SiteLock

SiteLock Website Security Insider

Q2 2018

Table of Contents

Page Number

Executive Summary 1

Malware 2

Web Application Firewalls (WAF) and Bots 4

Vulnerabilities and Patching 5

Risk Assessment and Social Media 7

Content Management Systems (CMS) 9

- WordPress 10
- Joomla! 11
- Drupal 12

Conclusion 13

Appendix 14

Glossary 18

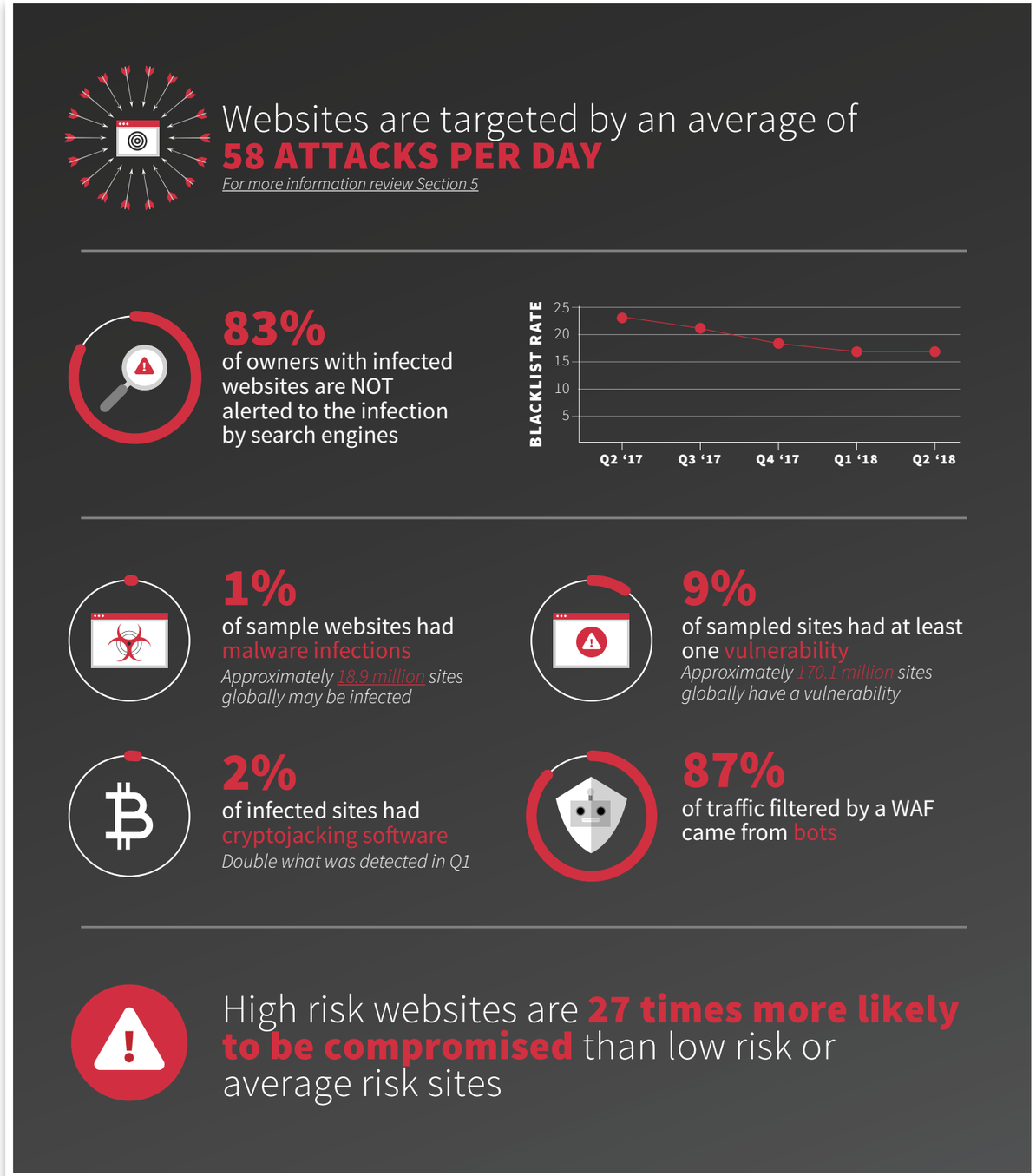
Section 1

Welcome to the Website Security Insider

"Who's responsible for website security?" This question regularly sparks heated debate between website hosts and their customers. When something goes wrong, website owners point fingers at everyone but themselves and place particular blame on their hosting providers. In reality, hosting providers manage their customers' network and server security, therefore website owners must be accountable for the security of their website applications.

The continued misconception over who is truly responsible for website security has left websites increasingly vulnerable to bad actors over the past quarter. To examine these threats facing website owners daily, SiteLock analyzes data derived from 10 million protected sites, from small businesses to enterprises. During our review of data from Q2 2018, several trends came to the forefront.

It has become apparent that cybercriminals are here to stay, and no site is too small to be targeted. The SiteLock Website Security Insider Q2 2018 offers valuable insight into cybercriminal activity, demonstrates how these trends apply to day to day business, and provides effective tips on how to keep your website secure. The analysis will give website owners and cybersecurity personnel the knowledge they need to tackle modern website security.



