# 2022 SITELOCK ANNUAL WEBSITE SECURITY REPORT

SiteLock
A SECTIGO® COMPANY

# TABLE OF CONTENTS

# EXECUTIVE SUMMARY

Website security is a constant race against ever-evolving cyberthreats, and the stakes are high. For businesses that increasingly rely on their websites to attract, communicate, and transact with their customers, the consequences of a breach can be costly and damaging. Yet, many small to medium-sized businesses (SMBs) still do not take their website security seriously enough, with almost half (48%) of businesses stating that they are too small to be targets, according to the 2021 State of Website Security and Threat Report from Sectigo, SiteLock's parent company. This overconfidence can be costly across multiple dimensions, including direct damages and tarnishing a business' reputation that can take years to rebuild.

The fact is that SMB websites are a prime target for cybercriminals due to their weaker security postures. As SiteLock has seen from our research, no website is immune from the increasing volume attacks and the wide, ever-evolving variety of threats.

**"The public internet is a very dangerous place and is increasingly getting worse. Don't commit the fallacy of the underdog -- SMB websites have enormous value to bad actors because they have customer data and can be used for phishing attacks."**

**- Jason Soroko, CTO at Sectigo**

In this report, we explore the current website security landscape and trends from 2021. We analyzed data from more than 14 million websites and 2.6 billion files scanned per month to determine the most prevalent cyberthreats organizations face today. Our findings show:

- **The volume of threats doubled in 2021 versus 2020** with SMBs across the SiteLock global scanning network facing a staggering 228 million threats per month.
- **The primary source of the increase in attack volume is malicious bots.** In fact, websites received 5.5 times more traffic from bots than human users with more than 60% of those bots being malicious.
- **Malware remains a significant problem for SMBs.** 18% of websites are infected with critical severity threats, such as backdoors and malicious file modification, and websites infected by high severity threats, which target visitors, nearly doubled in 2021 to a 26% infection rate.
- Websites based on popular CMS platforms like **WordPress and Drupal are being exploited at an alarming rate.**
- **Search engines often miss malware infections** with 92% of all malware-infected websites not flagged or blacklisted. This leaves website owners and their visitors vulnerable to attack.

To protect themselves and their visitors from the growing volume and broader types of threats, in 2022 and beyond, SMBs need to take a holistic approach to website security that includes implementing multiple layers of automated protection. These layers should include always-on protections against malware, DDoS, blacklisting, and spam, as well as automated vulnerability patching and website backups.

## PERCEPTION

**48%**
Of SMBs believe they are too small to be attacked

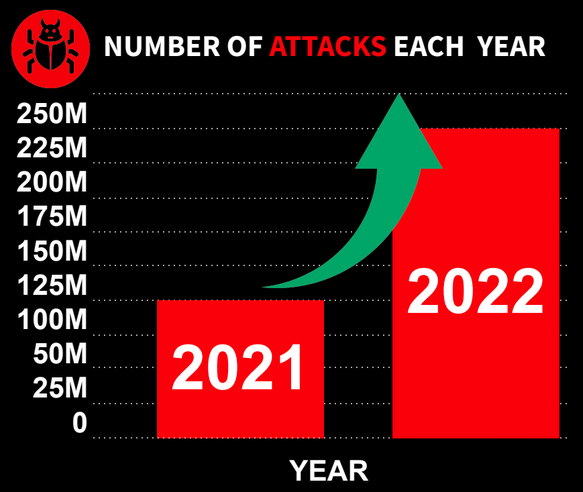
Only
**31%**
Of SMBs say they are vulnerable

## REALITY

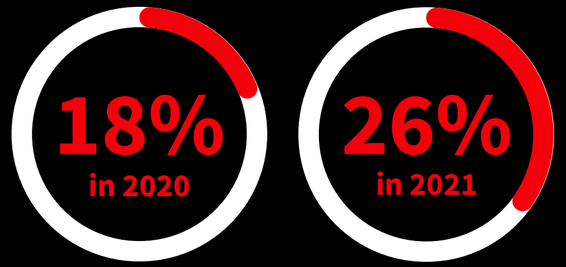
# 4.1 MILLION WEBSITES
HAVE MALWARE AT ANY GIVEN TIME

**5.5x**
more bot. traffic than human

and of those, more than 60% are malicious bots




Websites with
CRITICAL SEVERITY




**LESS THAN 8%**
OF MALWARE INFECTED WEBSITES WERE BLACKLISTED BY SEARCH ENGINES

HOW WE SOURCE OUR DATA

**14+ MILLION**
**Websites monitored**

**37+ BILLION**
**Files scanned each month**

**1.8 MILLION**
**Website owners with multiple domains**

**1.2 MILLION**
**Files cleaned each week**

# SMBs ARE MORE VULNERABLE THAN THEY THINK

To compile the findings in this report, SiteLock analyzed data from its global scanning network, which includes nearly 3 billion files scanned each month across more than 14 million websites. The company also looked at data from its CMS population, which covers more than 3.7 million websites. The vast majority of websites today are owned and managed by small-to-medium sized businesses with many ranging in size from sole proprietors to businesses with fewer than 50 employees.

