

SiteLock 2019 **Website Security Report**

Protecting Websites in the
Age of Stealth Attacks

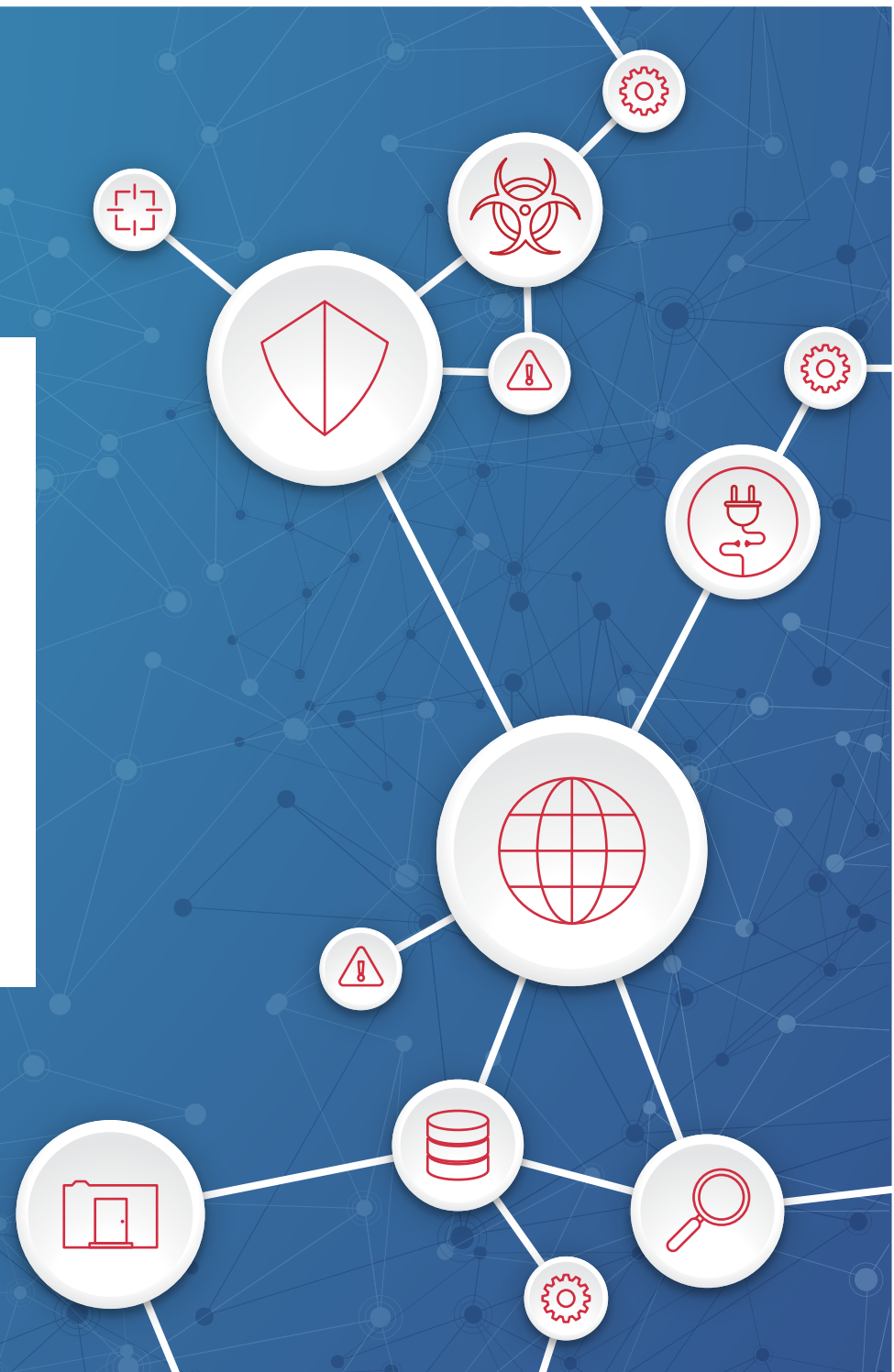


Table of Contents

Page Number

<u>Executive Summary</u>	1
<u>Attack Patterns and Risk Factors</u>	3
<u>Vulnerabilities</u>	4
<u>Malware</u>	5
<u>Conclusion</u>	6
<u>Appendix</u>	7

Executive Summary

Cryptojacking, nation-state attacks and compromised elections dominated the website security realm in 2018. The trend across all of them? High-profile, timely cybercrime.

However, after studying the website attacks that plagued 2018, a new trend arises. Rather than relying on hyped-up attack methods like cryptojacking, cybercriminals appear to be opting for more stealthy attacks to achieve greater success.

