

THE SECRET LIFE OF WEBSITES

SITELOCK WEBSITE SECURITY INSIDER [Q1 2018]



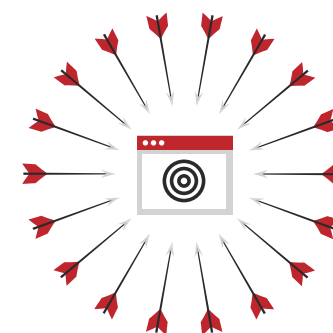
TABLE OF CONTENTS	PAGE NUMBER
Introduction and Key Takeaways	1
Malware and Blacklisting	3
Website Owners Misjudge Malware Threats	4
Prevalent Malware Types are Hard to Detect	4
Search Engines are Increasingly Poor at Blacklisting Infected Sites	6
Tips and Advice	7
Vulnerabilities, CMS, and Application Patching	8
Keeping Up With Vulnerabilities in Popular Platforms	9
Popular Platforms Propagate Vulnerabilities	10
Tips and Advice	12
Social Media, Web Application Firewall, and Risk Assessment	13
What Features Increase Risk of Website Compromise	14
Social Media Connectivity Increases Attack Surface	15
The Majority of Attacks are Automated	16
Tips and Advice	16
Conclusion	17
Appendix	18
Key Stats	18
Full Stats	19
Survey Questions	21
Glossary of Terms	23
Sources Cited	24
Further Reading	24

NO WEBSITE IS TOO SMALL TO HACK

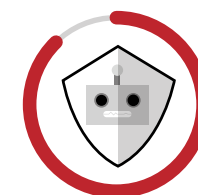
From Facebook to Panera Bread and MyFitnessPal, cyberattacks and data breaches continue to make headlines in 2018. However, it's not just large enterprises and high-profile brands in the cyberattack spotlight anymore. Small businesses and website owners are increasingly under attack by cybercriminals because their websites are left unprotected.

In Q1 2018, SiteLock studied more than 10 million websites and surveyed 250 website owners and found that small businesses continue to be the target of choice for cybercriminals. Cybersecurity expert Jessica Ortega analyzed this data for the most up-to-date insights on website attacks.

The SiteLock Website Security Insider Q1 2018 examines the trends, vulnerabilities, and risk factors that cause small business websites, like yours, to be the target of cyberattacks. Additionally, this report provides effective solutions for mitigating your risks and stopping attackers before your business becomes the subject of a news headline.



The average website is attacked
50 ATTACKS PER DAY.



88%
of traffic filtered
by firewalls was
bad bots.



Only
17%
of infected sites
were blacklisted
by search engines.



49%
of infected sites had at
least one Filehacker
designed to modify files
and upload malware.



In Q1, 1% of sampled sites were
infected with malware, on average.
**AT ANY GIVEN MOMENT ABOUT 18.7
MILLION SITES ARE INFECTED.**

RISK MODEL RANKINGS

1x
AVG/LOW

15x
HIGH

High risk websites were **15 times** more likely to be infected than the average site.

48% OF INFECTED WORDPRESS WEBSITES WERE RUNNING THE LATEST CORE UPDATES

for WordPress at the time of compromise, 3% more than in Q4 2017.



2x

WordPress sites were **two times more** likely to be infected than non-CMS sites.



1x

SURVEY RESULTS



60%

reported website incidents in the last year were malware infections.



24%

of website owners surveyed experienced damage to their business's reputation as a result of a website security incident.



36%

of website owners surveyed experienced damage to their business's bottom line as a result of a website security incident.

With the stakes so high for website owners, there is a clear need for a comprehensive understanding of the threats websites face. Using automated attacks, cybercriminals no longer need to target high-profile websites for the greatest return. In fact, it is more profitable to cast a wide attack net and compromise average websites in large numbers.

No website is too small to hack.

THE SOUND OF SILENCE

MALWARE AND BLACKLISTING

WE INTERRUPT YOUR REGULARLY SCHEDULED PROGRAMMING TO BRING YOU BREAKING NEWS ABOUT CYBERCRIME.

A website belonging to a popular music venue ticket seller has been the victim of a cyberattack. The popular website, used for purchasing concert and festival tickets, has been defaced by cybercriminals. Additionally, we are receiving reports that customer, venue, and promoter data may have been breached and made available on the dark web. At the time of reporting, the website is still down while the company repairs the damage done—costing both promoters and venues lost ticket sales as concert goers are unable to purchase tickets in advance.

This type of story has dominated mainstream headlines and is becoming increasingly common in the media. However, the news typically focuses on enterprise breaches and big names, leaving small businesses with the continued belief that they're "too small to be hacked."

In Q1 2018, SiteLock analyzed over 10 million websites to identify the threats posed to small business websites. Findings reveal that small businesses are progressively becoming the favored target of cybercriminals. Even more alarming, these small businesses don't know they are being targeted or compromised.



On par with last quarter, an average of 1% of sampled sites were infected with malware.
AT ANY GIVEN MOMENT ABOUT 18.7 MILLION SITES ARE INFECTED.



248

files were cleaned per infected site, on average.

▼ 24% COMPARED TO Q4 2017



31%

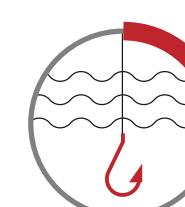
of files cleaned from infected sites were backdoor files.

▲ 18% COMPARED TO Q4 2017



12%

of infected sites had at least one malicious mailer script.



24%

of files cleaned from infected sites were visitor attack malware.

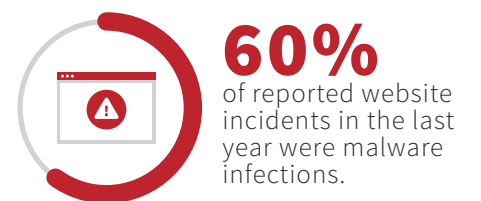
WE NEVER SAW IT COMING

If you've never seen a website defacement on your website or a message stating "Hacked by cybercriminals," it's safe to assume your website is safe, right? Nothing could be further from the truth.

In Q1 2018, SiteLock surveyed over 250 website owners to assess their knowledge and what they fear most about website security. The results were startling—while 78% of respondents reported being knowledgeable in website security, 14% of respondents reported that they had never updated their website application or did not know how. Additionally, a startling 4% of website owners surveyed were unsure if their website had ever been compromised. Of those that did report a cyberattack on their website, 36% reported that the incident caused lost revenue and harmed their bottom line.

A staggering 42% of respondents also reported that their biggest website security fear was a defacement, indicating a lack of awareness that the quieter and stealthier malware attacks are just as, if not more, damaging.

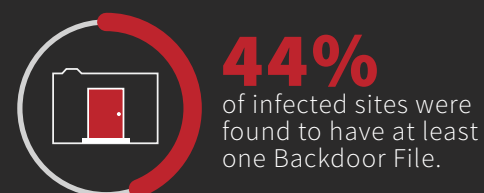
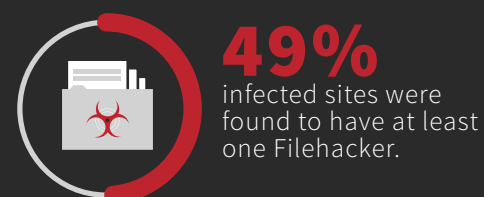
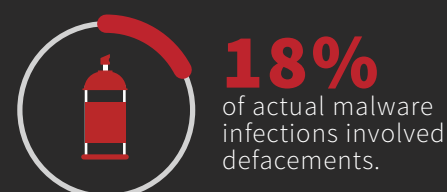
PERCEPTIONS



Filehacker:
Malicious files designed to modify or create additional malicious files.

Backdoor:
Malicious files designed to allow attackers continued undetected access to website files or databases.