In the 2021 State of Website Security and Threat Report, nearly half of all SMBs report being breached in the past. The impacts of breaches can be significant, ranging from website outages and loss of productivity to damage to the organization's reputation and brand. Every minute of downtime is a competitive disadvantage for SMBs, and a damaged reputation can be difficult, if not impossible, to repair. Hiscox calculated the average cost of a cyberattack for an SMB to be over $25,000, which can be crippling.

**CYBER ATTACK COSTS SMB**
**$25K ANNUALLY ON AVERAGE**

**Hiscox Insurance Company Inc**
https://www.hiscox.com/articles/average-annual-cost-cyber-attacks-us-small-business-25k-reveals-hiscox

Yet despite their own reports of past breaches and the many high-profile security breaches that have made headlines in recent years, many SMBs are overly confident in their security stance. Only 31% of survey respondents stated they were vulnerable to an attack, But as many eventually discovered, they were mistaken.

High-Risk Websites Are **41X More Likely** to Be Infected Than Low-Risk Websites

**41X**

To help inform SMBs of how vulnerable their websites actually are, website owners should assess their risks across a broad set of criteria. For example, the SiteLock Risk Score, which is a proprietary measurement that takes into account more than 500 data points to gauge the vulnerability of a website. The higher the risk score, from a scale of Low to High, the more likely it is that a website will be breached. Even a single data point can impact the score, underscoring the importance of taking website security seriously. Our data shows that high-risk websites are 41 times more likely to be infected than low-risk websites. With so much at stake, it's critical for SMBs to take website security seriously and take the necessary steps to protect their businesses.