The SiteLock 2019 Website Security Report analyzes more than 6 million websites to determine the most prevalent cyberthreats websites face today. Using proprietary algorithms and technology, SiteLock has identified the top website risk factors and emerging trends in 2019.

Throughout this report, we explore three primary topics that drive website security:

- Attack patterns and risk factors
- Web code vulnerabilities
- Malware types

Website attack attempts per day grew by 59% from January 2018 to December 2018, ending at a peak of 80 attacks per day and averaging 62 attacks per day for the year. Rising attack volume suggests cybercriminals are automating their attacks to expand their reach and frequency. However, the sample of infected websites remained steady at about 60,000 throughout the year, indicating that website security tools are likely becoming more successful at combating the increasing number of attacks.

Despite [predictions](#) that cryptomining would be the most pervasive threat of 2018, cryptojacking actually plateaued at 2% last year. Between the crypto crash and Bitcoin losing more than half of its value, it's likely that cybercriminals turned to more stable and lucrative attack methods.

Only 15% of malware-infected websites were blacklisted in 2018, which is a 4% decrease from the start of the year to the end. Many website owners assume a search engine will alert them if malware is on their site. However, that is not the case. Search engines are using greater caution when blacklisting websites to avoid reporting errors at the site owner's expense. When a blacklisting occurs, the consequences can impact a website's traffic, reputation, and even profitability.



Analysis from this report will help website owners understand today's attack surface, enabling them to make educated and proactive decisions about their website security in the future.

Attack Patterns & Risk Factors



17.6 million websites
have malware at any given time

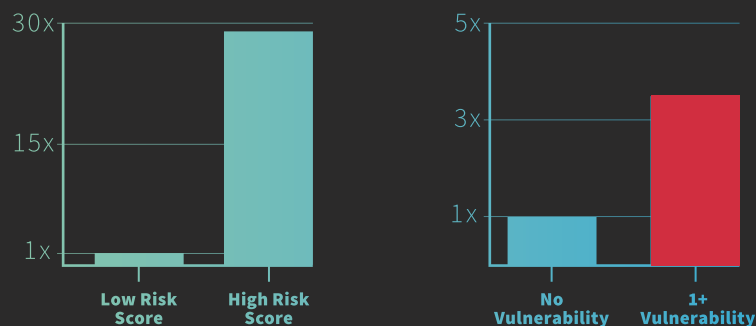
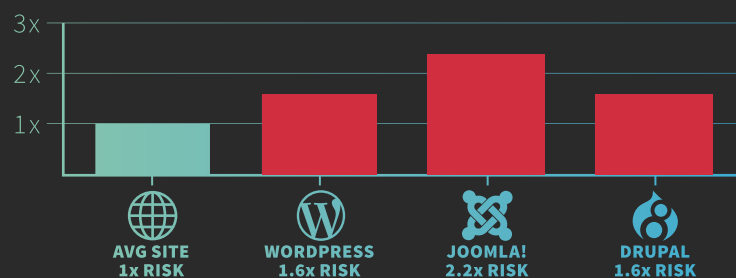


Average of **2,354**
bot visits per
site per week



Only 15% of websites infected
with malware were **blacklisted**
by search engines

RISK OF INFECTION



Websites experienced a staggering 62 attacks per day on average from more than 330 bots. Despite the high volume of website attacks, the number of infected websites remained constant at 1% throughout 2018, equating to 17.6 million websites worldwide at any given time. These findings suggest that website security solutions are becoming more effective to defend against the increasing volume and sophistication of attacks.

A key indicator of a site's likelihood of compromise comes down to its risk factors. SiteLock used its proprietary Risk Assessment, which analyzes more than 500 variables, to determine the factors that make a site susceptible to a breach on a scale of low, medium, and high. These variables are grouped into three main categories: website complexity, such as the size of the website; site popularity, such as site traffic and social media

presence; and site composition, like the software, content management system (CMS), plugins, and themes used to build the site. When deemed high-risk, a site is 26 times more likely to be infected than a low-risk, rudimentary site, such as an informational website that doesn't collect any visitor data or take payments.

It's important to note that no matter a website's level of risk, taking a proactive approach is critical to preventing malware or other threats. Additionally, too many businesses rely on search engines to flag their sites for malware when they should be proactively monitoring with their own tools before a blacklisting occurs. In fact, SiteLock found that search engines flagged only 15% of malware-infected websites, proving their unreliability as a tool in a holistic website security strategy.

