WEBSITE HACKED REPORT

2016 - Q1

Report on Post-Hack Actions by Attackers

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).

Whats inside this report

Introduction

There are currently over 1 Billion websites on the web. That number is growing as more of the world gets connected and technology makes it easier for people to have a voice and online presence through things like a website. This growth is being enabled by the explosion of technologies like open-source Content Management Systems (CMS).

Over a third of the websites online are powered by four key platforms: WordPress, Joomla!, Drupal, and Magento. -WordPress is leading the CMS market with over 60% market share. This explosion and dominance by WordPress is facilitated by global-user adoption,a highly extensible platform and focus on end users. Other platform technologies have experienced growth in more niche markets, like Magento in the online commerce domain with large and enterprise organizations, and Drupal in large, enterprise, and federal organizations.

This user adoption however brings about serious challenges to the internet as a whole as it introduces a large influx of unskilled webmasters and service providers responsible for the deployment and administrations of these sites. This assessment is amplified in our analysis, which shows that out of the 11,000 + infected websites analyzed, 75% of them were on the WordPress platform and over 50% of those websites were out of date. Compare that to other similar platforms that placed less emphasis on backwards compatability, like Joomla! and Drupal, the percentage of out-of-date software was above 80%.

As of March 2016, Google reports that over 50 million website users have been greeted with some form of warning that websites visited were either trying to steal information or install malicious software. In March 2015, that number was 17 million. Google currently blacklists close to ~20,000 websites a week for malware and another ~50,000 a week for phishing. PhishTank alone flags over 2,000 websites a week for phishing. These numbers reflect only those infections that have an immediate adverse effect on the visitor (i.e., Drive by Download, Phishing) and do not include websites infected with Spam SEO and other tactics not detected by these companies.

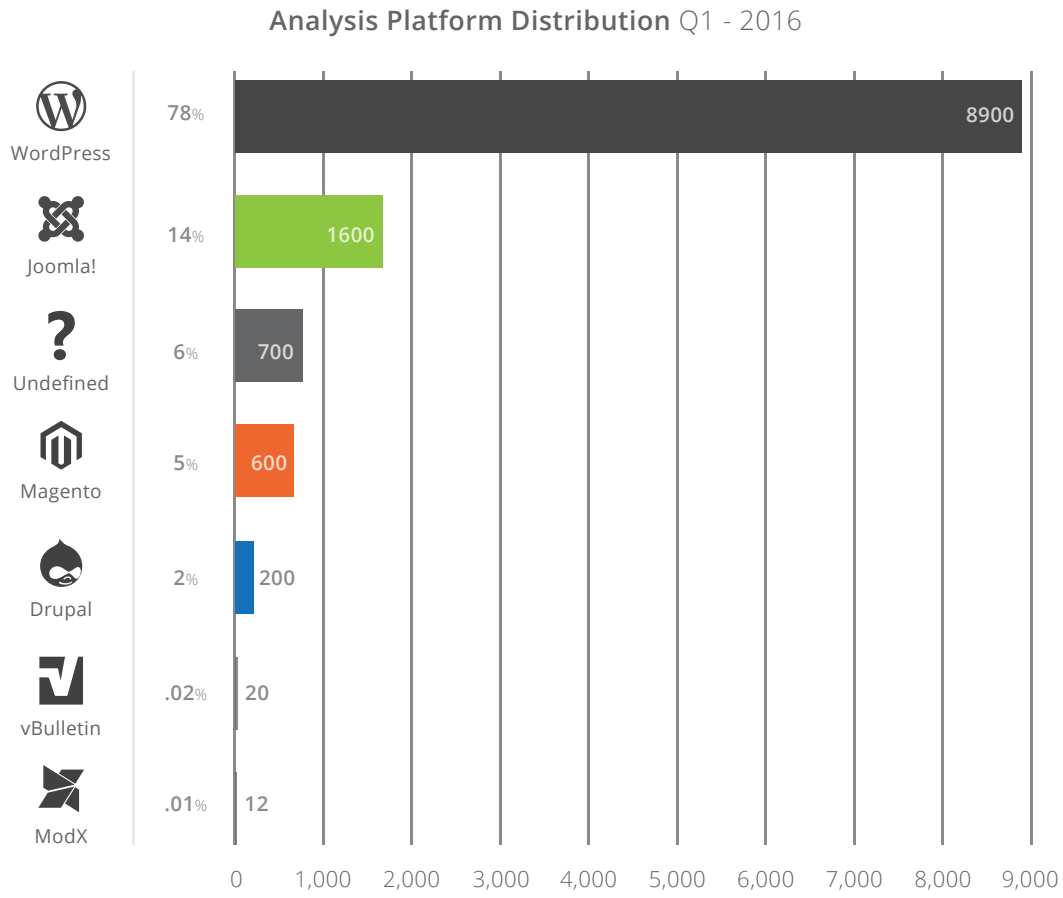
At Sucuri, we are well-situated to provide a unique perspective into what is happening once a website is hacked, and we have shared those findings in this report. We begin by trying to understand how websites are being hacked, then theorize and summarize those findings with quantifiable, measurable data collected from our customers.