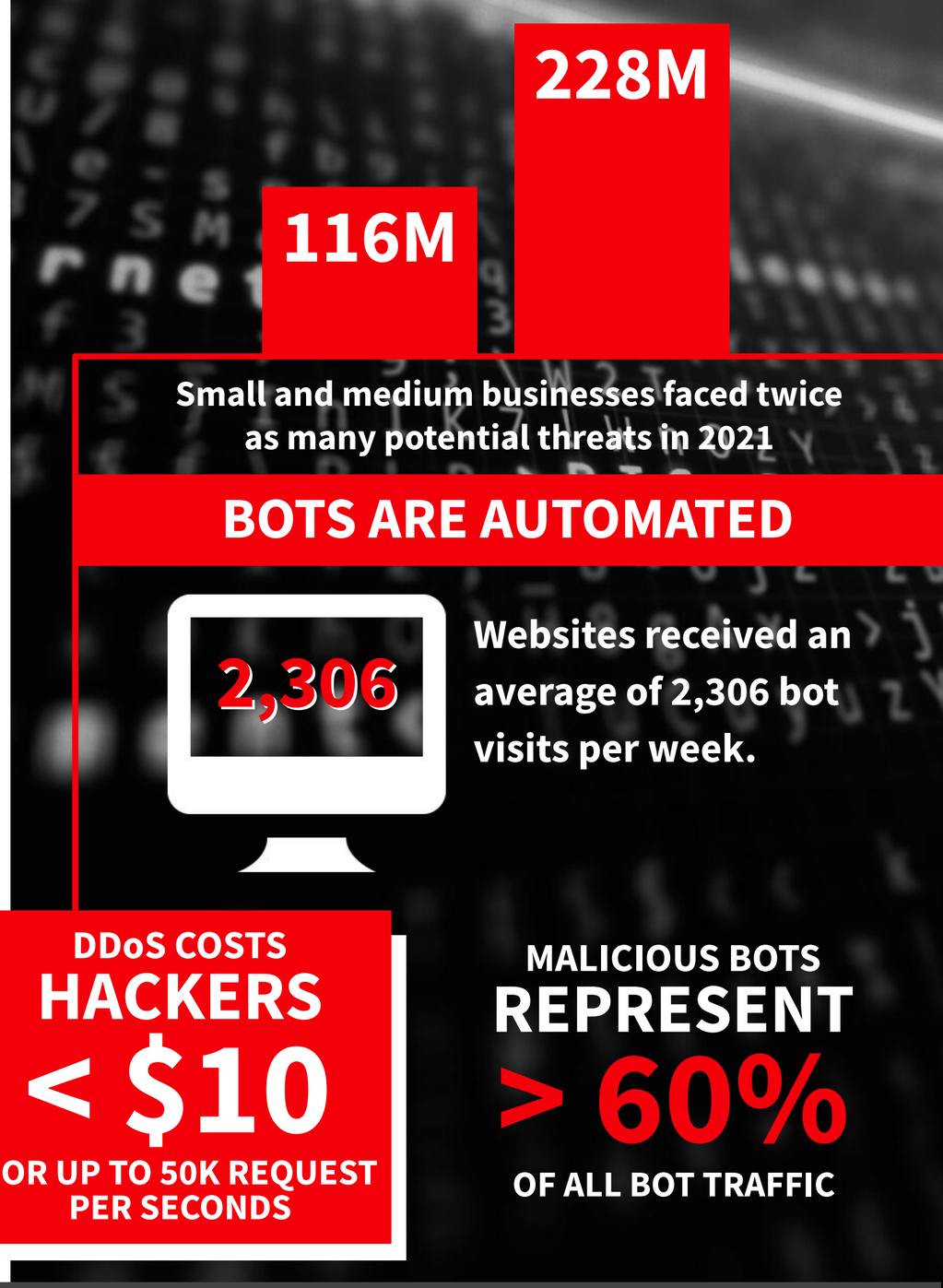
# THREATS DOUBLE IN VOLUME YEAR OVER YEAR WITH NO SIGN OF SLOWING

In 2021, small and medium businesses faced twice as many threats than they did in 2020. Our analysis of website security data found that SMBs experienced a staggering 228 million threats per month in 2021, compared to 116 million threats per month in 2020. This dramatic increase is due to the increasing scalability of attacks.

## SMBS BATTLE SKYROCKETING AUTOMATED BOT TRAFFIC

Hackers no longer sit behind their keyboard and launch attacks on big websites one at a time. The primary source of this doubling in attack volume is malicious bots. In fact, the vast majority of website attacks are conducted by automated bots and not by humans. Small and medium-sized businesses are facing a skyrocketing volume of bot traffic, with bots now accounting for an average of 2,306 visits per week per website according to our analysis of traffic data. Shockingly, that's 5.5 times more traffic to websites from bots than human users.

While there are legitimate reasons for bots to visit a website, such as search engine crawlers and copyright scans, bots are also used for a variety of nefarious purposes. Malicious bots can programmatically visit websites and identify vulnerabilities in the website's code to execute attacks at scale. From conducting distributed denial of service (DDoS) attacks to scanning for backdoor openings to insert malware to attempting brute force admin login credentials, this automated approach to attacks is actually very low cost and easy to deploy for hackers. Generic botnets can be purchased for a mere $5 per day, and malicious bot code builders are available on the dark web for just hundreds of dollars.




## AUTOMATION IS THE PROBLEM

Not only does automation increase the frequency any one site can be attacked and from different attack vectors, these bot-based attacks can also broaden the number of sites that hackers can attack. Hackers don't just attack high profile websites or businesses that collect financial data. Automated bot programs enable them to attack many sites at once no matter their size or type of business. They now have the tools to successfully exploit websites that likely do not have the resources or even the awareness to protect themselves.

In fact, many businesses and website owners are not ready nor even feel they need to protect themselves. Just under half (48%) of SMBs surveyed in the 2021 Website Security and Threat Report stated that they are too small to be a target for a website attack. As hackers scale their attacks using malicious bots, this belief poses a serious risk for any business as no website is immune from attack.

## AUTOMATION CAN ALSO BE THE SOLUTION

While automation is the problem, with attackers using bots to launch ever-more sophisticated and volumetric attacks, automation is also the solution. SMBs have access to specialized website security tools that are always on and auto-managed 24/7 and can automatically respond to attacks in order to stay ahead of threats.

For example, a web application firewall (WAF) that is constantly updated with real-time threat data is essential for blocking the bad bots, while allowing the good bots through. Additionally, each solution must have its own security protocol in order to provide redundancy in the event that one fails. For instance, a combination of domain name service security (DNSSEC) and a content delivery network (CDN) protects against DDoS attacks as a 'failover' if one component of your security infrastructure is unavailable.

By using a variety of specialized security automation tools and implementing a comprehensive security protocol, businesses can protect themselves from the ever-growing threat of bots and malware.