Vulnerabilities

XSS - Cross-Site Scripting

- **1.44%** of sites have an **XSS vulnerability**
- **3%** of sites with XSS vulnerabilities **have malware**
- **1,681,900** Total pages with XSS vulnerabilities

SQLi - SQL Injection

- **6%** of sites have an **SQLi vulnerability**
- **2%** of sites with SQLi vulnerabilities **have malware**
- **349,161** Total pages with SQLi vulnerabilities

CSRF - Cross-Site Request Forgery

- **1%** of sites have an **CSRF vulnerability**
- **3%** of sites with CSRF vulnerabilities **have malware**

THREATS BY POPULAR CMS



NO CMS
.05%



WORDPRESS
20%



JOOMLA!
15%



DRUPAL
2%

SiteLock's analysis of website security in 2018 included a look at three types of common vulnerabilities: Cross-site scripting (XSS), SQL injection (SQLi), and cross-site request forgery (CSRF). As noted, open-source CMS applications have grown in popularity due to their accessibility for beginner website owners. In fact, about [38% of sites](#) on the internet are built using WordPress, Joomla!, or Drupal CMS platforms.

These CMS platforms offer amazing benefits, allowing businesses of any size and industry to create an engaging and professional online presence. However, novice site owners may not know how to properly manage the security of that code or any add-on resources like plugins and themes, making their sites more susceptible to these weaknesses.

SiteLock compared the original sample of 6 million websites built using CMS applications to a control

group consisting of non-CMS-built sites. Findings reveal that 20% of WordPress sites, 15% of Joomla! sites, and 2% of Drupal sites had at least one XSS, SQLi, or CSRF vulnerability.

According to SiteLock data, vulnerabilities plague CMS sites even when they are running the latest core versions, indicating that solely patching or updating your CMS application is not enough to fully secure your website. Individual themes and plugins must be closely maintained as well. For example, 34% of Drupal sites running the latest core version still had a vulnerability, while 9% of Joomla! sites and 4% of WordPress sites struggled with the same issue.

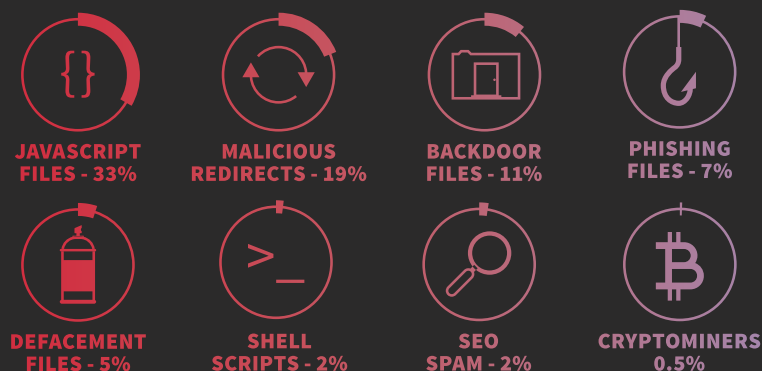
If your team runs its online presence from a CMS-built site, you must implement a holistic website security strategy to prevent vulnerabilities and a website compromise.

Malware

INFECTIONS FOUND ON HACKED SITES BROKEN DOWN BY MALWARE TYPE (1+ infection)



MALICIOUS FILES CLEANED BROKEN DOWN BY MALWARE TYPE



Once again, we see that the “old standards” of malware—backdoors, shells, and JavaScript files—are hackers’ most popular choices. The spike in backdoor attacks, such as last year’s [Drupalgeddon](#), indicate cybercriminals are showing interest in reusing existing and efficient malware, as well as the development of new malware.

Javascript files dominated files cleaned by our malware scanner at a rate of nearly two times the next closest category, malicious redirects. Javascript attacks are different than a backdoor file or a shell file because the intent is to hijack the visitors or the website, not to have control over the website itself.

Because the presence of malicious Javascript files are often symptomless to the website owner, they are becoming a new favorite weapon of cybercriminals. Defacements continued to drop in popularity, found on only 15% of infected sites and accounting for only 5% of malicious files cleaned in 2018.

One reason for the decrease in defacements can be attributed to cybercriminals leveraging quieter,

symptomless attacks. SEO spam, a former favorite attack kit, accounted for only 2% of malware cleaned this year and was found on only 18% of infected websites—likely due to its “noisy” attack nature.

Attackers are likely moving away from this method because of the attention the attacks draw. The preferred method of malware allows attackers to subtly view, modify, or steal content and data from its victims’ websites. Categories including backdoor, shell and filehacker (file modification) were found on more than 50% of all infected websites and accounted for more than 10% of files cleaned.

This is a departure from previous attacker behavior examined in late 2017 and early 2018, which showed hackers attempting to compromise website visitors through stealthy visitor-based attacks. Attackers have re-embraced strategies to gain control of websites by attacking the website directly, rather than the site’s visitors. However, as internet users become more educated on how to browse the web safely, visitor-based attacks will likely continue to decrease.