This report will provide trends based on the CMS applications most affected by website compromises and the type of malware families being employed by the attackers. This report is based on a representative sample of the total websites we worked on for Quarter 1, Calendar Year (CY) 2016 (CY16-Q1). A total of 11,485 infected websites were used. This is the sampling that provided us with the most consistent data from which we could prepare this report.

CMS Analysis

Based on our data, the three CMS platforms most being affected are WordPress, Joomla! and Magento. 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 and their hosts.

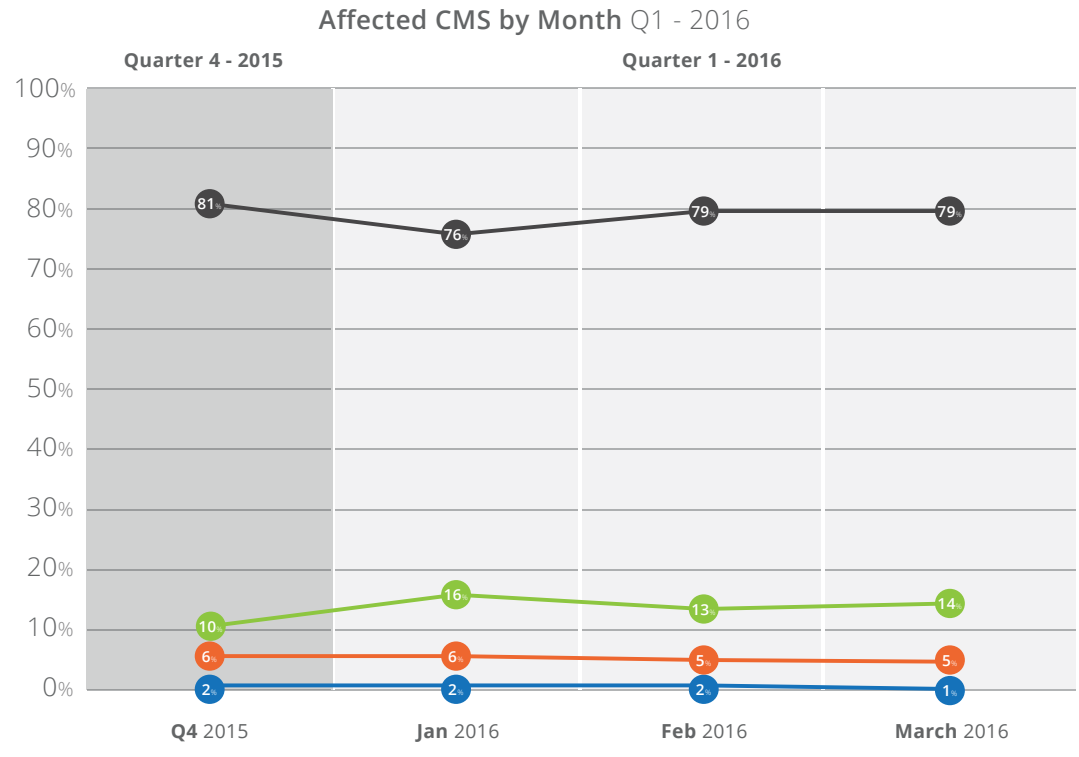


Over 78% of all the websites we worked on in the first quarter of 2016 were built on the WordPress platform, followed by Joomla! at 14%. WordPress is the leading open-source CMS platform on the market adopted by businesses of all sizes and everyday website owners. In all instances, regardless of platform, the leading cause of infection could be traced to the exploitation of software vulnerabilities in the platform's extensible components, not its core. Extensible components directly relate to the integration of plugins, extensions, components, modules, templates, themes and other similar integrations.

The vBulletin and Modx percentages are small, relatively speaking, and were removed from the rest of the report.