REALITY



THE UNDETECTED THREAT

In Q1 2018, defacements were found on less than 1 in 5 infected websites (18%). However, 49% of infected websites were found to have at least one Filehacker and 44% were found to have at least one backdoor file, indicating that stealthier attacks may be going undetected.

In addition to Filehackers and backdoor files, 60% of infected websites had at least one shell script. Shell scripts are administrative files used to access the backend of a website to modify, add, or delete content. These files are rich in functionality, often granting file and database access in addition to uploading or downloading files. The prevalence of files used for further propagating malware indicates that cybercriminals are continuously aiming to create and maintain access to infected websites.

Once an attacker has a foothold on an infected website via a backdoor, Filehacker, or shell script, they can use that presence to upload additional malicious files. In Q1 2018, SiteLock scanners cleaned over 3.1 million infected or malicious files with the average infected site having 248 malicious files. While this is a 24% decrease from Q4 2017, it is still a considerable number of unauthorized files, especially considering that it only takes one malicious file to wreak havoc on a website. A single malicious file could result in the website being taken down or blacklisted by search engines. During our research, we also looked at why attackers are infecting websites.

Research showed that a large number of cyberattacks are attempting to attack website visitors rather than website owners. We examined several different types of visitor attacks to determine what information attackers are looking for, including SEO spam and phishing.

Phishing kits, or groups of files disguised as popular shopping and banking apps used to steal login and/or credit card credentials, made up 11% of all files cleaned in Q1 2018. This was a sharp increase, nearly 10% higher than the previous quarter. Additionally, the prevalence of SEO spam increased by 5% from Q4 2017, representing 7% of all malicious files cleaned during Q1 2018.

Each of these types of malware are designed to change what visitors see when viewing the infected site, either by redirecting them to another malicious site or executing a malicious download to their local system. These types of files accounted for 24% of malicious files this quarter.

In Q1 2018, a new headline-making threat emerged in the form of cryptocurrency mining malware, or cryptojacking. Cryptojacking malware is compromised of malicious scripts that harness the power of a website visitor's local computer to mine for cryptocurrencies, such as Bitcoin or Monero. Approximately 1% of infected sites were found to have at least one cryptojacking file. However, only 35% of surveyed small business owners were aware of the threat this type of malware could pose.



7%

OF FILES CLEANED WERE SPAM FILES

SEO spam is the practice of stuffing keywords and backlinks onto a website in order to manipulate search engine rankings for malicious or unrelated websites.



11%

OF FILES CLEANED WERE PHISHING FILES

Phishing kits are groups of files disguised as popular shopping and banking apps used to steal login and/or credit card credentials.

UNDETECTED AND UNREPORTED

Each quarter SiteLock analyzes the number of malware-infected websites that have been blacklisted by search engines. To protect website visitors and search engine users, search engines will blacklist sites that are found to be infected with malware. Many website owners rely on search engines to look for malware on their sites and believe if their website is compromised, a search engine will notify them of the infection. However, this assumption has historically been incorrect. While the number of infected sites in Q1 2018 has remained steady at 1%, the number of websites blacklisted by search engines has continued to decline. In Q1 2018, only 17% of infected websites sampled were found on search engine blacklists. This is a 2% decrease from the previous quarter for the third quarter in a row.

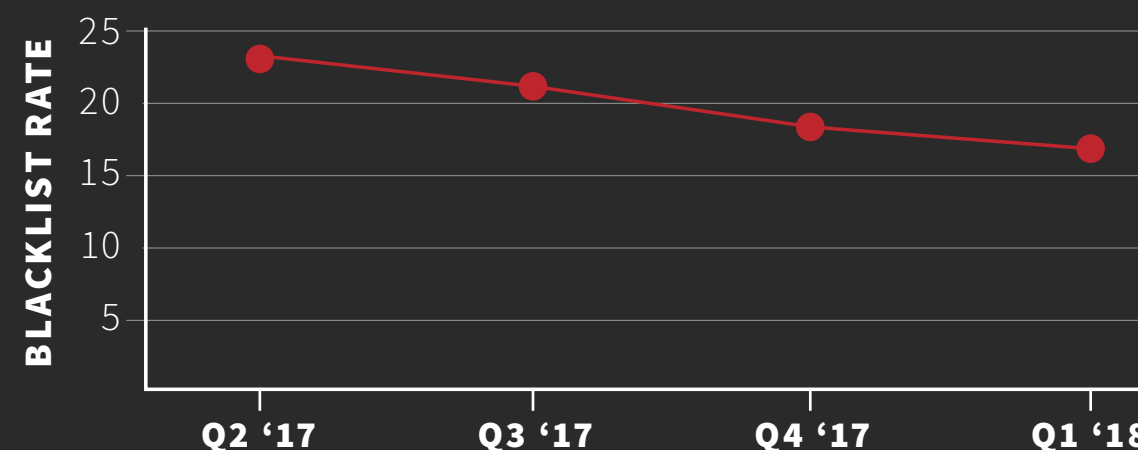
This continued decrease indicates that as search engines continue to grow in influence, they will also continue to err on the side of caution. The consequences of ending up on a search engine blacklist can be particularly detrimental to small businesses, including removal from search listings and a damaged brand reputation.

“MANY WEBSITE OWNERS RELY ON SEARCH ENGINES TO LOOK FOR MALWARE ON THEIR SITES AND BELIEVE IF THEIR WEBSITE IS COMPROMISED, A SEARCH ENGINE WILL NOTIFY THEM OF THE INFECTION. HOWEVER, THIS ASSUMPTION HAS HISTORICALLY BEEN INCORRECT.”



17%

of infected sites
were blacklisted
by search engines



REMAINING VIGILANT

Prominent headlines about cybercrime aren't going away anytime soon, but your website doesn't have to be just another line on a news ticker. Our expert, Jessica Ortega, provides some simple steps you can take to protect your website, data, and visitors.

Always Be Prepared: "It's alarming how many small businesses don't have a basic response plan in the event of a cyberattack. Cybersecurity experts often advise businesses to assume they will be hacked at some point. Having a plan for how to handle that can mean the difference between life and death for a small business," says Jessica.

Almost half (46%) of website owners surveyed reported that their website was the victim of a security incident in 2017. These responses serve as a reminder that a website security attack can happen at any time to anyone. To protect your website from malware, it is best to use a combination of proactive and reactive measures that include a malware scanner that automatically removes malware upon detection. It is also recommended that small businesses identify a point of contact in the event of an incident to help communicate the incident and its consequences to internal teams and customers. Having a plan and making

changes to that plan as new threats and trends emerge keeps you ahead of the curve when it comes to cyberthreats.

Be in the Know: Jessica says, "It's true that once upon a time, cybersecurity news was left to hacker forums and tech blogs, but as bigger names are compromised, the news becomes increasingly mainstream. I always tell small business owners to follow that news carefully. Knowledge is power, especially when it comes to technology."