Section 2

Malware: The Oldies Are Still Goodies

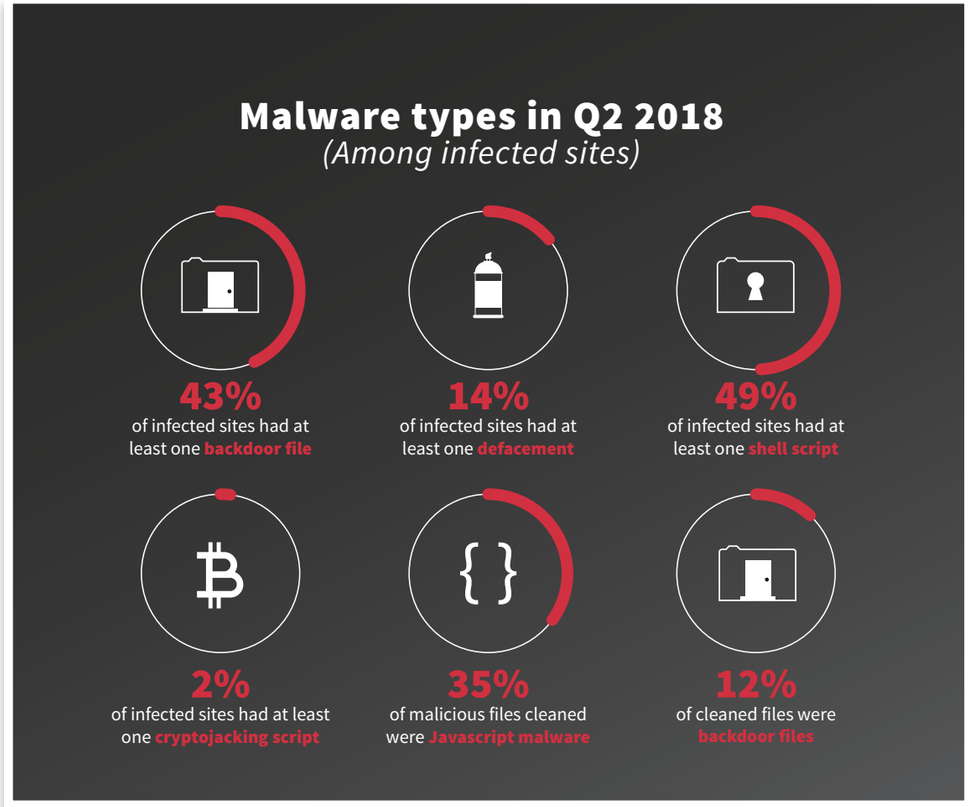
In Q2 2018, SiteLock examined more than 6 million websites protected by malware scanners. Our study revealed that cybercriminals are continuing to mount both new and traditional malware attacks. Using this analysis of malicious activity, we are also able to provide new tips and insights on how to protect your website from these attacks.

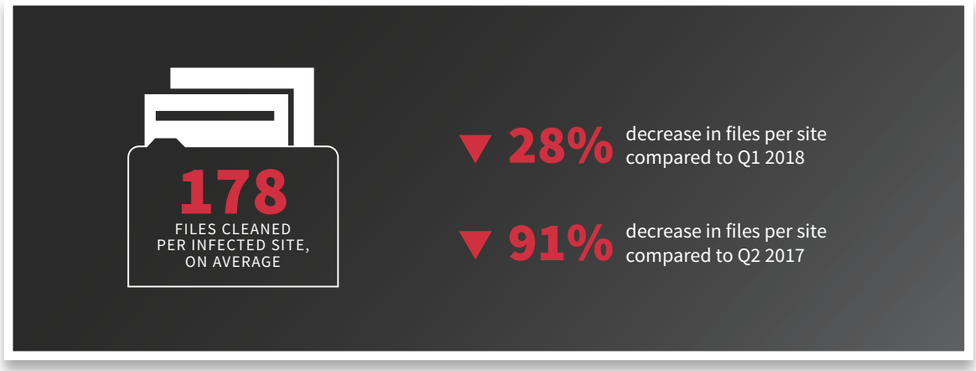
Malware Trends

The rate of tried and true malware attacks such as backdoors and defacements remained steady in Q2. However, the number of sites infected with a relatively new form of malware, cryptojacking, doubled from Q1 to Q2 2018. Additionally, there was a 16 percent increase in the prevalence of malicious Javascript files during the quarter. This new trend is not surprising because many cryptojacking scripts use Javascript kits to deploy and collect the mined cryptocurrency. Because cryptojacking and Javascript are often symptomless to the website owner, they are becoming a new favorite weapon of cybercriminals.

Counter to the increase in silent symptomless attacks, decreases in the number of traditionally noisier attacks containing a large number of files were detected. For example the prevalence of SEO spam, which traditionally contain many files, has shown significant decreases. The amount of SEO spam cleaned this quarter dropped a staggering 58 percent from the year before, a decrease of 4 percent from Q1 to Q2. Additionally, the average number of malicious files removed from infected sites decreased by 28 percent from the previous quarter, indicating not that attacks are decreasing, but that attackers are using smaller and sneakier attack kits.

As malware scanning technology improves, more conspicuous attacks, such as SEO spam and defacements, will continue to make way for sneakier and more profitable attacks, like backdoors used to deploy Javascript and cryptominers. This approach has minimal outward symptoms, such as a loss of search engine visibility or decreased site uptime. As such, these malicious files are less likely to be detected and removed from the compromised site.