CMS Analysis (Continued)

The platform distribution in the Sucuri environment was consistent over the quarter:



	Q4 2015	Jan 2016	Feb 2016	March 2016
WordPress	81%	76%	79%	79%
Joomla!	10%	16%	13%	14%
Magento	6%	6%	5%	5%
Drupal	2%	2%	2%	1%

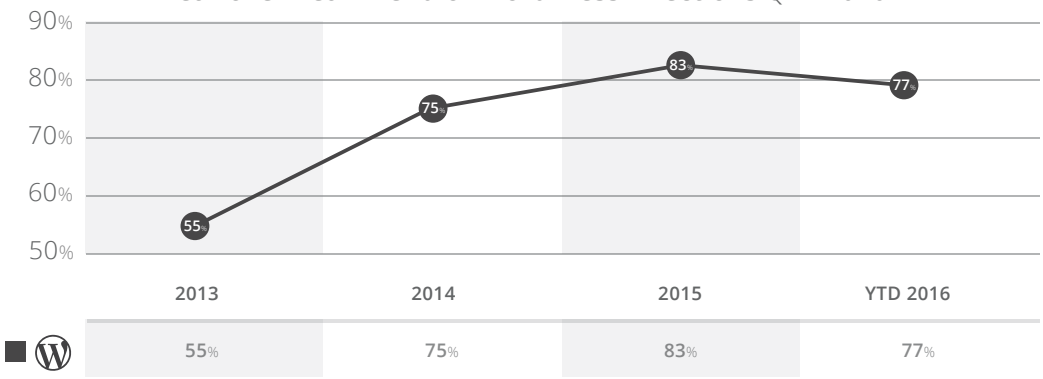
Had there been a major outbreak, the chart would have clearly depicted the anomaly with platform growth in the affected month. With this information, we can summize that nothing significant or out of the ordinary occurred during the first quarter of 2016. When comparing to Quarter 4 of Calendar Year (CY) 2015 we see there was a modest drop in infection in the WordPress platform and an increase in the infections of Joomla!-based websites.

Year after year things have looked fairly consistent, with WordPress leading the pack and Joomla! a distant second. There was a modest dip in 2015 of Joomla! sites, but it has picked up slightly in Quarter 1 of 2016.

CMS Analysis (Continued)

The impacts to the WordPress stems from vulnerability exploitation attempts against vulnerability software, specifically in plugins. The three leading Software vulnerabilities affecting the most websites in the first quarter were the RevSlider and GravityForms plugins, followed by the TimThumb script.

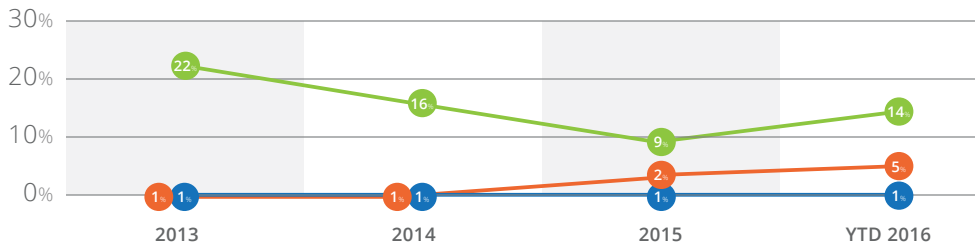
Year over Year Trend of WordPress infections Q1 - 2016



	2013	2014	2015	YTD 2016
WordPress	55%	75%	83%	77%

Another interesting change can be seen in the Magento platform. It has become a bigger target as online commerce (i.e., e-commerce) continues to grow. This can be seen in the 200% growth in infection between 2015 and Q1 2016.

Year over Year Trend of CMS infections Q1 - 2016



	2013	2014	2015	YTD 2016
	22%	16%	9%	14%
	1%	1%	2%	5%
	2%	2%	2%	1%

The increase in Magento compromises seems to be related to the ShopLift Supee 5344 vulnerability, **disclosed by CheckPoint**, in which they discovered a Remote Code Execution (RCE) that could be easily exploitable. Within 24 hours of its disclosure **we reported live attacks**, specifically targeting the SQL injection (SQLi) vulnerability and inserting malicious administrators into the Magento database. Additionally, compromises were correlated with a Stored Cross-site Scripting (XSS) vulnerability, **identified and disclosed by the Sucuri research team**, in which attackers could take over administrator accounts and insert new ones. The ShopLift vulnerability is the most serious of the disclosed vulnerabilities.

Additionally, unlike other platforms in which attackers are using websites to distribute malware, like phishing or SEO spam, the **attackers are targeting credit card** data via card scrapers. Stealing the data itself is not a surprise. It's the obvious target with an online commerce site. But the fact that we're seeing more card scrapers specific to Magento leads us to believe that the Magento users are processing card data locally on the web server in the place of using third-party integrators to handle the processing of the card information, and the attackers know this.