# MALWARE IS STILL A PROBLEM

The problem of malware is still very much alive and well for website owners. And that the types of malware being installed on websites are constantly changing. Not surprisingly, hackers constantly take advantage of disruptions and behaviors as new opportunities to exploit. For example, the outset of the COVID-19 pandemic saw a sharp increase in SQL injection attacks on customer websites as cybercriminals found this attack vector effective with website owners scrambling to adjust business practices and expand their online offerings. As SMBs became increasingly aware of this risk and took steps to protect their sites, cybercriminals adapted again.

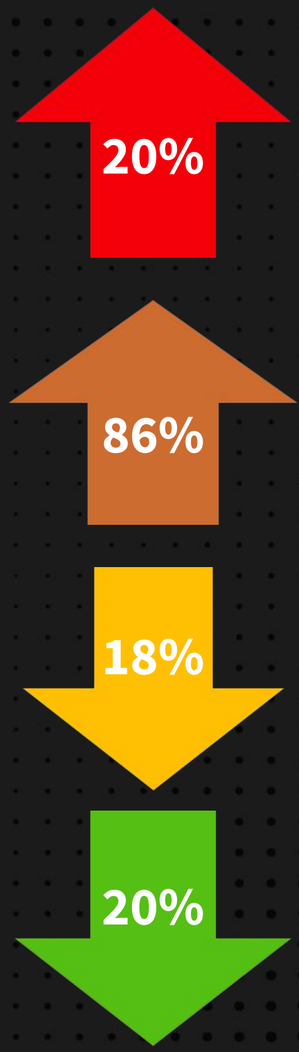
Now, criminals have turned to other attack vectors, such as backdoor, filehacker, malicious eval request, shell script, and phishing attacks. In line with OWASPs monitoring of website risks, SiteLock classifies the severity of website threats and malware into four categories based on the damage to business, though all threats can cause significant damage to businesses if left undetected and unremediated.

In 2021, high severity threats that often target website visitors, such as injector code, malware downloads, and redirects to malicious code, nearly doubled. Over a quarter of the sites with a malware infection included a high severity infection. Critical severity threats remain a significant problem as 18% of websites were infected with malware, such as shell scripts and filehacker, that can possibly spread and impact other connected systems and devices in an IT environment. Low severity threats declined slightly from 2020, though 25% of the infected websites had at least one low severity infection.

**HIGH SEVERITY MALWARE ATTACKS ARE UP**

**86%**

# THREAT SEVERITY




## CRITICAL

Critical severity threats if detected require immediate remediation as they can possibly affect other systems and devices that connect to your networked infrastructure. If left untreated, these threats have costly consequences, such as stolen data, permanent loss of visitor/customer trust, and irreparable damage to reputation and brand. Examples of critical severity threats include command control coordination malware and trojan scripts, such as shell scripts, filehacker, backdoor, eval requests, and uploaders.

**SHELL SCRIPTS** **FILEHACKERBACKDOOR** **EVAL REQUESTS** **UPLOADERS.**

## HIGH

High severity threats, like critical severity threats, can lead to stolen data, loss of visitor/customer trust, and damage to reputation and brand. High severity threats often impact users when simply visiting a website or clicking on a link, including injected code, phishing, malware downloads, and redirects to malicious code or websites.