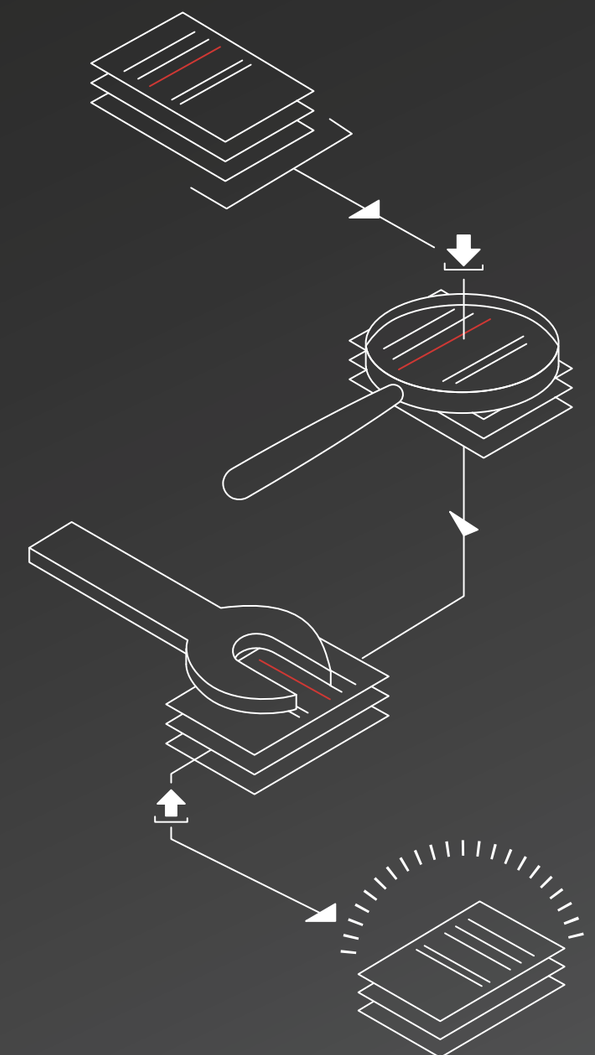


What to Look For

For years, cybersecurity professionals have rallied behind the message that all website owners and developers should be able to complete a basic review of their files for suspicious or unusual content. However, many do not know that bad actors often bury attack kits several directories deep, causing them to be missed by the naked eye. For example, overlooking a spam attack kit can wreak havoc on the search engine results of those sites, causing the site to lose customer trust and revenue—all without the site owner ever being alerted.

How do you combat commonly buried malicious content?

Use a file-based inside-out malware scanner. Malware scanners that access your website via FTP can scan every directory on your website for malicious, suspicious, and changed content. We recommend choosing a scanner that can also automatically remove malware upon detection. While a skilled web developer may be able to find buried attack kits, it will always be more efficient and effective to use an automated and proactive scanning solution.



Section 3

Good Blocks and Bad Bots - Web Application Firewalls

Websites are targeted by an average of **58 ATTACKS PER DAY**

A 16% INCREASE COMPARED TO Q1 2018

Malicious bots represent 87% of all traffic filtered by our WAFs

Suspicious bots represent 6% of all traffic filtered by our WAFs

Visitors from blacklisted countries represent 3% of all traffic filtered by our WAFs

Today, a stunning 60 percent of all website traffic comes from internet bots—not humans. While there are good bots in the mix, such as search engine crawlers used to index websites, far more bot traffic is malicious. Malicious bots can wreak havoc on a website, causing slow load times and even downtime if left unchecked. Bots can also be used to launch attacks that exploit common vulnerabilities, such as cross-site scripting (XSS) and load backdoor files for attackers to use on victimized sites later. In Q2 2018, we analyzed 75,000 websites protected by SiteLock's web application firewall (WAF) and advanced traffic filtering to study the activity of these malicious bots.

Automated Attacks

Cybercriminals are continuously working to hone their craft. They are not only getting better and quieter with their attacks but also making them easier to launch through automation. For example, clicking a single button that scans for and exploits vulnerabilities on thousands of websites at once is an easy way to make attacks more profitable. This is evident in the 16 percent increase in daily attacks on websites compared to Q1 2018. Additionally, bot traffic blocked by web application firewalls continues to account for the majority (87 percent) of blocked website traffic.

Seek and Destroy

Automated attacks and web robots may sound like a science fiction scenario, but they're a very real-world threat to websites of all shapes and sizes. For example, a small business owner running an e-commerce site could miss a website application update, resulting in a SQL injection (SQLi) vulnerability being left on the site. If this website is not protected by a WAF, it is highly visible to malicious bots. As a result, cybercriminals using custom bots to scan for such vulnerabilities will be able to automatically detect and launch an attack on the unprotected site. Because a single SQLi vulnerability could cripple a website with up to 818 vulnerable pages, attackers would be able to gain full access to this site's e-commerce admin panel and customer credit card information from any page of the store.

HOW TO CLOAK YOUR SITE FROM BAD BOTS

While not all bots are malicious, the majority are—and they pose a considerable threat. The fastest and most effective way to protect your website from malicious bot traffic is to implement a web application firewall (WAF). WAF settings can be customized to blacklist known malicious bots, visitors from certain countries known for launching attacks, and suspicious bots not yet recognized as malicious. A WAF can be deployed and begin protecting a site within minutes for virtually instant protection from evolving threats and automated attacks.

Section 4

Fixing Cracks in the Armor - Vulnerabilities and Patching

As cybercrime continues to plague well-known brands' websites, more independent website owners are increasingly aware their websites could also be attacked. When the media covers these security snafus, a key piece often left out of these stories is—How did this happen in the first place? The answer: unpatched vulnerabilities. Whether it's ignorance or oversight, unpatched vulnerabilities in website applications lead to website exploits and data theft.

In Q2 2018, SiteLock studied a sample of more than 6 million websites to identify trends associated with the three most common vulnerabilities: cross-site scripting (XSS), SQL Injection (SQLi), and cross-site request forgery (CSRF). By understanding the flaws that lead to compromise, website owners will be better prepared to defend against these types of exploits.

9% of sampled sites had at least one vulnerability

Globally, up to 171.3 million websites have a vulnerability

Cross-site scripting (XSS)

XSS vulnerabilities allow attackers to inject malicious scripts into legitimate websites. These are often used in visitor attacks, where the website visitor is targeted by the malicious script.

- **2%** of sites had XSS vulnerabilities
- Potentially **30 million** websites globally may have an XSS vulnerability
- Sites with an XSS vulnerability are **5 times more likely to be infected with malware** than the average website

SQL injection (SQLi)

SQLi vulnerabilities allow attackers to inject malicious database code into insecure website text fields or forms. This can allow cybercriminals to gain full access to a website's MySQL database, administrative back end, or even the entire website to steal information or deface the site.