Outdated CMS Analysis

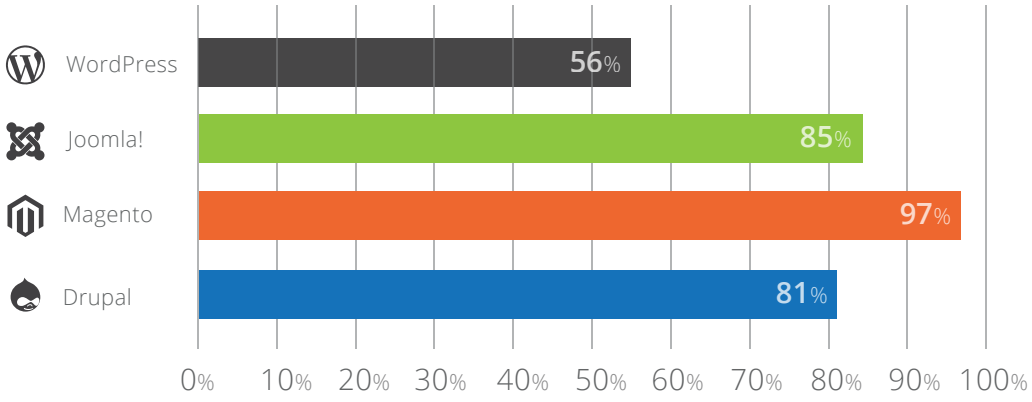
While the leading cause of infections stemmed from vulnerabilities found in the extensible components of the CMS applications, it's important to analyze and understand the state of CMS's in the websites we worked on. Out-of-date software has been a serious issue since the first piece of code was put to virtual paper. With enough time, motivation, and resources, attackers will identify and potentially exploit software vulnerabilities.

To make the data manageable, we've divided it into two distinct categories specific to the core of the application, not its extensible components:

- Updated CMS,
- Outdated CMS.

A CMS was considered out of date if it was not on the latest recommended security version at the time of the incident response.

Breakdown of Top Outdated WordPress Plugins Q1 - 2016



WordPress has been leading the pack with backwards compatibility and ease of updates for website owners, but the same cannot be said for other CMS platforms like Joomla!, Magento and Drupal. Even with the efforts the WordPress platform has placed on the importance of updates, out of the 11k + infected websites, 56% of the total WP infected websites, were still out of date. This is good, when compared to Joomla! (84%), Magento (96%), and Drupal (81%). The challenge of being out of date stems primarily from three places: highly customized deployments, issues with backward compatibility, and the lack of staff available to assist in the migration. These tend to create upgrade and patching issues for the organizations that leverage them for their websites, through incompatibility issues and potential impacts to the website's availability.

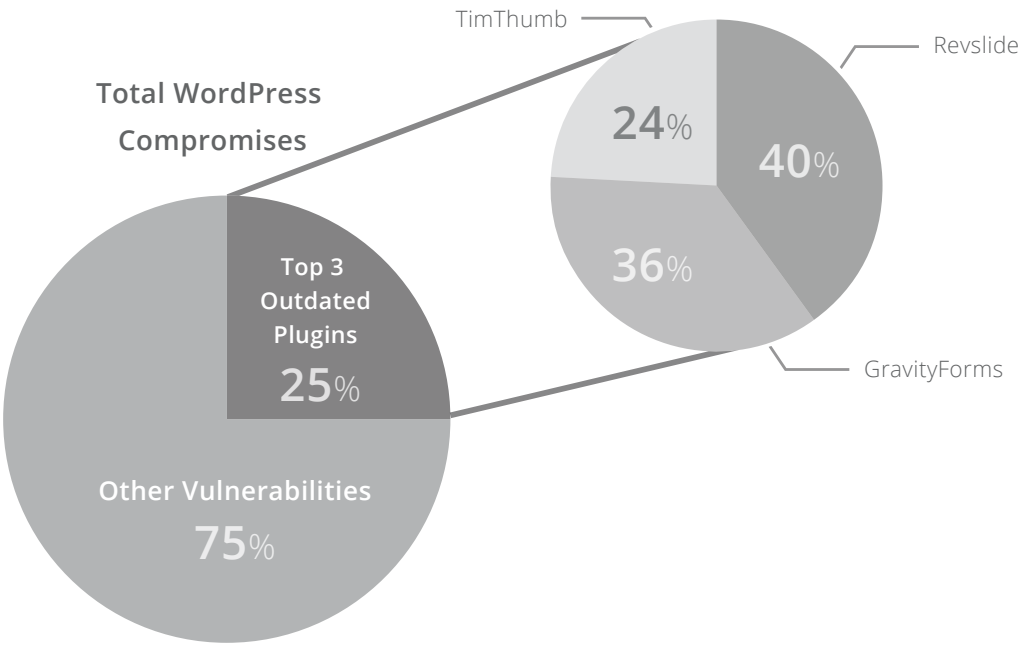
These statistics talk to the challenges website owners face, regardless of size, business, or industry. Website owners are unable to keep up with the emerging threats. As well, the guidance they receive to "stay current" or "just update" is not enough. Website owners are turning to other technologies, like Website Application Firewall (WAF), to give themselves and their organizations the time they require to more efficiently respond to the threats by way of virtual patching and hardening techniques at the edge.