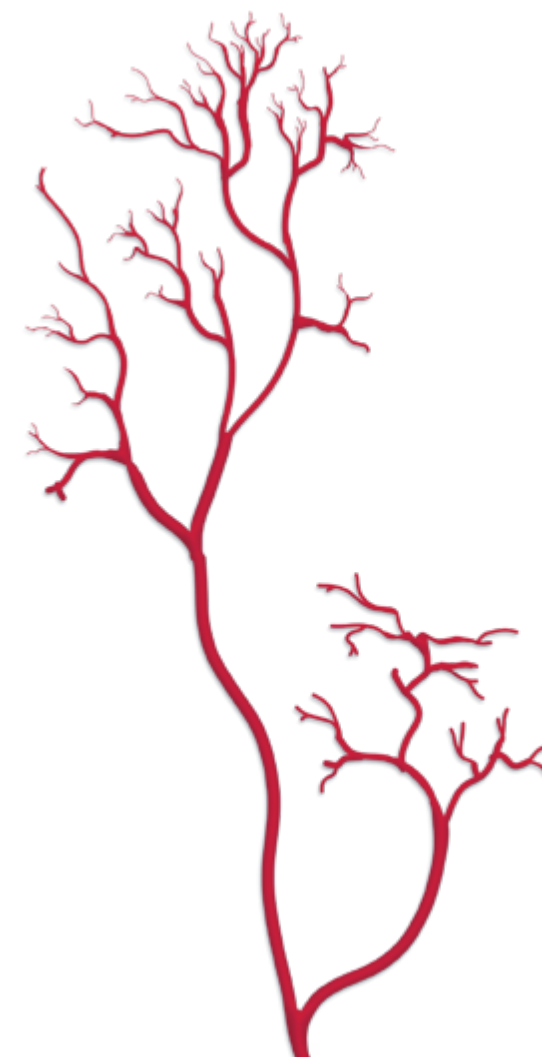
The news about data breaches and defaced websites can be a cautionary and intimidating tale, to say the least. However, staying abreast of cybersecurity news can also be a powerful tool against cyberthreats. SiteLock recommends following trusted cybersecurity news sources for current events and trends that could impact your website. This will help you develop a plan to protect your website and respond in the event of a security incident.

Malware and blacklists are not the only threats making headlines around the world for businesses, though. To stay out of the news and avoid becoming another statistic, it is also important to learn about the vulnerabilities in your website and the factors that increase the likelihood that your site could become a target.



60%

of reported security incidents in 2017 were malware infections.



WITH ACCESSIBILITY COMES GREAT RESPONSIBILITY

VULNERABILITIES, CMS, AND APPLICATION PATCHING

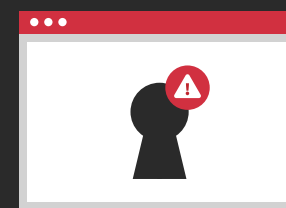
CONTINUING COVERAGE OF LAST WEEK'S BREAKING NEWS:

The cause of a large credit bureau compromise, which resulted in millions of consumer records being leaked, has now been disclosed. A spokesperson for the bureau reported that an unpatched vulnerability in the company's content management system was exploited by attackers in a successful attempt to steal customer data. A patch for the application was released three months prior, but engineers had not yet updated their applications to address the vulnerability, leaving it exposed to attack.

We have all heard this story: A corporation fails to patch a vulnerability that results in a large-scale attack or data breach. However, what you may not be hearing is that content management systems (CMS), commonly used to run small business websites, are being left unpatched, opening them to becoming stories like this one.

Unpatched applications are leaving these websites open to attacks daily. When surveyed, 59% of small business owners

reported that they were responsible for the upkeep of their website, but only 42% of website owners updated their applications monthly or more frequently. An alarming 9% of respondents admitted they were unsure how to update these applications. Considering websites experience an average of 50 cyberattacks per day, many of them targeting unpatched vulnerabilities, a lot of websites are at a higher than average risk of attack or malicious activity.



Approximately 6% of websites—up to **113 MILLION WEBSITES** globally—have a security vulnerability.

CMS USED BY SAMPLE SITES



 **No CMS - 68%**

 **WordPress - 31%**

 **Joomla! - 1%**

 **Drupal - 0.13%**

PATCHING THE FLAWS

Over 29 million websites worldwide use one of the three biggest CMS platforms: WordPress, Joomla!, and Drupal. These platforms make building a small business website more accessible than ever before by being free, easy to use, and open source with large communities. However, with accessibility comes great responsibility. Open source applications and self-built websites require periodic core, theme, and plugin updates. However, not all website owners are aware that their CMS-run website is a living entity that requires regular updates to remain secure. Research from Q1 2018 found






that only 68% of WordPress sites were running the latest core version updates, meaning nearly one third, or up to 6.3 million WordPress sites globally, were potentially vulnerable to attack.

As an example, in Q1 2018, popular CMS applications released security updates that addressed a total of 95 vulnerabilities. These vulnerabilities required over 1,900 patches, more than 6 times the number of patches written in Q4 2017. WooCommerce alone patched 38 vulnerabilities in Q1 2018. Among the vulnerabilities patched were cross-site scripting (XSS), SQL injection (SQLi), and cross-site request forgery (XSRF).

Due to the nature of most database-driven website applications like WordPress and Joomla!, it takes a smaller number of static files for an application to function, making sites easier to build and maintain. However, this means that a single vulnerability in an application could make every single page on a website vulnerable to attack. Additionally, when a vulnerability is disclosed in a major CMS, attackers use automated scanning tools to find not only vulnerable pages on an individual website, but also any website running the vulnerable version. This opens doors to countless attack possibilities for cybercriminals.

While only 1% of the sampled population had an XSS vulnerability, they accounted for over 1.6 million vulnerable website pages—about 424 pages per vulnerable website. Sites with SQLi vulnerabilities had more than 1,000 vulnerable pages on average. This means attackers scanning sites for vulnerabilities could potentially gain unauthorized access to the sites through any page on them.

CONTENT MANAGEMENT SYSTEM (CMS) SECURITY PATCHING IN Q1 2018

CMS	VULNERABILITIES	PATCHES REQUIRED TO ADDRESS ISSUES
 WordPress	1	29
 Joomla!	6	77
 Drupal	35	637
 Magento	15	139
 WooCommerce	38	1,141



XSS
CROSS-SITE SCRIPTING

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.

SITES THAT HAD AN XSS VULNERABILITY HAD AN AVERAGE OF 424 VULNERABLE PAGES

A 2% increase from Q4 2017



SQLi
SQL INJECTION

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 the entire website in order to steal information or deface the site.

SITES THAT HAD AN SQLI VULNERABILITY HAD AN AVERAGE OF 1023 VULNERABLE PAGES

A 6% increase from Q4 2017



XSRF
CROSS-SITE REQUEST FORGERY

CSRF vulnerabilities allow attackers to force users to execute unauthorized actions, like transferring funds on a banking website, without their knowledge.

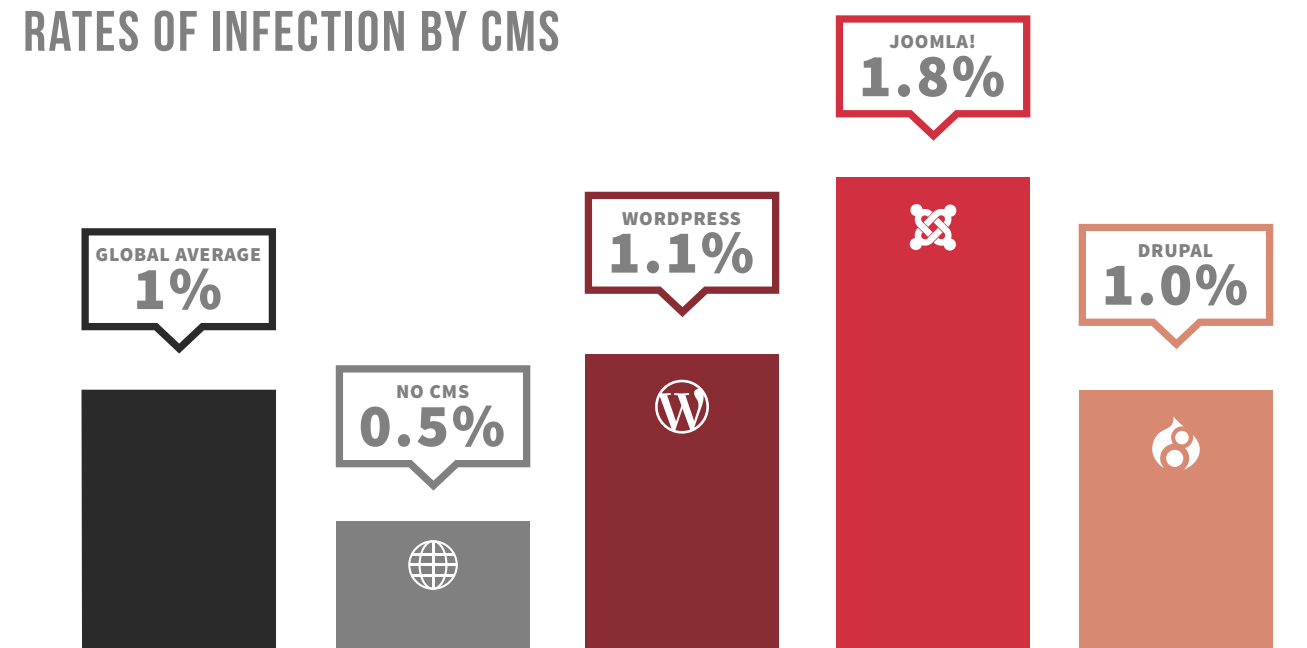
CONTENT MANAGEMENT AND COMPROMISES

While website vulnerabilities do not exclusively impact open source CMS applications, the continued rise in popularity of these applications means their security flaws are more publicized than ever before. SiteLock examined 1.9 million websites using content management systems to determine how likely they were to be compromised, as well as the factors that put them at increased risk.