- **7%** of sites had SQLi vulnerabilities
- Potentially **126 million** websites globally may have an SQLi vulnerability
- Sites with an SQLi vulnerability are **4 times more likely to be infected with malware** than the average website

Cross-site request forgery (CSRF)

CSRF vulnerabilities allow attackers to force authenticated users to perform unauthorized actions while logged into vulnerable applications. This could allow an attacker to force a user to transfer funds or change their login credentials. These attacks are often coupled with social engineering.

- **0.2%** of sites had CSRF vulnerabilities
- Potentially **3.4 million** websites globally may have an CSRF vulnerability
- Sites with an CSRF vulnerability are **2 times more likely to be infected with malware** than the average website

Patches Released During Q2

WordPress
70 patches addressing
5 vulnerabilities

Joomla!
480 patches addressing
24 vulnerabilities

Drupal
549 patches addressing
32 vulnerabilities

The Most Common Flaws

The number of websites with at least one vulnerability (XSS, CSRF, or SQLi) reached 9 percent, a 3 percent increase over last quarter. Worldwide, there are as many as 171.3 million websites that may have a vulnerability that could expose sensitive data to cybercriminals. As the barrier to entry into online business continues to get lower, more and more sites will become vulnerable to attack.

Vulnerabilities are often found in open source applications, such as Joomla!, WordPress, and Drupal, and their associated plugins and themes. Because of the way that most CMS applications serve dynamic content through a limited number of files, a single vulnerability can require updates to as many as 20 individual files. During Q2 2018, we reviewed 4 million open source content management system (CMS) websites that use vulnerability patching services. Across the three largest CMS applications, Joomla!, WordPress, and Drupal, 61 individual vulnerabilities were discovered, requiring an astounding 1,099 individual patches to address them. This is an increase of 48 percent compared to Q1 2018, indicating that vulnerabilities remain a constant theme in the world of cyberthreats.

Protection from the Flaws

While it is understood that open source CMS applications may have vulnerabilities in their code, some traditional wisdom custom coded applications are also vulnerable to these types of attacks—and the consequences are serious. For example, a web developer custom coding a website could accidentally create a single XSS vulnerability in an application. According to our study, this could leave up to 441 pages on the site vulnerable to XSS attacks, that would allow attackers to inject a malicious redirect onto the site, tricking visitors into entering their login credentials on a phishing site. This would likely damage that website or company's reputation and revenue.

Tempering the Flaws

While highly skilled web developers and coders may be able to spot vulnerabilities in their code with the naked eye, it is uncommon and inefficient to trust this method alone. It is recommended that website owners deploy code analysis and vulnerability scanning tools to ensure their websites are free of easily exploited vulnerabilities. Vulnerability scanners should run automatically at least once per week, preferably daily, for sites that are subject to frequent updates and changes. All sites should have a vulnerability scanner that runs each time they are changed or updated to ensure those updates don't create vulnerabilities.

Section 5

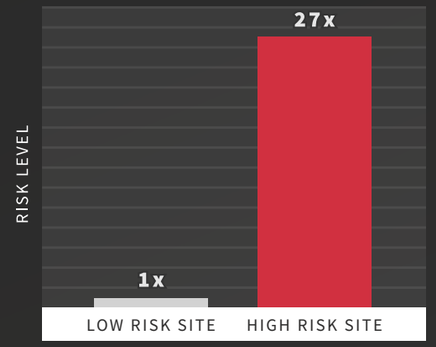
Risky Business and Missed Opportunities - Risk Assessment and Social Media

When it comes to internet security, there's no way to completely eliminate risk. The best anyone can do is lower risk and mitigate the consequences, as all websites - regardless of size - are inherently at risk of compromise or malware infection. Cybercriminals do not discriminate based on a website's size, industry, or traffic; in fact, smaller sites tend to be easier targets because there are fewer security precautions in place. That's because owners of smaller websites often don't realize that it's the very features that make a website popular and engaging (i.e. plugins, more pages, and linked social media accounts) that actually increase the attack surface available to cybercriminals.

During the second quarter of 2018, SiteLock analyzed the risk factors on 6 million websites using a proprietary algorithm that analyzes website risk based on more than 500 variables including complexity, composition and popularity. This analysis revealed an exponential rise in the likelihood of malware infections for sites that ranked high on our risk assessment.

RISK SCORE

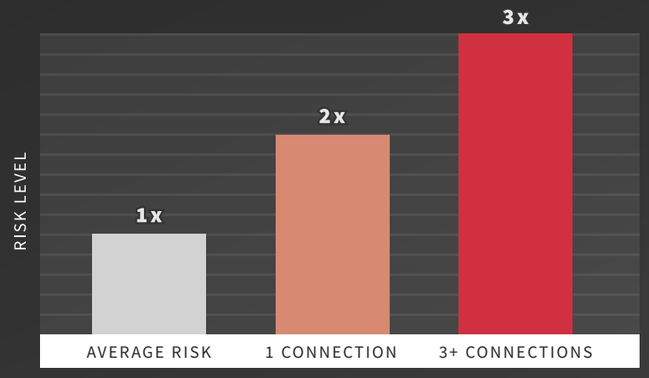
2.47% of websites rated as high risk were infected with malware



High risk websites are 27 times more likely to be infected than low risk websites

an 80% increase from Q1

SOCIAL MEDIA



Connecting to one social media platform makes a site 2x more likely to be infected with malware

Connecting to 3 or more platforms makes a site 3x more likely to be infected with malware

The Risk of Being in Vogue

One of the major factors that increases a website's risk is popularity. When examining site popularity, we look at the impacts of traffic and social media among other variables. Surprisingly, social media popularity presents a unique challenge to small businesses and their websites. While social engagement with customers is critical to developing a business's online presence and reputation, SiteLock data shows that connecting to just one social media platform doubles the chances of a website being compromised. Connecting to three or more social platforms, such as Facebook, Twitter, and Instagram, makes a website three times more likely to be infected with malware than websites that are not connected to social media.

Social media can be used as a weapon against websites because cybercriminals can scan for domain names and information revealed on each platform. This information can be used to launch brute force attacks against website admin credentials or to create phishing campaigns designed to attack website visitors. Businesses with more followers than others have increased visibility, making them prime targets for these types of attacks.