WordPress Deep Dive

With WordPress dominating a very large percentage of the total infected websites we analyzed (77%), we decided to dive deeper to understand the leading causes of infections. With the number of plugins in the repo alone (over 40k) and the plethora of vulnerabilities being disclosed daily, it's sometimes hard to make sense of all the noise.

These were the top three plugins that were out of date and insecure during our cleanup time:

Breakdown of Top Outdated WordPress Plugins Q1 - 2016

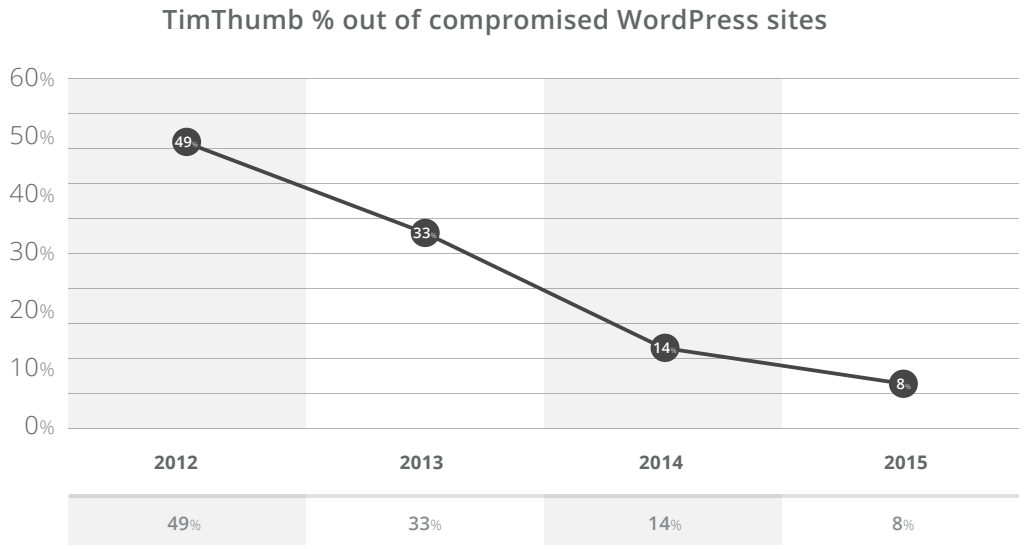


Almost 10% of the compromised WordPress sites that we analyzed had a vulnerable version of RevSlider. When you combine RevSlider, Gravity Forms, and TimThumb,they account for 25% of the total compromised WordPress sites.

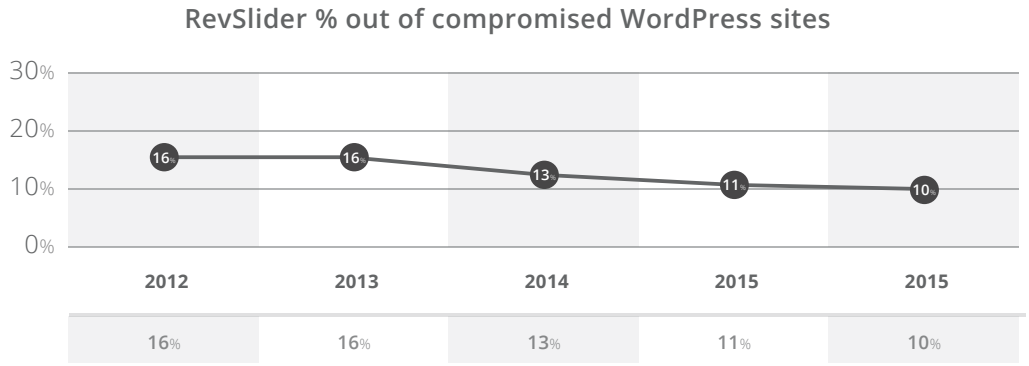
All three plugins had a fix available over a year, with TimThumb going back multiple years (four to be exact, circa 2011). This goes to show and reiterate the challenges the community faces in making website owners aware of the issues, enabling the website owners to patch the issues, and facilitating the everyday maintenance and administration of websites by their webmasters. TimThumb was by far the most interesting revelation in this analysis.