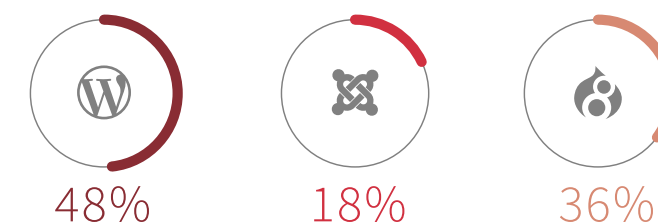
On average, it was found that CMS websites are approximately twice as likely to be compromised as sites that do not use a content management system. While out-of-date applications are a likely reason for the increased risk, it was not the only risk factor. In fact, among WordPress sites, nearly half (48%) of infected sites

were running the latest core security updates at the time of compromise. Among Joomla! sites that had malicious content, 18% were running the latest core updates. Interestingly, the number of up-to-date Drupal sites doubled from 18% in Q4 2017 to 36% in Q1 2018. This is most likely due to Drupal releasing multiple updates and public service announcements for the critical Drupalgeddon2 vulnerability. “Engaging with the open source community and following the developer’s blog for your CMS is an easy way to stay ahead of potential security vulnerabilities and plan for patching,” says expert Jessica Ortega. This kind of engagement likely increased among Drupal users during Q1, increasing the number of Drupal sites running the latest core security updates.

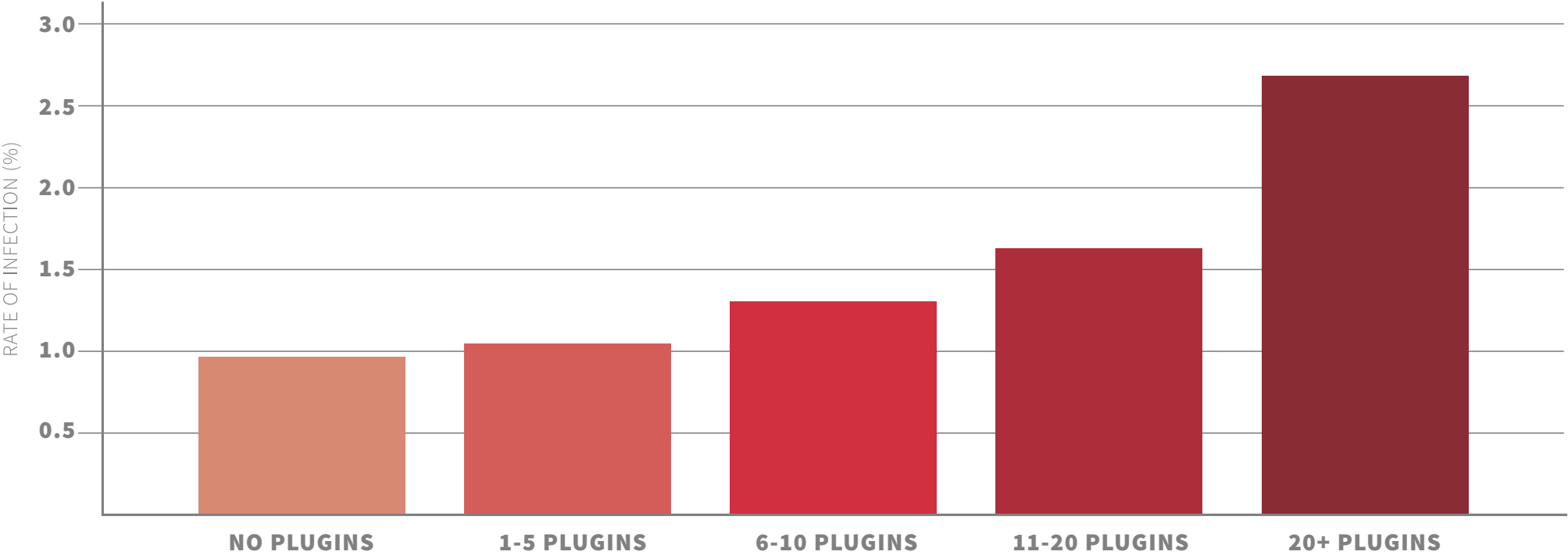
RATES OF INFECTION BY CMS



HOW MANY OF THE COMPROMISED SITES WERE RUNNING THE LATEST CORE VERSIONS OF THEIR CMS AT THE TIME OF COMPROMISE?



WORDPRESS INFECTION RATES VS PLUGINS



Research also shows that using plugins to customize CMS sites increases a site's likelihood of compromise. Plugins are add-ons used by CMS website applications to increase functionality or add features to a website. However, the more plugins added to WordPress sites, the more likely the sites were to be infected with malicious content. Sites with no plugins or five or fewer plugins shared a similar low risk level. Sites with 6-10 plugins were 1.3 times more

likely to be infected and sites with 11-20 plugins were 1.7 times more likely to be infected with malware. However, when sites had more than 20 plugins installed, their risk dramatically increased. Sites with 20 or more plugins were 2.8 times more likely to have malware.

The most likely reason for this is that plugins increase the website's attack surface by creating more

entryways for attack. Attack surface refers to the number of possible ways that an attacker could gain access to your website's data. When selecting plugins for your website, it is important to ensure you're only downloading necessary plugins from reputable sources. Installing pirated or unnecessary plugins could result in an increased risk of website compromise.

MITIGATING THE RISKS

“Open source applications are an amazing tool for businesses of any size, including large enterprise corporations. They’re also useful for novice website builders and small business owners who need to build a presence online, but if left unattended they lead to a higher risk of compromise,” says Jessica. That said, there are steps you can take to mitigate your website’s chance of being infected with malware.

Check for Leaks: Use a vulnerability scanner that reviews your CMS files daily for security vulnerabilities. These scanners are particularly beneficial when they are capable of patching vulnerabilities and applying CMS security updates automatically. This allows you to plan for full version upgrades and ensure compatibility with your website’s features at your convenience, while maintaining a secure website.

“OPEN SOURCE APPLICATIONS ARE AN AMAZING TOOL FOR BUSINESSES OF ANY SIZE...BUT IF LEFT UNATTENDED THEY LEAD TO A HIGHER RISK OF COMPROMISE.”

Clean House: If your site uses a CMS with plugins and themes to enhance its functionality, take some time each month to review your application for updates. On most content management systems, updating core files, themes, and plugins is as easy as one click in the administrative panel. While you’re checking for updates, you should also review your plugins to ensure they are still necessary to your site. Deactivate and delete any unneeded plugins and themes. Leaving plugins deactivated without removing them means they won’t receive updates anymore and will likely become vulnerable to attack over time.