Knowing that social media is critical to building a business, many web developers use plugins to connect sites to their social media platforms. However, vulnerabilities and insecure connections from these plugins can result in malware infections and stolen credentials.

HOW CAN WEBSITE OWNERS PROTECT THEMSELVES WHILE REMAINING ENGAGED?

Always review plugins before installing them and entering your credentials. Read plugin reviews and developer notes to ensure regular security patches are released for your chosen social button plugins. Additionally, it is critical that patches and updates be applied as soon as they are released. Many plugins offer automatic updates and email alerts for when patches are released. Staying informed about update activity will ensure your social media connections don't leave open vulnerabilities on your website.

Section 6

Managing Your Content While Managing Your Risks - CMS Applications

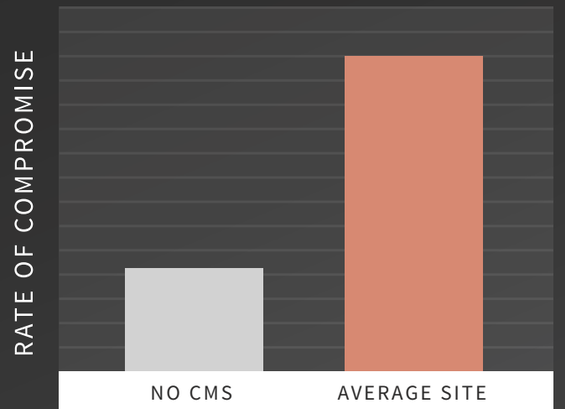
An estimated 53 percent of websites are built on a content management system (CMS). During Q2 2018, SiteLock analyzed more than 6 million websites built using CMS applications and compared them to a control group consisting of sites not built on an open-source CMS platform. After studying the three largest open-source CMS platforms—WordPress, Drupal, and Joomla!—we drew conclusions about the risks associated with using publicly available code to build websites.

Open-source CMS applications have grown in popularity due to their accessibility for even the most novice website owner. This has had amazing benefits, allowing businesses of any size and industry to create an engaging and professional online presence. However, because the code is open source, and novice site owners may not know how to manage that code, these applications can be vulnerable to attack. The following pages examine the risks and provide tips on how you can best protect your website and data without changing platforms.

33%
of websites were running a major CMS, such as WordPress, Drupal, or Joomla!

67%
of websites were not running CMS

Non-CMS sites were found to have malware about 1/3 as frequently as the global population. This equates to a 0.32% infection rate for non-CMS sites.



WordPress Sites and Malware Infections

Approximately 1 in 3 sites on the internet are built using WordPress, making it the most popular open-source CMS application available. In fact, WordPress accounts for 60 percent of all CMS-built websites. Our sample mirrors the global market share for WordPress, with 31 percent of sampled websites using the platform. This sampling allowed us to examine how core version updates impact vulnerabilities and subsequent malware infections on WordPress websites.

MAINTENANCE IS REQUIRED

WordPress allows all website owners to create engaging and professional websites in a cost-effective and accessible way. However, many website owners don't realize that CMS applications, like WordPress, are living and breathing entities that require regular upkeep. During Q2 2018, 28 percent of WordPress sites were not updated to the latest core version. When security updates are not applied to CMS applications, it leaves the site vulnerable to attack.

That said, it is important to note that just updating the core application is not enough to secure a CMS-driven website. Our study revealed that 16 percent of WordPress sites had the latest core version installed, but still had at least one vulnerability (XSS, SQLi, or CSRF). We found that 6 percent of infected WordPress sites, as many as 350,000 sites globally, had up-to-date core installations but still had a vulnerability. These sites were more than likely infected with malware through a vulnerability in either a plugin or theme used on the site. Using responsibly sourced and maintained themes and plugins, as well as applying security updates when they are released, are critical steps to keeping WordPress sites secured.

THREATS BEYOND PLUGINS

One of the unique features of many open-source CMS applications is that they offer an easy-to-use administration panel, often available live on the website. This too, however, can be an additional attack vector for cybercriminals. Developers leaving their "/wp-admin" pages accessible and unencrypted can result in attackers using brute force attacks or "sniffing" passwords typed on public Wi-Fi networks to gain full control of a WordPress site. This could have a catastrophic impact on a website and business.

1% of WordPress sites have malware, which is on par with Q1. Globally, this means 5.8 million WordPress sites may be infected with malware

55% of sites infected with malware were running the latest core versions

24% of WordPress sites had a vulnerability and 16% of WordPress sites had a vulnerability and malware

6% of infected WordPress sites were most likely infected through a vulnerable theme or plugin

HOW TO STOP A HOSTILE TAKEOVER:

There are several ways you can protect your CMS dashboard from potential attackers. First, using a strong passphrase that includes mixed case letters, numbers, and special characters is a must, and it's important to only enter that password over secured networks. Second, change the URL associated with your dashboard from the default using custom plugins. Doing so makes it harder for attackers to gain access to the administration of your site and cause damage.

Joomla!, Updates, and Infections

With more than 59 million active installs (representing 3 percent of the total internet population), Joomla! is one of the most popular open source CMS applications in the world. While it is widely considered to be one of the more flexible and advanced CMS platforms, Joomla! carries a unique set of challenges and security risks. Joomla! can be more difficult to update and patch than other CMS applications, with some security updates breaking contingencies, such as plugins and themes. This can lead website owners to leave vulnerabilities unpatched, allowing cybercriminals to easily capitalize on these vulnerabilities.

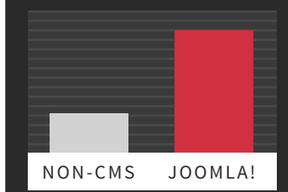
OPEN WINDOWS OR BROKEN WINDOWS?