WordPress Deep Dive (Continued)

The charts show the percentage of vulnerable instances of TimThumb found in compromised WordPress websites over the years.



RevSlider never reached the TimThumb scale, but it still affects websites months before it was first disclosed. The biggest challenge with RevSlider however, is that it's embedded within Themes and Frameworks and some website owners are unaware they have it installed until it has been used to adversely affect them via a compromise.



The leading cause of compromises in today's websites comes from the exploitation of software vulnerabilities found in out-of-date software, specifically in its extensible components, as outlined above in the WordPress platform.

The idea of patch and vulnerability management are not new concepts in the world of security or technology. But in the world of everyday business operations, the non-technical staff, it is. Perhaps the most challenging aspect is that this applies to all teams, even those with more formal security controls and processes. The fact is that even large organizations are faced with the same challenges as everyday website owners (i.e., bloggers and small businesses)of staying current as new updates are released to address all issues, including security patches.

Malware Families

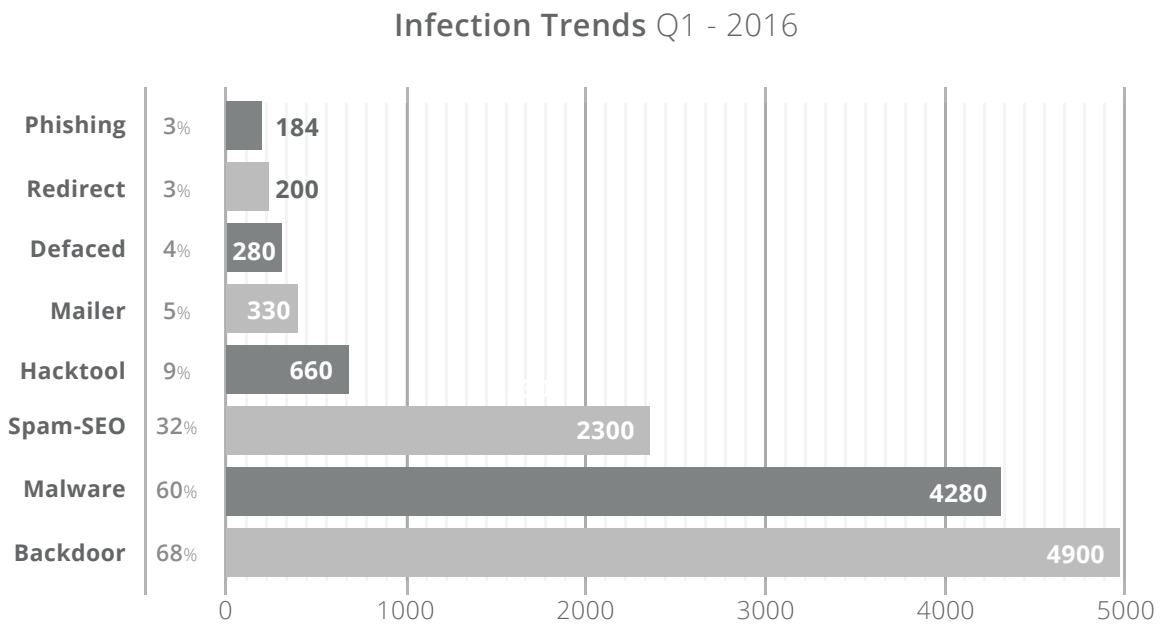
Part of our research over the past quarter includes analyzing the various infection trends, specifically how they correlate to our malware families. Malware families allow our team to better assess and understand the attackers actions, which inevitably leads us to their intentions.

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 or goal in how they plan to leverage their new asset (asset is the term used to describe the website that they have acquired and is now part of their network). On average, we clean 132 files per compromised site. This shows how deep the malware can be embedded within a website.

Over the course of the previous quarter, 66% 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 illusiveness to most website scanning technologies. The backdoors themselves are often well written, do not always employ obfuscation, and present no external signs of a compromise to website visitors.

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.