**INJECTOR CODE** **PHISHING** **MALWARE DOWNLOADS** **REDIRECTS TO MALICIOUS CODE OR WEBSITES**

## MEDIUM

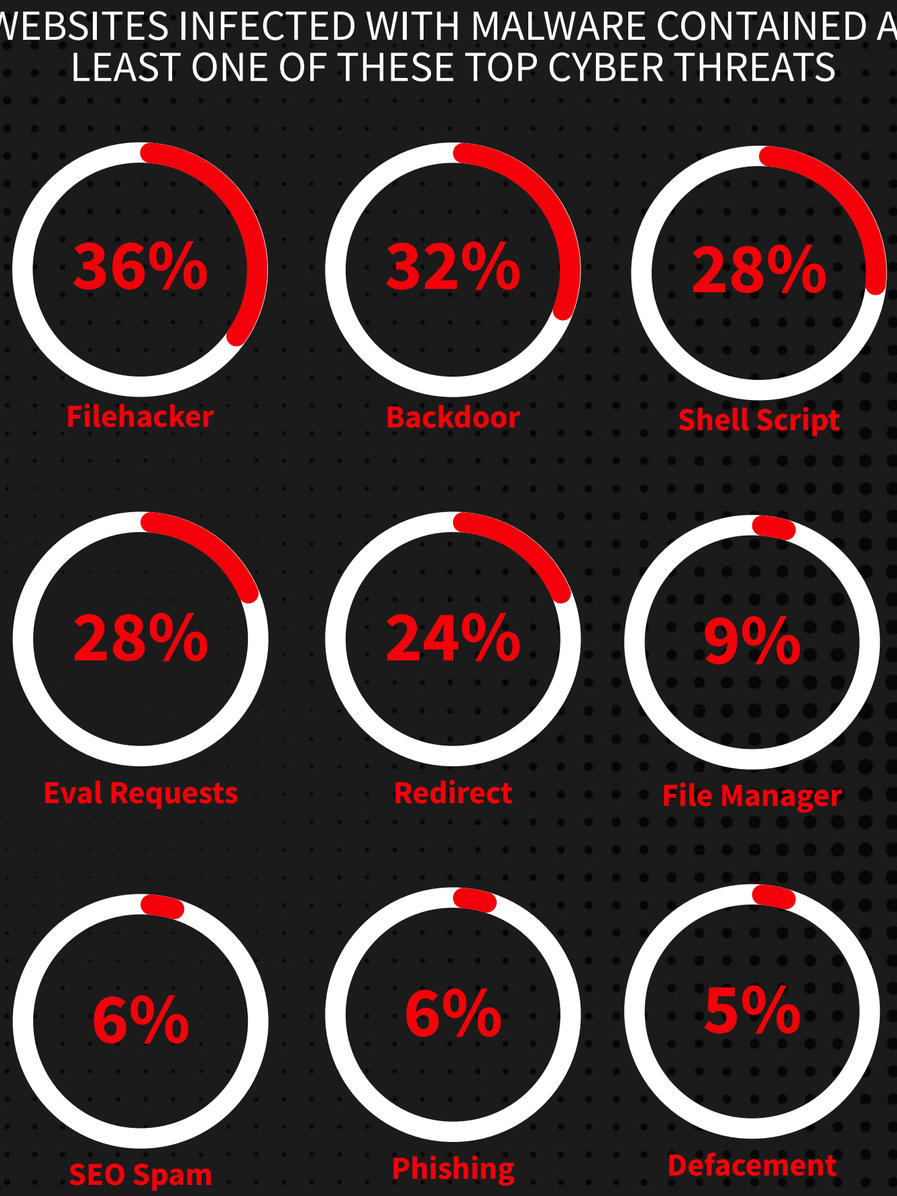
Medium severity threats can still cause reputational and trust damage, as well as 3rd party blacklisting. These threats should be addressed immediately as they include visitor attacks and generic PHP malware, such as Cryptominer and Mailer malware.

**CRYPTOMINER** **MAILER MALWARE**

## LOW

While low severity threats have a low impact or cost, they still cause reputational damage and loss of customer/visitor trust. Examples of low severity threats are defacement techniques, such as SEO spam and comment spam. While not ideal, these issues can be addressed over time without causing a significant amount of disruption.

**DEFACEMENT TECHNIQUES** **SEO SPAM** **COMMENT SPAM**




Results of our analysis of the types of threats deployed against websites in 2021.

## BACKDOORS AND MALICIOUS FILE MODIFICATION LEAD A LONG LIST OF WEB THREATS

Interestingly, SiteLock's analysis found that the number of websites infected by malware is down 20% in 2021 from 2020. However, this is more of an indication of appropriate levels of website remediation against malware threats. As malware threats evolve and increase due to automation, SiteLock found that the number of files cleaned of malware increased 237% over the previous year. Once a website has been infected, the number of attempts through varied automated attack vectors only increases and is a persistent challenge for website owners.

- 36% of infected websites had a filehacker attack. This type of file modification malware enables hackers to change or steal files.
- 32% of infected websites had a backdoor attack. This type of malware grants hackers unauthorized access directly to web site files, and in many cases, database access, which can lead to file or database modification, deletion, and data theft, including customer PII.
- 28% of infected websites had a shell script attack. This can enable hackers to take control of a website.
- 28% of infected websites had a malicious eval request attack. This can allow hackers to execute undesired code on a website.
- 6% of infected websites had a phishing attack. This is when fraudulent emails or other data forms are used to steal personal information.
- 6% of infected websites had comment section SEO spam. This is spam that uses black-hat SEO tactics to manipulate search engine results.


HOW CAN WEBSITE OWNERS KEEP MALWARE AT BAY

## AUTOMATE WEBSITE MALWARE SCANNING AND REMEDIATION

This data highlights the importance of having a robust website security strategy in place that protects against all types of threats being deployed against them, as well as effective remediation when malware has been injected. And these solutions must be automated so that SMBs are able to focus on running their business instead of worrying about becoming the next victim of a cyberattack.

Businesses can protect themselves from these damaging threats by staying up-to-date on patches, by using a scanning solution to find and fix vulnerabilities, and by training employees to be aware of the dangers of clicking on links or opening attachments from unknown sources.