Join the Party: The open source community is rich with information and nearly all of the major CMS applications have online forums for users. These communities also have conferences, such as WordCamp, where developers, users, and small business owners come together to learn about website applications. Joining these communities and participating in the forums is an easy way to stay ahead of security updates, troubleshoot errors on applications, and find reputable plugin sources.

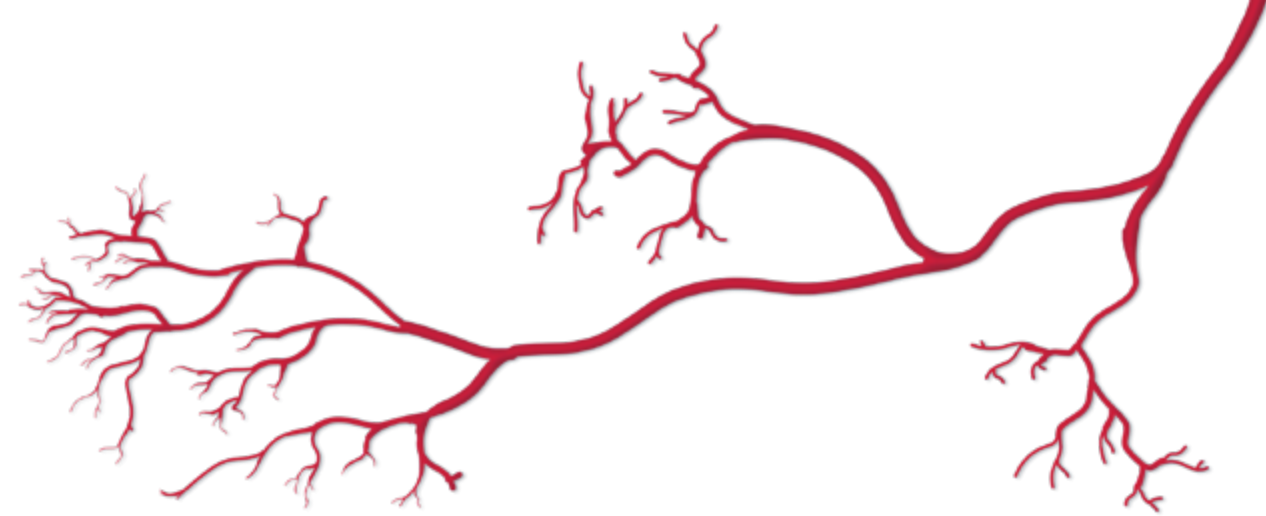
By making your website maintenance a part of your daily and monthly routines, it will be easy to stay informed and keep your website secure. In addition to securing your website’s applications, it is also important to look at other factors that put your site at risk, such as composition and social media.

MANAGING THE RISKS

SOCIAL MEDIA, WEB APPLICATION
FIREWALL, AND RISK ASSESSMENT

A POPULAR SOCIAL MEDIA PLATFORM HAS BEEN USED TO SPREAD MALWARE VIA POSTS ON THEIR SITE.

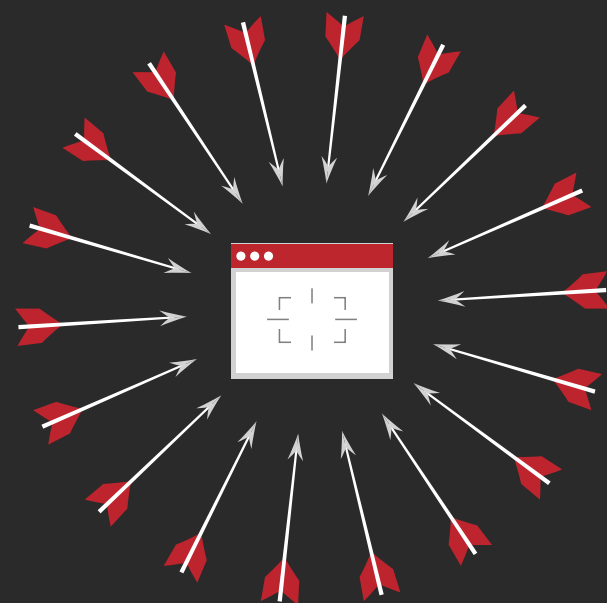
The malware in question was used by cybercriminals to install cryptojacking extensions on victims' browsers and steal their website login credentials. These credentials were used to take over business websites to spread more malicious content. Could basic traffic monitoring and social media safety have saved these businesses time and money?



Social media connections, feature-rich website experiences, and search engine visibility have become a critical part of the SMB business plan. These strategies are table stakes to both new and established businesses, with the understanding that they're necessary to succeed. All too often, though, businesses fail to realize how these factors increase their likelihood of experiencing a cyberattack. An important part of developing any website should be assessing the factors that might make it a target

for cyberattacks. By examining more than 10 million websites in Q1 2018, SiteLock was able to look at the ways social media and site composition impact risk. Additionally, by examining traffic to over 60,000 sites through a web application firewall, we identified trends in attack activity.

By taking a holistic look at the factors that make your website a potential target, you can take steps to prevent successful attacks. Jessica Ortega also provides practical safety tips to keep your business ahead of the curve.



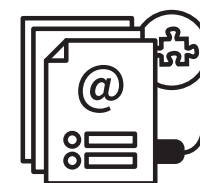
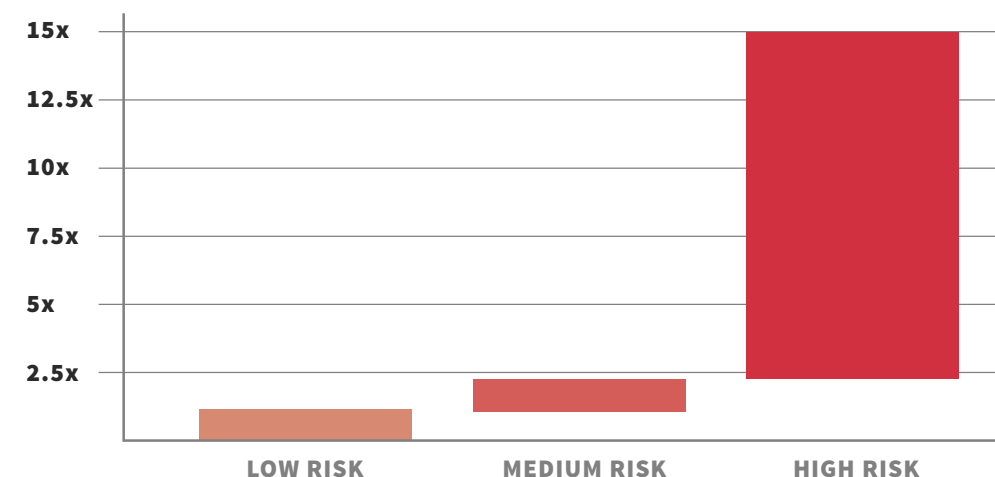
WEBSITES
EXPERIENCE
AN AVERAGE OF
**50 ATTACKS
PER DAY.**

A TARGET ON YOUR BACK

SiteLock examined more than 10 million websites using 500 variables broken into categories, including site composition, popularity, and complexity, to predict the sites' likelihood of experiencing a cyberattack. This is used to create a risk assessment that can help gauge what factors may put a small business site at increased risk. After reviewing these factors, sites are broken into three categories based on their risk of attack —low, medium, and high risk.

Understanding the factors that put your website at risk can help you prepare for cyberattacks, an important part of any security plan. During Q1, SiteLock found that sites considered to have a medium risk were twice as likely to be compromised as the average, or low risk, website. However, complexity, popularity, and composition increase risk exponentially. Sites found to be at high risk were 15 times more likely to be infected with malicious content than the average website.

RISK OF WEBSITE COMPROMISE



SITE COMPLEXITY

Site complexity refers to the number of features and add-ons on your website. This could include themes, social media connections, contact forms, pages, or plugins.



SITE COMPOSITION

When examining site composition, SiteLock looks at the code and CMS applications used in building the website.