Malware Families (Continued)



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.
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..).

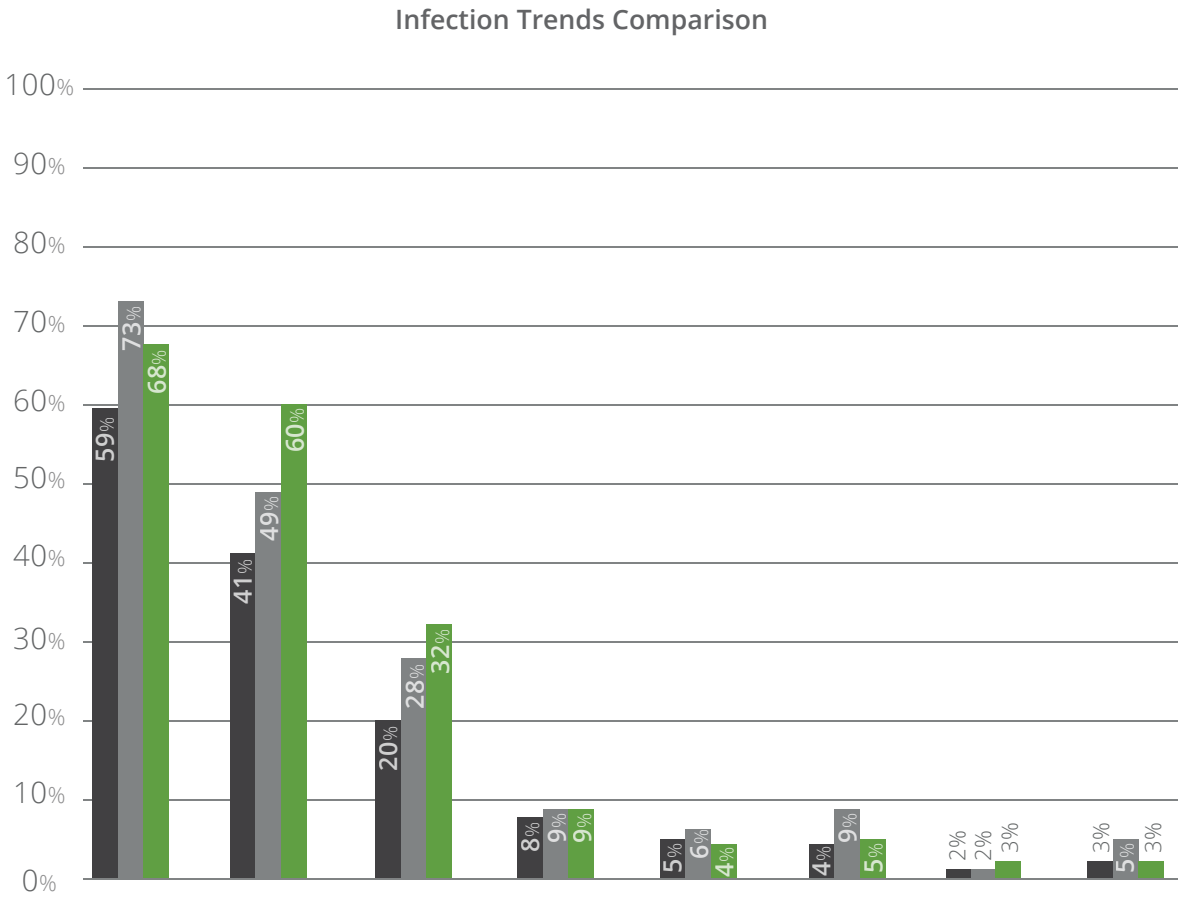
Approximately 31% of all infection cases are misused for SEO Spam campaigns (either through PHP, Database injections or .htaccess redirections) where the site was infected with spam content or redirected visitors to spam-specific pages. The content used is often in the form of Pharmaceutical ad placements (i.e., erectile dysfunction, Viagra, Cialis, etc...) and includes others injections for industries like Fashion and Entertainment (i.e., Casino, Porn).

Having SEO Spam make up 31% of the infections we're seeing is interesting, specifically because it's not part of the warnings Google or any other search engines are reporting on. Year after year, we're seeing this number continue to rise. In 2014, it was at about 20% of the total compromised sites; in 2015 it grew to 28% and as of 2016 it's at 32% and steadily rising.

Malware Families (Continued)

The number of defacements have gone down to about 3%, but that's not surprising. The economic benefits of attacks that successfully compromise websites is growing. As more players get involved, more emphasis is put on doing something substantial with the compromised environment.

