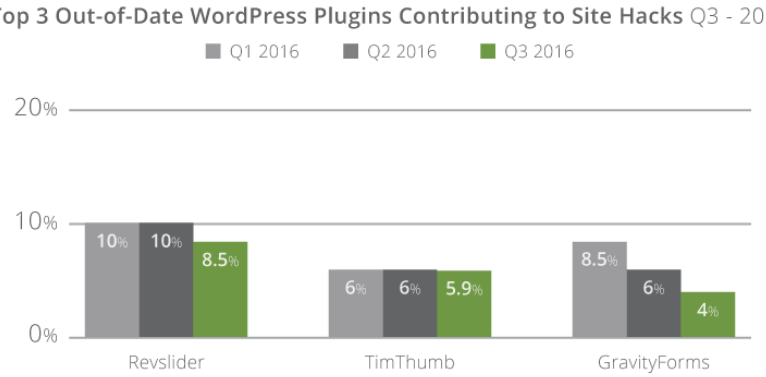
Similar to prior quarters, Magento (94%) and **Joomla! websites** (84%) were mostly out of date and vulnerable at the point of infection.

There was no change in why we believe this is happening. It appears to stem from three areas: highly customized deployments, issues with backward compatibility, and the lack of staff available to assist in the migration within the respective organizations. These tend to create upgrading and patching issues for the organizations that leverage them for their websites through incompatibility issues and potential impacts to the website's availability.

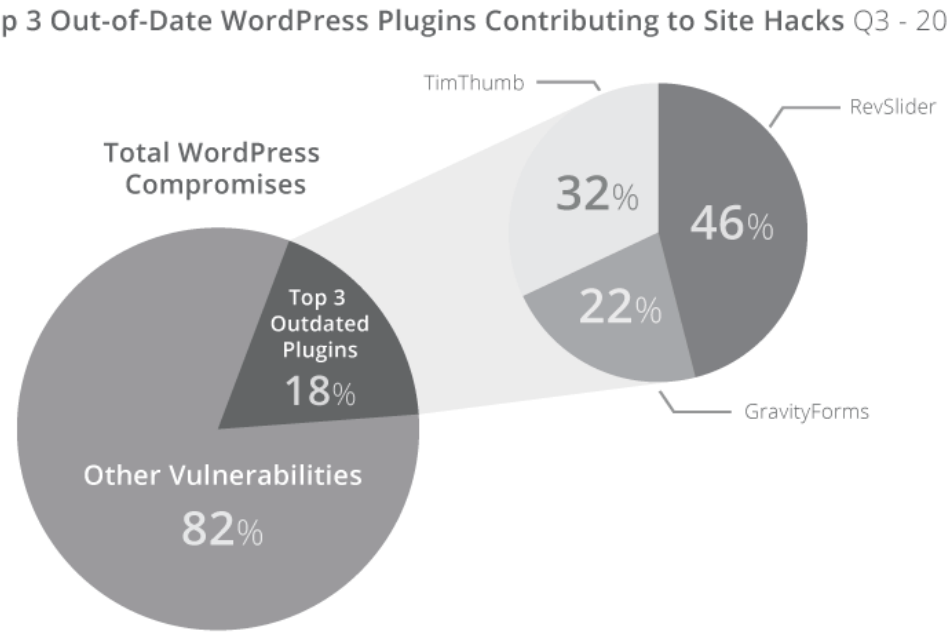
The most concerning aspect of this trend is with the Magento platform, one of the leading platforms for online commerce by large organizations. There is an increase in interest by attackers targeting the platform for its rich data environment, targeting cardholder data (i.e., credit card information, including up to PAN information). There will be more information on this in the Q4 report.

WordPress Analysis

Similar to prior quarters, we provide a deep dive analysis into the WordPress platform as it makes up 74% of our sampling. The top three WordPress plugins continue to be TimThumb, Revslider, and Gravity Forms:



These were the top three out-of-date, vulnerable, plugins at the point in Sucuri provided incident response services:



In Q3 we saw an improvement in Revslider, dropping 1.5% to 8.5%, and in GravityForms, dropping 2% to 4%. The total number of infected WordPress installations as a result of these three platforms has dropped significantly this year, from 25% in Q1, to 18% in Q3. The continued decrease is expected as more website owners and hosts continue to proactively patch out of date environments. The most interesting, and possibly disturbing, dataset is the lack of change in TimThumb. We believe this has to do with the fact that many website owners are unaware that they have the script on their site at all, similar to what we see with Revslider.

WordPress Analysis (Continued)

The data shows, however, that as these get patched, others will begin to take its place. Currently there are no other plugins that are being used in mass that would represent greater than 1% of our dataset.