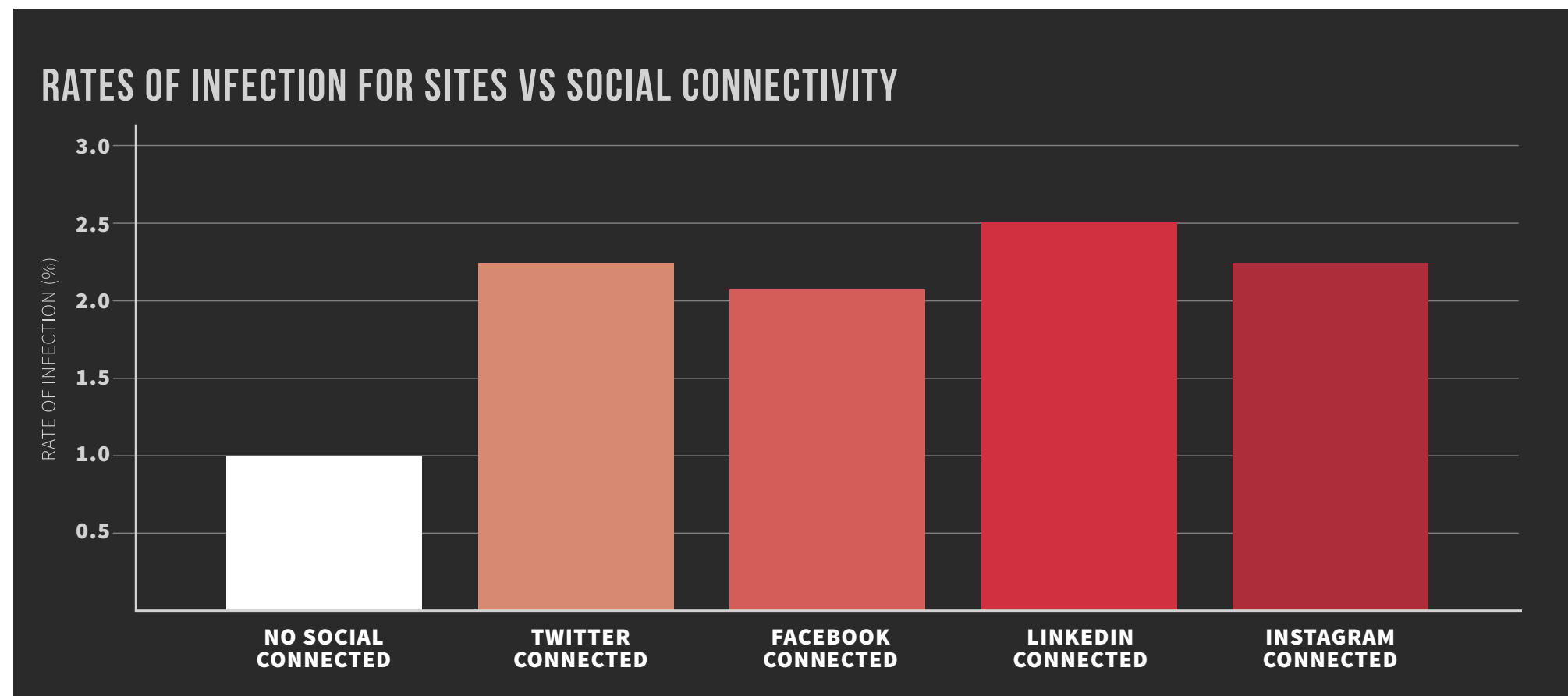
SITE POPULARITY

Website popularity is examined using a number of factors that include traffic calculations, search engine rankings, and social media following.

STAYING CONNECTED, BECOMING INFECTED

Social media continues to be an increasingly important tool for small businesses to connect to their customers. Many websites connect to social media for marketing purposes, troubleshooting, and customer testimonials. Real time social media interaction can also keep customers updated on new products or product issues. However, connecting to social media presents new avenues for potential compromises.

As social media becomes the communication channel of choice for more consumers, traditional attack tools are being adapted for use in an increasingly connected world. For instance, phishing has moved beyond the realm of email and website attacks into social media messenger systems. Attackers may scan social media websites looking for pages that list business information such as website

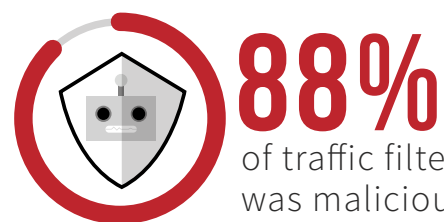


addresses, email addresses, or phone numbers. This information can then be used by cybercriminals to target businesses through their websites. Additionally, sharing posts from malicious sources can cause malware to spread to website visitors or initiate credential-stealing attacks.

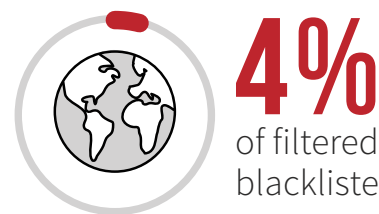
In Q1 2018, sites connected to social media were more likely to be infected with malware likely due to their increased attack surface and visibility. Sites connecting to LinkedIn had the greatest risk, being 2.5 times more likely to be infected with malware. Though the odds were close, sites connected to Facebook had the lowest infection

rate—2 times more likely to be infected than sites without a presence on social media.

While social media has its risks, there are easy steps that can be taken to mitigate your risk, such as avoiding sharing content from unfamiliar sources and not reusing passwords.



of traffic filtered by firewalls was malicious bots.



of filtered traffic was from blacklisted countries.

Bots: Also known as spiders or crawlers, bots are automated programs that browse websites. Some bots are harmless and even useful, such as bots used by search engines to index website content. However, bots can also be used to steal content and scan websites for vulnerabilities.

STOPPING THE BOTS

SiteLock examined over 60,000 sites protected by a web application firewall (WAF) to analyze trends amongst would-be attackers. The results were startling—on a weekly basis, more than 141 million visits to these websites were from malicious or suspicious bots. In fact, bad bots accounted for 88% of traffic stopped by the firewall. Additionally, we found that the firewall blocked over 773,000 threats on a weekly basis, including attempted SQLi and XSS attacks. These threats mean that websites experienced an average of 50 attacks per day in Q1 2018.

Web application firewalls also filter traffic from known malicious IP addresses and URLs. Visitors from these sources accounted for 1% of traffic filtered by the WAF and have been found to be the source of many cyberattacks. Across our sample, this means 3.5 million blocked visitors during Q1 were from known malicious IP addresses or URLs. Website owners can also customize their WAF to blacklist visitors from any country, including those where most cyberattacks originate. In Q1 2018, visitors from countries blacklisted by WAF rules accounted for 4% of traffic to sampled sites, or approximately 14 million blocked visitors.

A CYBER-SUIT OF ARMOR

“There’s no such thing as a no-risk website. Social media schemes, bot traffic, and a high-risk assessment can be very intimidating, but you don’t have to run for the hills. There are easy ways to suit up and protect your site,” says Jessica. While only 22% of small business owners surveyed said they intend to increase their website security budget in 2018, not all security steps have to be expensive or complicated.

Know Your Risk: Knowledge is half the battle. Understanding how your website features increase your risk makes it easier to decide whether or not they are truly necessary. Website owners should strive to build their sites with only the necessary features and plugins for engagement and functionality purposes. Remove any add-ons or plugins that are not necessary to reduce the likelihood of compromise.

Be Greedy with Your Information:

Social media can be fun as well as strategic for businesses. Unfortunately, cybercriminals often capitalize on the powerful role social media plays in a business’s success. It is critical to be aware of the information you’re sharing on your social media pages. Never share or participate in surveys that ask for seemingly innocuous information, such as first pet’s name or first concert. These answers are often used in password retrieval and two-factor authentication applications, and sharing this kind of data can lead to data theft and compromise. By protecting your information, you can prevent attackers from using it to gain access to your website applications.