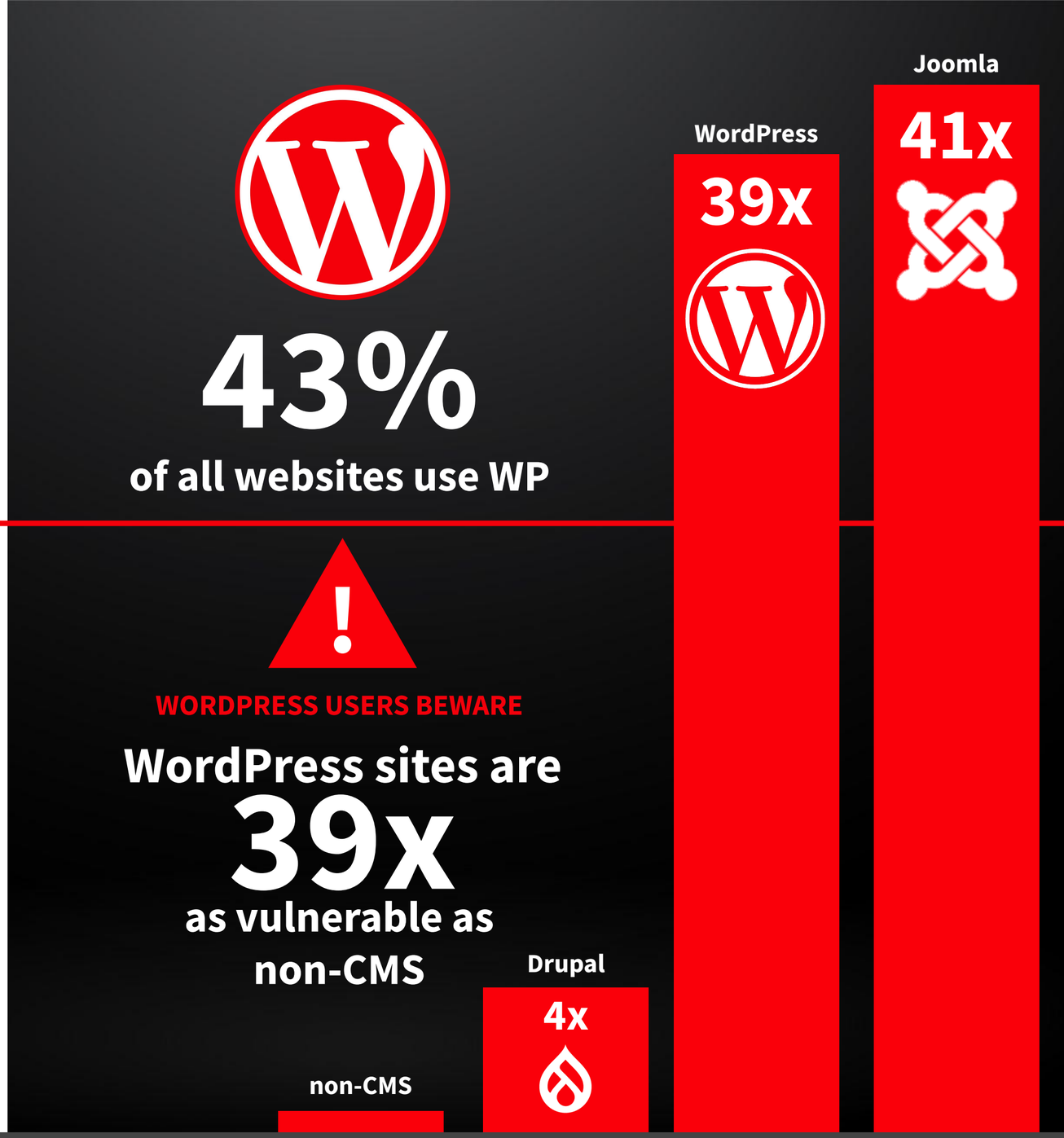
# CMS WEBSITES ARE BEING EXPLOITED AT AN ALARMING RATE

Content management systems (CMS) have many benefits for busy SMB website owners, from ease of content creation to added features with time-saving plugins and themes. However, with these benefits come significant security risks. Hackers increasingly target CMS websites in order to exploit vulnerabilities and inject malicious code. As a result, SMBs need to be especially vigilant in ensuring the security of their CMS-based websites.

## WORDPRESS & DRUPAL-BASED WEBSITES ARE POPULAR TARGETS

SiteLock's data shows that WordPress sites are 39 times more likely to be infected than non-CMS sites. This is largely due to the fact that WordPress is such a popular CMS- according to w3techs.com, 43% of the world's websites are built on it. Consequently, WordPress is a prime target for hackers. In fact, 9% of WordPress sites have at least one vulnerability, including SQLI, XSS, and CSRF attacks.