Approximately 70% of all infected websites had some form of backdoor. This talks to the growing sophistication by the attackers to ensure they retain control of the environment. It's also one of the leading causes of website reinfections. They present a unique challenge to website owners. Most scanning technologies are ineffective at detecting these paylods.



	Backdoor	Malware	Spam-SEO	Hacktool	Deface	Redirect	Phishing	Mailer
2014	59%	41%	20%	8%	5%	4%	2%	3%
2015	76%	49%	28%	9%	6%	9%	2%	5%
Q1 2016	68%	60%	32%	9%	4%	5%	3%	3%

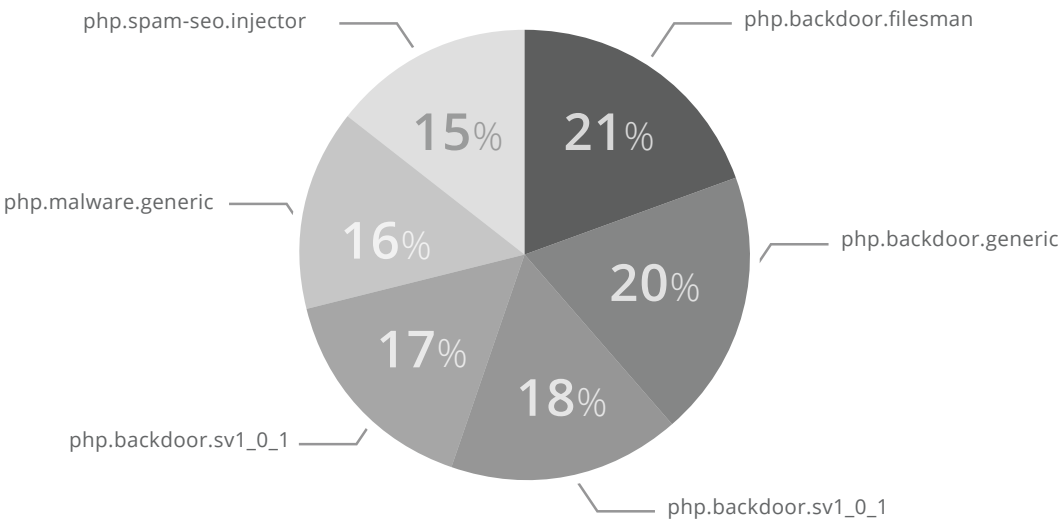
Malware Families (Continued)

On average, we clean 132 files per compromised site. This shows how deep the

malware can be embedded within a website. It also explains why Google sees a 30% reinfection rate via their webmaster tool, which speaks directly to the challenges website owners face when trying to fix their own infected websites.

When we look at signature types we can see the top malware for the quarter:

Top Malwares for Q1 - 2016



The Filesman backdoor is No.1 in terms of the signature type we find the most often in the compromised websites we clean. Filesman is a feature-rich backdoor that allows an attacker full control of the site.

Conclusion

If there is one thing we know from this report is that vulnerable software is a big problem, contributing to a large number of compromises. The blanket guidance to stay current and update is falling on deaf ears. Some initiatives, like those undertaken by WordPress - emphasis on backward compatibility and auto-updates - are having positives effects on the core of the platform, but we know that the majority of the compromises are coming from a platform's extensible components, not its core. Additionally, these initiatives are not global across all platforms.

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. As the technical aptitude required to have a website drops, the inverse will be seen in attacks (increasing as they are dependent on its weakest link, the webmaster). There is a sharp drop off in the knowledge required to have a website, which is breeding the wrong mindset with website owners and service providers alike. This leads to a rude awakening for website owners as established entities, like Google, take a hard stance against malicious websites.

The argument that website owners should simply update, isn't going to be enough. Most of these websites are but one piece of a much larger, complex, environment in which website owners integrate everything they have access too. It's not that a website owner needs to focus on the single instance of WordPress, Joomla!, Magento or Drupal, but rather all the websites within the same environment to avoid things like cross-site contamination. This is complicated by the different deployment and configuration options available, and the general lack of knowledge by the website owner. These challenges are not only affecting small website owners, but can be seen in large organizations as well. Unfortunately the knowledge and education distribution is not as fast as the user adoption.

Thank you for taking the time to read our report and we hope you found it engaging and thoughtful. If there is additional information you think we should be tracking and reporting on, please let us know. We have a number of new datasets we've started to track for the Q2 report which we hope you'll find just as engaging.

SucuriSecurity
sucuri.net
info@sucuri.net
1.888.873.0817