All three plugins had a fix available over a year, with TimThumb going back multiple years (four to be exact, circa 2011). **Gravity Forms was patched in version 1.8.20**, December 2014 to address the **Arbitrary File Upload (AFU) vulnerability** that is causing the issues identified in this report. RevSlider was patched silently February 2014, publicly disclosed by **Sucuri September 2014**, and mass compromises started, and have continued, **since December of 2014**. This illustrates the challenges the community faces in making website owners aware of the issues, enabling the website owners to patch the issues, and facilitating the everyday maintenance and administration of websites by their webmasters.

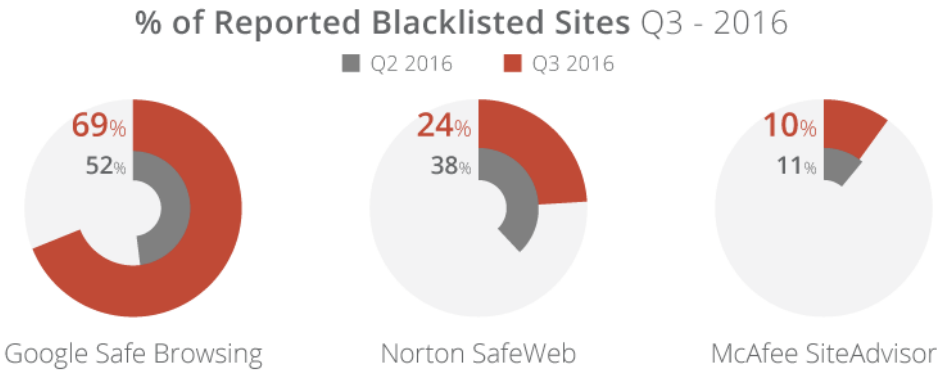
Unfortunately, in this report we had to remove the plugin distribution due to corrupted data during the analysis. We hope to reintroduce this dataset in future quarters.

Blacklist Analysis

In Q3 we continued our analysis of blacklists. Website blacklists have the ability to adversely affect website owners, so it'simportant to understand **how to remove a blacklist warning**.

A website being flagged by a blacklist authority like Google can be devastating to website functionality. It can affect how visitors access a website, how it ranks in Search Engine Result Pages (SERP) and also adversely affect communication mediums like email.

Per our analysis, approximately 15% of the infected websites were blacklisted (a 3% drop from 18% in Q2). This indicates that approximately 85% of the thousands of infected websites we worked on were freely distributing malware. This highlights the importance of continuous monitoring of your web property beyond traditional means like Google and Bing webmaster tools. It also highlights that blacklist monitoring is not enough to detect whether a site has been compromised.



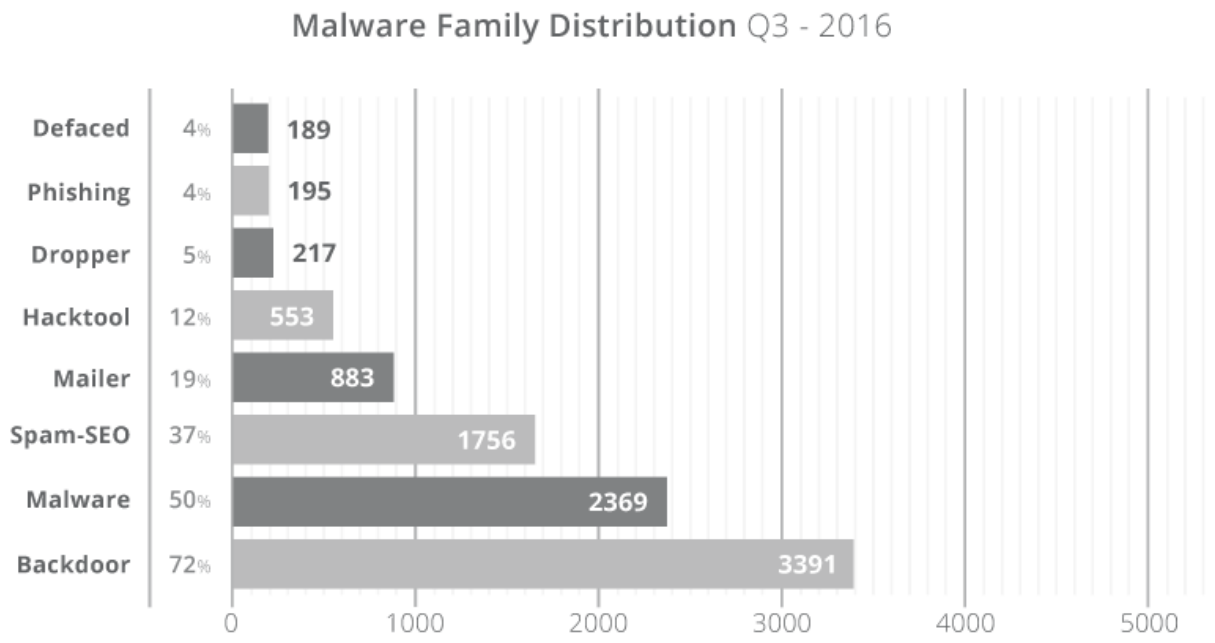
In our scans, we leverage a number of different blacklists. The most prominent blacklist was Google Safe Browsing; it accounted for 69% of the blacklisted sites, which also happens to be 10% of the total infected sites we worked on. Norton Safe Web had 24% of the total blacklists and McAfee SiteAdvisor captured 10% of the blacklists. All other blacklists we check flagged less than 1% and were removed from the report (including: PhishTank, Spamhaus, and a couple of smaller ones).