While the statistics can be frightening, that’s no reason to be discouraged. Remaining vigilant about risk and being aware of your cyber-surroundings can help keep your website secure without drastically changing its functionality.

NO WEBSITE IS TOO SMALL TO HACK, BUT EVERY WEBSITE OWNER CAN PROTECT THEMSELVES.

Recent reports indicate that a high-profile group of cybercriminals are launching targeted attacks on small business websites. Due to the sophistication of these attacks, the majority of victimized small businesses could have taken a massive hit to their reputation and bottom line. Fortunately, more small businesses are taking a proactive approach to website security and cybercriminals have been unsuccessful in infiltrating their sites.

Cyberattacks targeting large corporations and major brand names have historically dominated headlines, but as cybercriminals continue to focus on small businesses, stories like this will become increasingly common. “Based on the numbers we’ve seen, it has become clear that no website is too small to hack,” says Jessica. “As cybercriminals become more sophisticated and continue to hone their craft, small businesses will need to keep up by taking a proactive, holistic approach to website security.”

While websites may experience an average of 50 attacks per day, taking the necessary precautions can prevent those attacks from being successful. Dodging a cyberattack might seem far-fetched for small businesses without a security budget, but it is actually very attainable.

There are easy to implement, affordable, and effective ways websites owners can mitigate their risks and prevent cyberattacks.

YOU CAN KEEP YOUR WEBSITE SECURE WITHOUT BREAKING THE BANK BY:

- Remaining vigilant. Keep an eye on cybersecurity news and trends.
- Planning ahead. Know what to do in the event of a cyberattack.
- Implementing a web application firewall (WAF) to filter out malicious and bot traffic.
- Using two-factor authentication whenever possible. Adding another layer of security to your passwords can help keep cybercriminals out.

Knowing your risk of a compromise and following the best practices highlighted in this report can help you proactively protect your website, small business, and—most importantly—your site’s visitors.

Q1 QSR APPENDIX

KEY STATS

Average number of attacks per day - 50
14% increase from Q4 2017

Percentage of sites with malware - .71%
On par with Q4 which was .7%

Only 17% of sites infected with malware were blacklisted
Down 2% from Q4

88% of traffic mitigated by the WAF was bad bots

3.6% of mitigated traffic was from blacklisted countries

DDoS attacks dropped to just .04% of mitigated traffic in Q1

The WAF blocked 348,794,591 threats in Q1

.06% of sampled sites had an XSS vulnerability

.001% of the population had a SQLi vulnerability

CMS Statistics

WordPress

WordPress infection rate - 1.11%—1.6 times more likely to be infected than the global population

48.3% of WordPress sites were running the latest core updates when they were infected with malware
3% increase from Q4

Joomla!

Joomla! infection rate - 1.09%—1.53 times more likely to be infected than the average website
Down from 2% in Q4

18.2% of Joomla! sites were up to date with the latest core version when they were infected

Drupal

Infection rate for Drupal - 1.03%—1.4 times more likely to be infected than the average website

36% of Drupal sites had the latest core version when they were infected

Non-CMS

Non-CMS infection rate - .5%—.7 times less likely to be infected than the average website

Patching

WordPress had 1 vulnerability requiring 29 patches

Joomla! had 6 vulnerabilities requiring 77 patches

Magento had 15 vulnerabilities requiring 139 patches

Drupal had 35 vulnerabilities requiring 637 patches

Malware

Malware by sites impacted—sites infected with malware were found to have at least 1 of the following types of files on them:

Filehackers - 49%

Backdoor Generic - 44%

Shell - 40%

Defacement - 18%

PHP Mailer - 12%

Phishing - 8%

Cryptominer - 1%

Malware by files cleaned:

Backdoor Generic - 31.35%

Phishing - 10.78%

Defacements - 10.67%

Filehacker - 6.56%

Mailer - 3.33%

SEO Spam - 1.51%

Customer Survey Key Stats

59% of respondents are responsible for their own website upkeep

69% of respondents consider themselves moderately knowledgeable about website security, while only 9% said very knowledgeable

41% of respondents update their website applications monthly or more often, while 3.3% have NEVER updated their website applications

9% of respondents admitted to not knowing how to update their applications

42% of respondents reported their biggest fear was a website defacement, despite the fact that less than 1 in 5 malware infections included a defacement

24% of respondents who had a security incident reported it damaging their business reputation, while 36% reported it endangered their bottom line

35% of respondents were aware of what cryptocurrency mining (cryptojacking) malware is, despite the fact that only 1% of infected websites in Q1 had cryptojacking malware

FULL STATS

QSR Q1 2018 Full Stats List

GENERAL STATS

Sample - 6,095,601 websites
From Jan 1 to April 1
Average combined infected sites each week - 43,053
Average global infection rate - .71%

SMART STATS

Average number of infected sites per week - 2,083
Average number of files cleaned - 511,533
Files cleaned per site - 248
Average infection rate in Q1 - 0.03%

WAF STATS

WAF sample size - 61,993
Average bot visits per week - 141,613,350
Per site - 2,102
Average threats blocked per week - 773,316

WAF ATTACK STATS

Average number of attacks per day - 50
Types of attacks as percentages of the total number of attacks intercepted by the WAF

in Q1 - 348,794,591
Backdoor Protect - 0.04%
Bot Access Control - 88.05%
XSS - 0.01%
Illegal Resource Access - 2.67%
Remote File Inclusion - 0.08%
SQLi - 0.43%
Suspected Bots - 4.91%
DDoS - 0.04%
Blacklisted Country Visitors - 3.64%
Blacklisted IP Visitors - 0.03%
Blacklisted URL visitors - 0.03%

MALWARE SCANNER STATS

Malware scanner sample size - 6,095,601
Average infected sites per week - 41,155
Average infection rate on malware scanner - 0.68%

VULNERABILITY STATS

Percentage of sites with an XSS vulnerability - 1.34%
XSS pages - 1,640,871
Pages per site - 423.68
Percentage of sites with an SQLi vulnerability - 4.87%
SQLi pages - 304,416
Pages per site - 1,022.92

Percentage of sites with a CSRF vulnerability - 0.19%

SOCIAL MEDIA STATS

Sites connected to Twitter - 622,074
Percentage of the population connecting to Twitter - 10.21%
Infected sites connected to Twitter - 8,382
Percentage of sites connected to Twitter that are infected - 1.35%
Sites connected to Facebook - 1,172,155
Percentage of the population connected to Facebook - 19.23%
Average number of infected sites connected to Facebook - 14,410
Percentage of sites connected to Facebook that are infected - 1.23%
Sites connected to LinkedIn - 184,299
Percentage of the population connected to LinkedIn - 3.02%
Average number of infected sites connected to LinkedIn - 2,632
Percentage of sites connected to LinkedIn that are infected - 1.43%
Sites connected to Instagram - 125,506
Percentage of the population connected to Instagram - 2.06%

Average number of infected sites connected to Instagram - 1,640
Percentage of sites connected to Infected that are infected - 1.31%
Sites without social media links - 4,814,191
Percentage of the population - 78.98%
Infected sites without social media - 27,444
Infection rate for sites without social media - 0.57%

WORDPRESS STATS

WordPress site count - 1,864,148
Percentage of the sample population - 30.58%
Infected WordPress sites - 20,668
Infection rate - 1.11%
WordPress sites running the latest core version at the time of infection - 9,985 - 48.28%
WooCommerce users - 203,993
Percentage of the sample population - 3.35%
Percentage of the WordPress users - 10.94%
WooCommerce sites with malware - 2,009
WooCommerce site infection rate - 0.99%