What's Next for Website Security?

Studying malware and making predictions about cybercriminals can be difficult as attackers are always evolving to become more effective. For 2019, SiteLock predicts that website attacks will revolve around a few key themes.

Downfall of cryptocriminals:

Crypto-related malware will continue to decrease as it is no longer a profitable attack. With the crash of Bitcoin, the closing of cryptomining service Coinhive, and reduction of value on other currencies, bad actors have less motivation to leverage this strategy.









Decrease in noisy attacks:

SEO spam, .htaccess attacks, redirects, and other “noisy” attacks will decrease. The more files an attack kit requires, the more likely it is that either a malware scanner or website developer will spot it and remove it. Bad actors will have no choice but to adapt to rising user awareness.

Shrinking attack footprints:

As cybercriminals use more stealthy attacks, search engines will continue to err on the side of caution when blacklisting websites for fear of false-positives. Attackers will act on this opportunity, becoming sneakier and making malware more difficult for search engine scanners to detect. More than ever, it's crucial to rely on a defined website security strategy—rather than a search engine—to call out potential infections on your site.

With this in mind, how can small business owners, bloggers, and website developers use the information in this report? They can get ahead of the game by staying abreast of trends, attack patterns and creating an effective security strategy. Here is your 2019 checklist:

-  Choose strong passwords and unique usernames
-  Use an inside-out malware scanner that scans daily and automatically removes malware
-  Implement a website application firewall to block malicious traffic and attacks
-  Conduct quarterly website audits and file review for unusual file names or content
-  Remove outdated and unused plugins
-  Use a tool that automatically patches vulnerabilities in applications, plugins and themes
-  Select open-source applications based on security factors, such as date of the last update
-  Offer ongoing company-wide cybersecurity training

The website security landscape can be intimidating thanks to its ever-changing attack methods and increasingly sophisticated bad actors. However, with proper cyber hygiene and a proactive website security plan, you can ensure your cybersecurity strategy is effective and your website remains secure in 2019.

Appendix

KEY STATISTICS

Total sample size: 6,056,969

Average number of attacks per day: 62
59% increase from January 2018 – December 2018

Approximately 1% (0.78%) of websites are infected with malware at any given moment

Approximately 17.6 million websites may be infected with malware at any given time

17.6 million websites worldwide are infected with malware at any given time

Website receive 2,354 bot visits per site per week on average

Only 15% of websites infected with malware were blacklisted by search engines

Risk by CMS

Drupal sites were 1.6 times more likely to be infected with malware than the average site

Joomla! sites were 2.2 times more likely to be infected with malware than the average site

WordPress sites were 1.6 times

likely to be infected with malware than the average site

Sites with a vulnerability are 3.3 times more likely to be infected with malware than those that have no external-facing vulnerabilities

Cross-Site Scripting (XSS)

1.44% of sites have an XSS vulnerability

3% of sites with XSS vulnerabilities have malware

Total pages with XSS vulnerabilities: 1,681,900

SQL Injection (SQLi)

6% of sites have an SQLi vulnerability

2% of sites with an SQLi vulnerability have malware

Total pages with SQLi vulnerabilities: 349,161

Cross-Site Request Forgery (CSRF)

1% of sites have a CSRF vulnerability

3% of websites with a CSRF vulnerability have malware

Threats by popular CMS

20% of WordPress sites had a vulnerability (XSS, SQLi, or CSRF)

15% of Joomla! sites had a vulnerability (XSS, SQLi, or CSRF)

2% of Drupal sites have a vulnerability (XSS, SQLi, CSRF)

.05% of non-CMS sites had a vulnerability (XSS, SQLi, CSRF)

Malware

By Sites Impacted

47% of infected sites had at least 1 *filehacker*
50% of infected sites had at least 1 *backdoor*
46% of infected sites had at least 1 *malicious eval request*
34% of infected sites had at least 1 *injector file*
48% of infected sites had at least 1 *shell script*
18% of infected sites had at least 1 *SEO spam file*
15% of infected sites had at least 1 *defacement file*
9% of infected sites had at least 1 *phishing file*
2% of infected sites had a *cryptominer*

By Total Files Cleaned

33% of malicious files cleaned were *JavaScript files*
19% of malicious files cleaned were malicious *redirects*
2% of files cleaned were *shell scripts*
11% of malicious files cleaned were *backdoors*
7% of files cleaned were *phishing files*
5% of files cleaned were *defacements*
2% of files cleaned were *SEO spam*
5% of files cleaned were *cryptominers*