Drupal is another popular CMS that is often targeted by hackers. Our data shows that 9.5% of Drupal websites in our dataset were infected due to a vulnerability. This is, in part, due to the fact that Drupal is an open-source platform with many available modules and plugins.

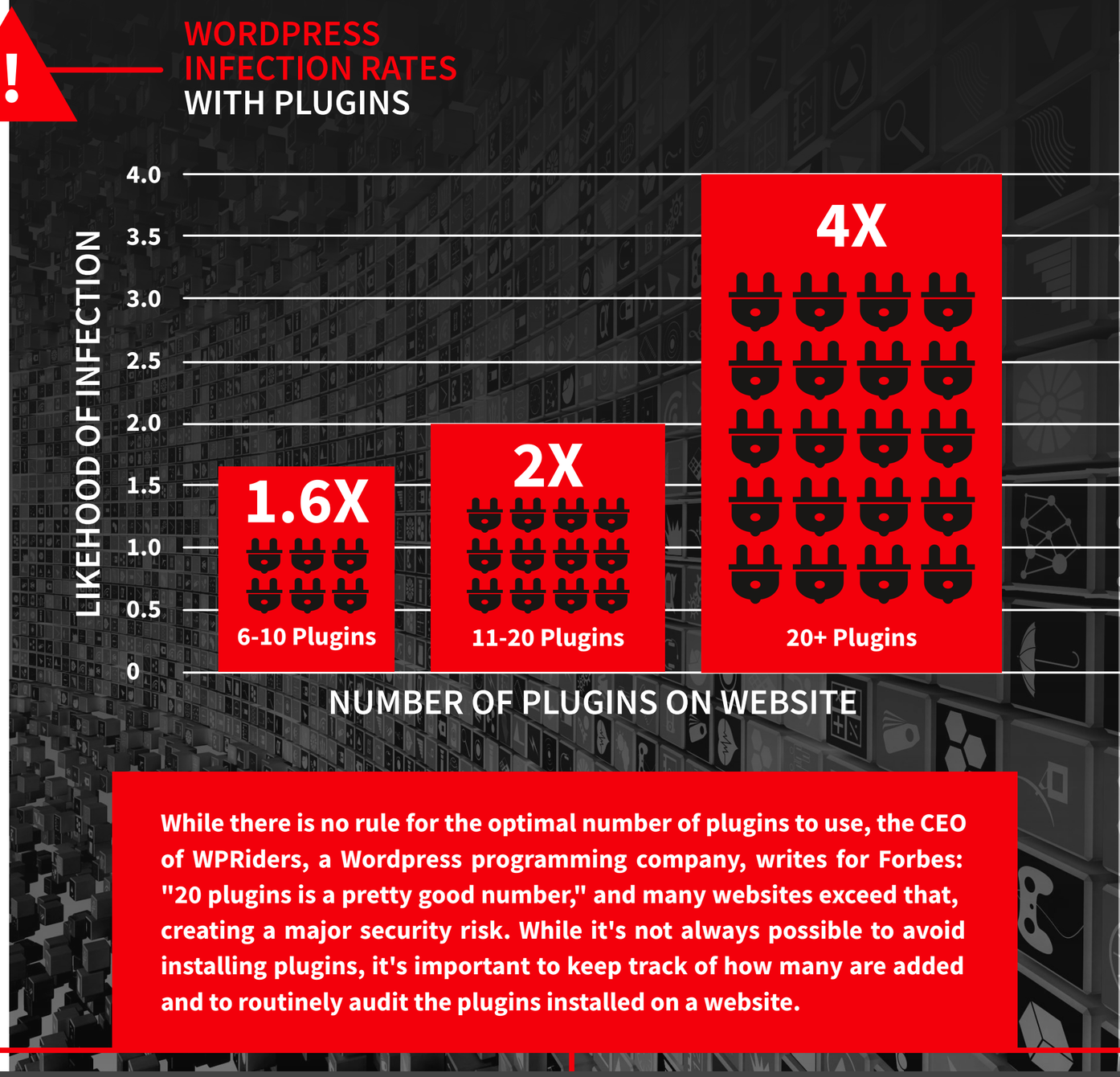


## THE MORE PLUGINS USED, THE MORE A SITE IS VULNERABLE

Plugins are an easy and effective way to add features and functionality to a CMS website. However, each plugin a website installs introduces new code to the website that is potentially exploitable by hackers. Making matters more difficult, website owners do not control the plugin code directly and rely on the publisher of the plugin to constantly patch their code against vulnerabilities.