Application updates can be time consuming, difficult, and sometimes risky, but they are a critical step in keeping your website secure. SiteLock found that 77 percent of Joomla! websites were not running the current secure version. Of those that were running the latest core version, only three percent still had a vulnerability. Furthermore, the majority of malware infections on Joomla! sites are likely caused by vulnerabilities in out-of-date core applications.

While core updates can potentially impact themes and plugins, causing issues for website appearance or functionality, this should not be taken as a sign to skip the updates. Instead, it should be a reminder that sourcing your plugins and themes responsibly is a necessary part of managing your CMS sites. Leaving vulnerabilities unattended in the core application is a dangerous open door, as attackers can use automated bots to scan for and exploit them.

CAN YOU MAKE THE LOCKS AUTOMATIC?

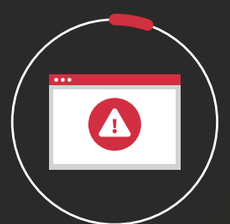
Skipping security updates simply is not an option if you want to keep your website secure. However, there are options for keeping your site safe while planning for these updates. Use an automated application patching service to apply surgical security updates to the core application. This will ensure full version upgrades will not harm your site. The diligent nature of these patches means they won't break themes or plugins, but they will address security vulnerabilities thwarting potential attacks on your site.



Joomla! sites are 3 times more likely to be compromised than non-CMS websites

77% of sampled Joomla! sites were *not* running the latest core security updates

10% were running the latest updates at the time of infection



3% of Joomla! sites had a vulnerability despite running the latest security updates

OVER 99% of infected Joomla! websites were likely compromised through an out-of-date or vulnerable core version

Drupal Makes Headlines Again

At the end of Q1 2018, Drupal announced a critical security update to address a major SQLi (SQL Injection) vulnerability, dubbed "Drupalgeddon2." Throughout the beginning of Q2, Drupal continued to release supplemental security patches and public service announcements reminding users to update their core applications. SiteLock examined sites built with Drupal and protected by malware scanners to determine what impact this kind of critical security update could have on malware infection rates and vulnerabilities in the application.

INCREASED AWARENESS DOES NOT EQUAL INCREASED SECURITY

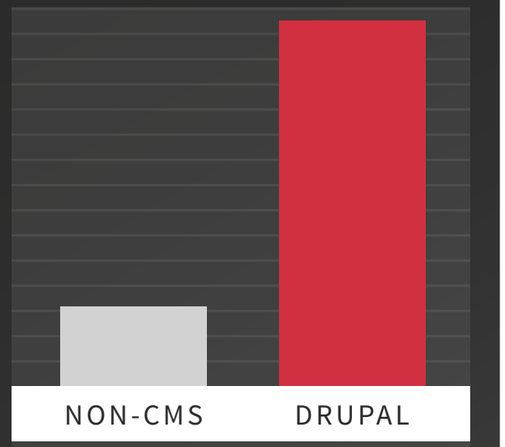
Drupal released multiple patch notices and announcements regarding the critical security vulnerability that impacted over 1 million live sites. Despite this, our research shows that Drupal users did not rush to update their applications. During Q2 2018, 77 percent of Drupal sites were found to be running out of date and potentially vulnerable core versions. Additionally, there was a 4 percent decrease in the number of infected Drupal sites running the latest core version compared to Q1 2018, indicating continued infection through out of date core installations.

However, vulnerable core applications were not the only cause of malware infections during the quarter. Drupal sites were 4.5 times more likely to be infected than non-CMS websites during Q2 2018. Of those that were infected with malware, 5 percent had current core installations, yet they still had vulnerabilities and were infected by malware. Additionally, 33 percent of Drupal sites running the latest core version still had vulnerabilities linked to application add-ons. These exploited vulnerabilities and subsequent malware infections were more than likely the result of out-of-date or otherwise vulnerable themes and plugins. In addition to heeding warnings about security issues in the core application, website owners must continue to update themes and plugins in order to secure their Drupal sites.

23% of Drupal sites were running the latest core versions

33% of Drupal sites with a vulnerability were running the latest core versions
a total of 7% of Drupal sites had vulnerabilities

5% of WordPress sites had a vulnerability and 16% of WordPress sites had a vulnerability and malware



Drupal sites are 4.5 times more likely to be infected with malware than non-CMS websites

HOW TO THWART APPLICATION SCANNERS

One of the features that attracts website owners and developers alike to open-source CMS applications is ease of installation, as most hosting providers offer one-click install options for major CMS platforms. However, these easy installations don't always have security in mind and can leave configuration files accessible to the open web. In order to stop automated scans attackers may launch looking for sensitive information, you should always review and update file permissions. Using a file manager or FTP client, you can ensure that critical configuration files do not have open read or write access. Many CMS applications have support documentation with detailed instructions to help you do this.

Section 7

CONCLUSION

In the constantly changing landscape of cybersecurity, there are a few things that hold true: threats will continue to advance, attackers will evolve, and malware will become increasingly covert. However, website security advice largely stays the same—taking proactive steps to secure websites is the only way to stay ahead of the cybercrime curve. Cybercrime will only continue to rise, forcing website owners to own the security of their own websites.

Moving into the remainder of 2018, there's no indication that cyberattacks will slow down. While the average number of attacks on websites per day may fluctuate, there's no question that attacks will continue and likely accelerate. Based on SiteLock data, we predict a continued rise in symptomless attacks, such as cryptojacking.

As website owners take accountability for their data security, SiteLock will continue to remain a trusted partner and resource to assist them.