WORDPRESS PLUGIN STATS

Sites with 1-5 plugins - 1,288,053
Percentage of the WordPress population - 69.09%
Sites with 1-5 plugins and malware - 13,387
Infection rate in the WordPress population - 0.72%
Infection rate in the 1-5 plugin population - 1.04%
Sites with 6-10 plugins - 376,330
Percentage of the WordPress population - 20.19%
Sites with 6-10 plugins and malware - 4,904
Infection rate in the WordPress population - 0.26%
Infection rate in the 6-10 population - 1.30%
Sites with 11-20 plugins - 81,565
Percentage of the WordPress population - 4.38%
Sites with 11-20 plugins and malware - 1,322
Infection rate in the WordPress population - 0.07%
Infection rate in the 11-20 population - 1.62%

Sites with 20+ plugins - 3,785
Percentage of the WordPress population - 0.20%
Sites with 20+ plugins and malware - 101
Infection rate in the WordPress population - 0.01%
Infection rate in the 20+ population - 2.67%
Sites with no plugins - 253,657
Percentage of the WordPress population - 253,657
Sites with no plugins and malware - 2,434
Infection rate in the WordPress population - 0.13%
Infection rate in the no plugins population - 0.96%

JOOMLA! STATS

Joomla! site count - 66,234
Percentage of the sample population - 1.09%
Joomla! sites with malware - 1,220
Joomla! infection rate - 1.84%
Percentage of Joomla! sites running the latest core version at the time of infection - 18.24%

DRUPAL STATS

Drupal site count - 21,998
Percentage of the sample population - 0.36%
Infected Drupal sites - 226
Drupal infection rate - 1.03%
Percentage of Drupal sites running the latest core version at the time of infection - 35.96%

NON-CMS SITE STATS

Non-CMS site count - 4,143,496
Percentage of the sample population - 67.98%
Non-CMS sites with malware - 20,746
Infection rate for non-CMS sites - 0.50%

BLACKLIST STATS

Average number of infected sites blacklisted per week - 7,487
Blacklist rate - 17.39%

RISK ASSESSMENT STATS

Infection rate for Low Risk sites - 0.08%
Infection rate for Medium Risk sites - 0.17%
Infection rate for High Risk sites - 2.5%
Medium Risk - 2x more likely than low
High Risk - 15x more likely than low

MALWARE STATS

Malware categories by sites impacted (These sites were found to have at least one file with these malware types):
Filehackers - 49%
Malicious Eval Requests - 45%
Backdoor Generic - 44%
Shell - 40%
PHP Injector - 31%
PHP Uploader - 28%
Defacement - 18%
PHP Mailer - 12%
Cookie Encoded Shell - 10%
File Manager - 10%
C99 Shell - 10%
Malicious .htaccess files - 9%
Phishing - 8%

Malicious Redirect - 6%
SEO Spam - 6%
Malicious Javascript - 11%
Trojan - 2%
Meta Refresh - 2%
Cryptominer - 1%

Malware Files Cleaned in Q1 by Category:

Backdoor Generic - 31.35%
Malicious Javascript - 18.62%
Phishing - 10.78%
Defacements - 10.67%
Filehacker - 6.56%
Japanese Spam - 4.61%
Mailer - 3.33%
Malicious .htaccess files - 3.30%
Malicious Eval requests - 2.56%
Shells - 2.14%
Malicious Redirects - 1.72%
SEO Spam - 1.51%
PHP Injectors -0.70%
Uploaders - 0.66%
Cookie Encoded Shell - 0.52%

PATCHING STATS

Patchman websites protected - 3,482,708

Vulnerabilities disclosed in Q1

WordPress - 1
Joomla! - 6
Magento - 15
WooCommerce - 38
Drupal - 35

Patches Written in Q1

WordPress - 29
Joomla! - 77
Magento - 139
WooCommerce - 1141
Drupal - 637

WEBSITE SECURITY CUSTOMER SURVEY RESULTS

277 respondents to 14 questions - SiteLock customers surveyed

What is your website’s purpose?

19.9% eCommerce
35.4% Informational
5.8% Personal
38.8% Other business

How many people do you employ?

39.8% Sole proprietor
41.1% 1-9 employees
11.4% 10-50 employees
1.6% 51-100 employees
2.8% 101-250 employees
3.3% 250+ employees

How will your website security investment change in 2018?

72% Plan to keep investments the same
17.1% Plan to increase their investments somewhat
5.3% Plan to increase their investments significantly

2% Plan to decrease their investments significantly
3.7% Plan to decrease their investments somewhat

In 2018 - who will be responsible for website upkeep?

58.9% - Me (website owner)
12.6% Freelance webmaster
13.8% Internal IT person
6.5% External IT firm
4.5% Website hosting provider
0.8% Family friend
1.2% Family member
0.8% Security software vendor
0.8% Don’t know

How would you rate your knowledge of website security?

22.4% Have no knowledge
8.9% Very knowledgeable
68.7% Moderately knowledgeable

How often do you update your website applications?

41.5% Monthly or more often
18.7% Every 2-3 months

6.1% Every 3-6 months
2% Every 6-9 months
4.9% Every 9-12 months
3.3% I have never updated my website
8.9% I Don't know how to update their website applications
14.6% Someone else handles website updates

What is your biggest security concern in 2018?

18.7% - Data theft
2.8% - Internal threat (Employee/user error)
11.4% - Nation State attack
3.7% - IoT Security
1.2% - GDPR compliance
41.5% - Website Defacement
10.6% - None
10.2% - Other

Did you have a website security incident in 2017?

45.9% - Yes
50% - No
4.1% - Don't know

What kind of security incident did you experience?

59.6% - Malware infection
13.9% - Website Defacement
2% - Ransomware
8.6% - Phishing scam
2% - Data Theft
7.3% - Unsure
6.6% - Other

Did the security incident cause damage to your business reputation?

23.9% - Yes
76.1% - No

Did the security incident endanger your business profits?

36.3% - Yes
63.7% - No

Are you aware of the potential impact on your business's website from cryptocurrency mining malware?

35.2% - Yes
43% - No

21.7% - Don't know what cryptojacking malware is

What is your gender?

61.9% - Male
31.6% - Female
6.1% - Prefer not to answer
0.4% - Other

Age Groups

0.4% - 18-23yrs
4.9% - 73+yrs
29.3% - 24-38yrs
32.8% - 54-72yrs
33.6% - 39-53yrs

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 and place a warning on the listing. 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 - A layer of protection placed on HTTP applications using a set of rules designed to block malicious traffic or content from reaching websites.

CITED SOURCES

<http://www.internetlivestats.com/total-number-of-websites/>
<https://websitesetup.org/popular-cms/>
<https://trends.builtwith.com/cms/WordPress>
[https://www.owasp.org/index.php/Cross-site_Scripting_\(XSS\)](https://www.owasp.org/index.php/Cross-site_Scripting_(XSS))
https://www.owasp.org/index.php/SQL_Injection
<https://central.wordcamp.org/>

FOR MORE INFORMATION FROM SITELOCK CHECK OUT THESE ARTICLES

What is a Vulnerability
<https://blog.sitelock.com/2017/04/what-is-a-website-vulnerability/>
Drupalgeddon2
<https://blog.sitelock.com/2018/04/drupal-geddon2-updates/>
<https://blog.sitelock.com/2018/04/drupal-geddon-2-exploit/>
<https://blog.sitelock.com/2018/03/drupal-8-5-1/>
A Process for Managing Updates
<https://wpdistrict.sitelock.com/blog/keeping-wordpress-updated-a-process-for-managing-updates/>

What is SMART PLUS?
<https://blog.sitelock.com/2017/12/smart-plus/>
Building a Cybersecurity Plan
<https://blog.sitelock.com/2013/08/cyber-security-plan/>
SiteLock WAF
<https://blog.sitelock.com/2016/11/web-application-firewall-waf-video/>
Bots – The Good, The Bad and The Even Worse
<https://blog.sitelock.com/2016/05/good-and-bad-internet-bots/>