Note: The percentage will never be 100% as some sites were flagged by multiple blacklists at the same time.

Malware Families

Part of our research over the past quarter includes analyzing the various infection trends, specifically how they correlate to our malware families. Malware families allow our team to better assess and understand the attackers 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).



A quick glossary of terms:

Malware Family	Description
Backdoor	Files used to reinfect and retain access.
Malware	Generic term used for browser-side code used 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 promoting an unrelated subject (i.e., Hacktavism).
Phishing	Used in phishing lures in which attackers attempt to trick users into sharing sensitive information (i.e., log in information, credit card data, etc..).

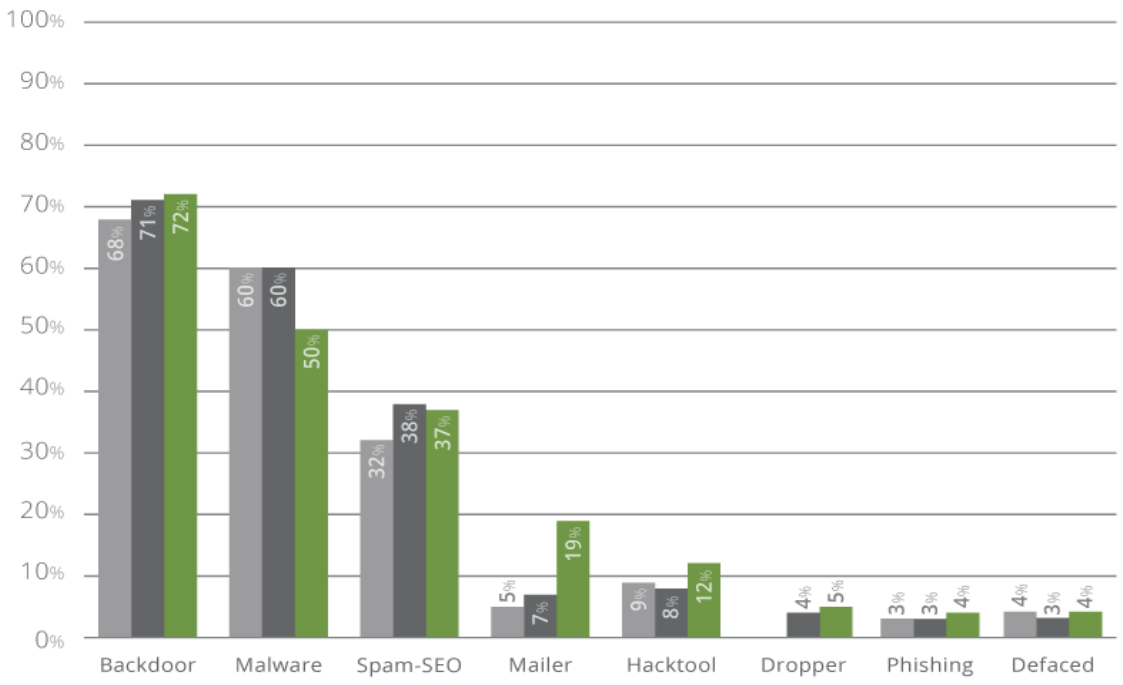
Malware Families (Continued)

Over the course of the previous quarter, 72% 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. These backdoors allow the attackers 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.

Approximately 37% of all infection cases are misused for SEO spam campaigns (either through PHP, database injections or .htaccess redirects) where the site was infected with spam content or 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 raybans, gambling, pornography).