Appendix

KEY STATISTICS

Websites experience an average of 58 attacks per day
- 16% increase over Q1 2018
- 8% decrease from Q2 2017

87% of traffic blocked by the SiteLock WAF was bots
- 17% of infected sites were blacklisted
- 6% decrease from Q2 of last year

On average 1% of sampled sites were infected with malware

The average malware infection resulted in 178 cleaned files
- 28% decrease from Q1 2018
- 91% decrease from Q2 2017

Malware:
- 46% of infected sites had at least one filehacker
- 43% of infected sites had at least one backdoor file
- 49% of infected sites had at least one shell script
- 2% of infected sites had at least one cryptojacking script
  - ***2 times what was detected last quarter***
- 35% of malicious files cleaned were Javascript malware
  - ***a 16% increase from last quarter correlating to the increase in cryptojacking which frequently uses Javascript***

Vulnerabilities - Approximately 9% of sampled sites had a vulnerability
- XSS Vuln - 1.56% of sites have an XSS vulnerability, on par with last quarter
  - ***2.56% of sites with an XSS vulnerability have malware***
- SQLi vuln - 7.19% of sites have a SQLi vulnerability
  - ***2.94% of sites with a SQLi vuln also have malware***
- CSRF - .19% of sites have a CSRF vulnerability
  - ***1.42% of sites with a CSRF vulnerability were infected with malware***

WordPress - 1% of WordPress sites have malware
- 6% of WordPress sites are running the latest core versions but still have a vulnerability and malware, likely meaning they were compromised through a vulnerable theme or plugin

Joomla! - 1% of Joomla! sites have malware
- 0.51% of infected Joomla! Sites were most likely infected through a vulnerable theme or plugin

Drupal - 1.5% of Drupal sites have malware
- 5% of infected Drupal sites were most likely infected through a vulnerable plugin or theme

Non-CMS sites
- 0.32% of sites not running a CMS are infected with malware

Risk Score
- High risk websites are 27 times more likely to be infected than low risk websites

Patching
- 3,756,040 websites protected with patching services
- WordPress: 5 vulnerabilities with 70 patches
- Joomla!: 24 vulnerabilities with 480 patches
- Drupal: 32 vulnerabilities with 549 patches

FULL STATISTICS

General Stats

Q2 2018 - April 2, 2018 - July 1, 2018

Sample Size - 6,043,040 sites protected by scanners

WAF Sample - 63,455

Attacks Per Day

Websites experience an average of 58 attacks per day

This is a 16% increase compared to Q1 2018

This is an 8% decrease compared to Q2 2017

Blocked traffic through the firewall

Backdoor Attacks - 0.03%

Blocked bots - 87%
1% drop from Q1 2018
Same as Q2 2017

XSS attacks - 0.03%

Illegal resource access - 2%

Remote file inclusion - 0.11%

SQLi attacks - 0.54%

Suspicious bots - 6%
1% increase from Q1 2018

DDoS attacks - 0.06%

Visitors from blacklisted countries - 3%

Visitors from blacklisted IPs - 0.02%

Visitors from blacklisted URLs - 0.03%

Blacklisting Stats

17.5% of infected sites were blacklisted
Same as Q1 2018
6% decrease from Q2 2017

WAF Stats

Average bot visits per week across all sites - 155,634,683
Increase in bot visits of 9% from Q1 2018
Average of 2,451 bot visits per site per week
Increase of 17% per site from Q1 2018

Average threats blocked per week across all sites - 578,058
Average of 9 threats blocked per site per week
Decrease of 25% from Q1 2018

Malware Stats

Categories by sites affected

Definition: At least one of each file type was found on these sites

Filehacker - 46%
Down 3% from Q1 2018

Backdoor - 43%
Down 1% from Q1 2018

Shell - 49%
Up 9% from Q1 2018

Malicious Eval Request - 35%
Down 10% from Q1 2018

Uploaders - 29%
Up 1% from Q1 2018

Injectors - 29%
Down 2% from Q1 2018

Malicious .htaccess files - 16%
Up 7% from Q1 2018

Defacements - 14%
Down 4% from Q1 2018
Up 6% from Q2 2017

Redirects - 17%
Up 11% from Q1 2018

Phishing 9%
Up 1% from Q1 2018

Mailers - 11%
Down 1% from Q1 2018

SEO Spam - 9%
Up 3% from Q1 2018
Up 1% from Q2 2017

File Manager - 7%
Down 3% from Q1 2018

Javascript - 10%
Down 1% from Q1 2018

Cryptominer - 2%
Up 1% from Q1 2018 (This represents 2x last quarter)

Malware by files affected

Percentage of the total files cleaned categorized

Javascript - 35%
Up 16% from Q1 2018

Filehacker - 18%
Up 11% from Q1 2018

Backdoor - 12%
Down 19% from Q1 2018
Down 12% from Q2 2017

Phishing - 9%
Down 2% from Q1 2018

Defacements - 4%
Down 7% from Q1 2018

Malicious .htaccess - 4%
Up 1% from Q1 2018

Mailer - 4%
Up 1% from Q1 2018

Malicious Eval Request - 3%
Same as Q1 2018

SEO Spam - 4%
Down 2% from Q1 2018
Down 58% from Q2 2017

Shell - 2%
Same as Q1 2018

Uploaders - 1%
Same as Q1 2018

Redirects - 1%
Down 1% from Q1 2018
Down 7% from Q2 2017

Injectors - 1%
Same as Q1 2018

Scanner Stats

Average infection rate for the entire sample - 0.67%
Global infection rate remained the same from Q1 2018

Average number of files cleaned per site - 178
A decrease of 28% from Q1 2018
A decrease of 91% from Q2 2017

Vulnerability Stats

XSS Vulnerabilities

Sites with an XSS vuln - 1.56%
Increase of 0.22% from Q1 2018

Sites with an XSS vuln and malware - 2.65%

XSS pages per site - 441
Increase of 4.26% from Q1 2018
Increase of 496% from Q2 2017

SQLi Vulnerabilities

Sites with a SQLi vuln - 7.19%
Increase of 2.3% from Q1 2018

Sites with a SQLi vuln and malware - 2.94%

Average SQLi pages per site - 818
Decrease of 20% from Q1 2018
Increase 3990% from Q2 2017

CSRF Vulnerabilities

Sites with a CSRF vuln - .19%
Same as Q1 2018

Sites with a CSRF vuln and malware - 1.42%

Social Media Stats

No Social Media

Sites that do not connect to social media - 79%

Sites that do not connect to social media and have malware - 0.54%

Twitter

Percentage of sites connected to Twitter - 10%

Twitter connected sites with malware - 1.27%

2.3 times more likely to be infected than no social media

Facebook

Percentage of sites connected to Facebook - 19%

Facebook connected sites with malware - 1.15%

2 times more likely to be infected than no social media

LinkedIn

Percentage of sites connected to LinkedIn - 3%

LinkedIn connected sites with malware - 1.35%

2.5 times more likely to be infected with malware than no social media

Instagram

Percentage of sites connected to Instagram - 2%

Instagram connected sites with malware - 1.27%

2.3 times more likely to be infected than no social media

Sites connected to all 4 social platforms

Percentage of sites connected to all platforms - 1%

Connected to all platforms with malware - 1.61%

3 times more likely to be infected than no social media

WordPress Stats

Total WordPress sites sampled - 1.88 million

WordPress sites with malware - 1%
Same as Q1 2018

Total percentage of WordPress sites running the latest core version - 72%

WordPress sites running latest core with malware - 55%
A 15% increase from Q1 2018
A 14% decrease from Q2 2017

WordPress sites with a vulnerability (XSS, SQLi, CSRF) - 24%
WordPress sites with a vulnerability and malware - 1.88%

WordPress sites with a vulnerability running the latest core version - 16%
WordPress sites running latest core, with a vulnerability, and malware - 1.67%

6% of WordPress sites are running the latest core versions but still have a vulnerability and malware, likely meaning they were compromised through a vulnerable theme or plugin.

10% of WordPress sites are ecommerce sites running WooCommerce

Percentage of WooCommerce sites with malware 1%

Same as Q1 2018

Infection Rates based on number of plugins

1-5 plugins - 1%
6-10 plugins - 1.25%
11-20 plugins - 1.54%
20+ plugins - 2.24%
No plugins - 0.12%

Joomla! Stats

Joomla! sites sampled - 62,000

Joomla! sites with malware - 1.66%

Same as Q1 2018

Total percentage of Joomla! Sites running the latest core version - 23%

Joomla! Sites running the latest core version with malware - 10%

Decrease of 8% from Q1 2018

Joomla! sites with a vulnerability - 19%

Joomla! sites with a vulnerability and malware - 1.6%

Joomla! sites with a vulnerability and running the latest core version - 2%

Joomla! sites with a vulnerability, running the latest core version, and infected with malware - 3%
0.51% of infected Joomla! sites were most likely infected through a vulnerable theme or plugin

Drupal Stats

Drupal site count - 21,000

Represents .35% of the sampled population

Drupal sites infected with malware - 1.46%

.43% increase from Q1 2018

Total Drupal sites running the latest core versions - 23%

Infected Drupal sites running the latest core versions - 32%

4% decrease fro Q1 2018

Drupal sites that have a vulnerability - 2%

Drupal sites with a vulnerability and malware - 7%

Drupal sites running the latest core versions with a vulnerability - 33%

Drupal sites running the latest core versions with a vulnerability infected with malware - 3%
5% of infected Drupal sites were most likely infected through a vulnerable plugin or theme.

Non-CMS Sites Stats

Sites sampled not running a CMS - 67%

Non-CMS sites with malware - 0.32%

Risk Score Stats

Infection Rates By Risk Score

Low - .09%
Medium - .03%
High - 2.47%

High risk websites are 27 times more likely to be infected than low risk websites

An 80% increase from Q1 2018

Patching Stats

3,756,040 websites protected by Patchman patching services

Patches and vulnerabilities by CMS:

WordPress: 5 vulnerabilities with 70 patches
Joomla!: 24 vulnerabilities with 480 patches
Drupal: 32 vulnerabilities with 549 patches
WooCommerce: 38 vulnerabilities with 543 patches
Magento: 58 vulnerabilities with 528 patches

Glossary of Terms

Attack Kit - A collection of malicious scripts or files used to compromise and proliferate malware on a website.

Attack Surface - The attack surface refers to the total number of entry points an attacker can use to gain unauthorized access to a website's files or content.

Backdoor File - A backdoor file is a piece of malware designed to allow attackers to gain unauthorized access to a website's content.

Blacklisting - Blacklisting refers to when search engines remove websites from their results. In this report, blacklisted refers to sites that were removed from search engine results as a result of malware.

Bot - Web bots or web robots are programs that automatically crawl websites for content or search engine purposes. These can be either benign or malicious based on the intent of the program.

Compromise - A website compromise refers to when a website is attacked (or hacked) and infected with malicious content. This may also refer to when data is stolen from a website.

Content Management System (CMS) - An application used to build and manage website content. Examples include Magento, Joomla!, Drupal, and WordPress.

CMS Core - The central files that make up a content management system without themes or plugins.

Cross Site Scripting (XSS) Vulnerability - A vulnerability that enables attackers to inject malicious code into website content viewed by visitors/users.

Cyberattack - This refers to any malicious action taken against a website by attackers.

Defacement - When website content is replaced by malware with a web facing message such as "hacked by."

DDOS Attack - A flood of malicious requests sent in order to overwhelm a web server causing websites to become inaccessible.

Eval - A function that runs any code as a legitimate function. Often used to disguise malicious content as benign code.

Malware - Malicious software intended to disable or damage networks, computers, or websites. This report focuses on website malware.

Patch - An update made to code in order to correct a bug or vulnerability.

Plugin - Add on code that enhances the features or functionality of a CMS.

Shell - A file or script used to gain unauthorized access to a website or server, and modify the content.

SQL Injection (SQLi) Vulnerability - A vulnerability that allows attackers to inject malicious code into a MySQL database using insecure website forms or fields.

Vulnerability - A flaw in a website's code that can lead to infection or injection of malicious content.

Web Application Firewall (WAF) - A layer of protection placed on HTTP applications using a set of rules designed to block malicious traffic or content from reaching websites.