Malware Family Annual Trend Analysis Q3 - 2016



	Backdoor	Malware	Spam-SEO	Mailer	Hacktool	Dropper	Phishing	Defaced
Q1 2016	68%	60%	32%	5%	9%	-%	3%	4%
Q2 2016	71%	60%	38%	7%	8%	4%	3%	3%
Q3 2016	72%	50%	37%	19%	12%	5%	4%	4%

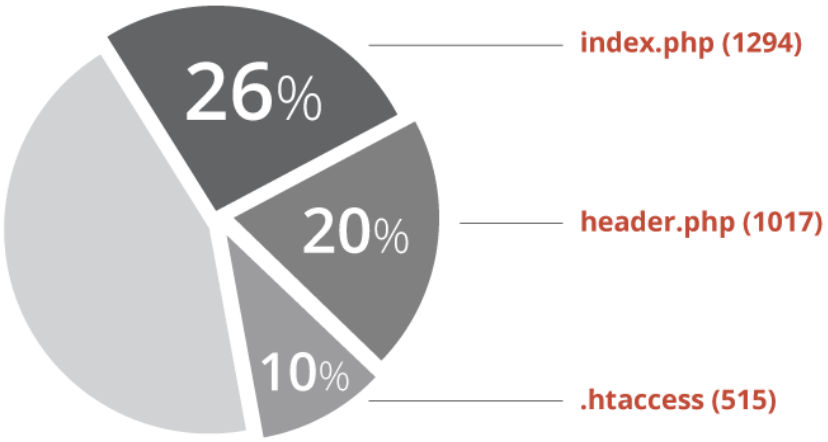
Malware Families (Continued)

One very interesting observation was the sharp increase in mailer scripts in Q3, jumping 12% to 19% from 7% in Q2. There was also a modest 4% increase in the hack tools found on infected sites. Abusing system resources for things like spam emails is not new, but the sharp increase to 19% in a quarter speaks to more attackers making use of this technique or new, improved methods of abusing these resources.

Another interesting observation was the 10% decline in malware distribution, from 60% in Q2 to 50% in Q3. It's difficult to say if this is an anomaly, seasonal, or another unidentified reason. Q4 should shed light into the latest trends.

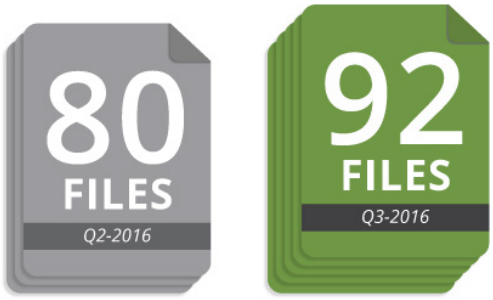
Additionally, we analyzed what attackers modified once a compromise was successful and we were able to attribute them to the following three files:

Top 3 Modified Files Post-Hack Q3 - 2016



Our incident response service also cleaned approximately 92 files on each malware removal request. That's a 15% increase from Q2. 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 speaks to the issue that cleaning the symptom on one file is often not enough to remove an infection completely.

Files Cleaned Per Compromised Site Q3 - 2016



Conclusion

This report confirms what is already known; vulnerable software continues to be a problem and is the leading cause of today's websites hacks.

A few takeaways from this report include:

- WordPress continues to lead the infected websites we worked on (at 74%).
- The top three plugins affecting WordPress continue to be Gravity Forms, TimThumb, and RevSlider, dropping from 25% in Q1 to 18% in Q3. However, there has been a noticeable increase in their impacts.
- There was a notable increase in WordPress installations out of date at the point of infection, which increased from 55% in Q2 to 61% in Q3. Both Joomla! and Magento continue to lead the pack with out-of-date vulnerable installations at the point of infection.
- The blacklist telemetry showed a 3% reduction in sites being blacklisted (only 15%), increasing the number of infected websites that are going undetected by blacklist engines to 85%. Google increased its share to 69% from 52% in Q2.
- The malware families analysis showed that SEO spam continues to be on the rise, holding steady at 37% (down 1% from Q2). It also showed a sharp increase in mailer scripts, from 12% to 19%, and a 10% decrease in malware distribution from 60% in Q2 to 50% in Q3.
- A new dataset was introduced this quarter that depicted which files bad actors are modifying most consistently with each incident: index.php (25%), header.php (20%), and .htaccess (10%).

There is little in the data to indicate that there is any change occurring between the guidance being disseminated by information security (InfoSec) professionals and the actions website administrators are taking.

Similar to what we reported in prior quarters, we can expect that as open-source technologies continue to change, the website industry we will continue to see evolutions in the way they are compromised. There is currently a sharp decline in the knowledge required to have 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 and 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. We have a number of new datasets we hope to be tracking for the Q4 report.

English
sucuri.net
SucuriSecurity

Spanish
sucuri.net/es
Sucuriseguridad

Portuguese
sucuri.net/pt
SucuriSeguranca

Real People. Real Security.
info@sucuri.net
1.888.873.0817