As more plugins are added to a website, as many businesses do, plugin management quickly becomes a significant maintenance challenge. From keeping inventory of what plugins are installed to knowing if publishers are actively maintaining their own code to regularly updating as new patches are released, it is easy for a vulnerability to creep unknowingly into a website.

SiteLock's analysis of plugin vulnerabilities indicates that having a large number of plugins installed on your website also greatly increases risk. Websites with 5 or more WordPress plugins have nearly 2x the risk of being infected than websites with 0-4 plugins installed. The risk increases as the number of plugins increase, reaching 4x for websites with 20 or more plugins installed.



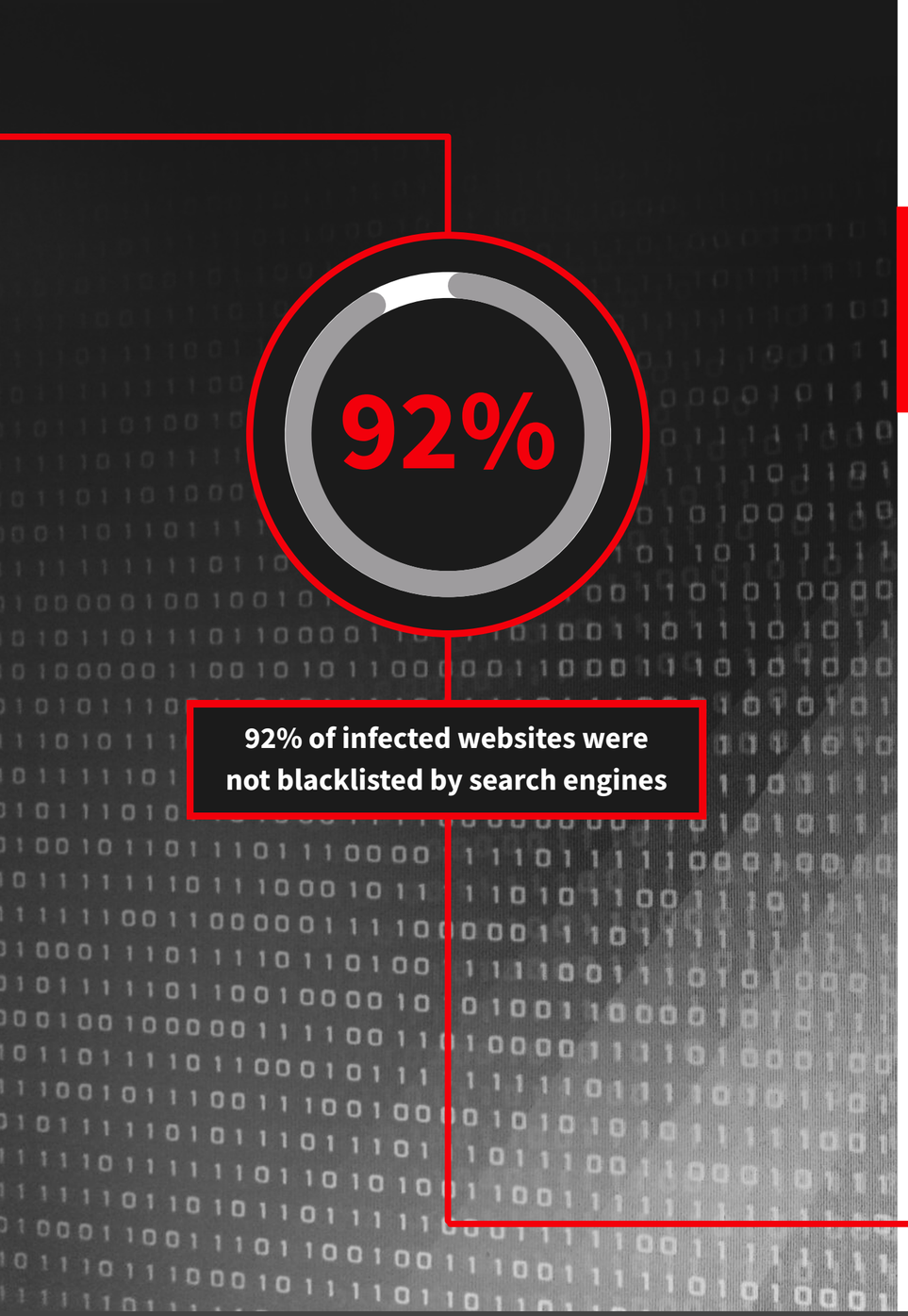

**While there is no rule for the optimal number of plugins to use, the CEO of WPRiders, a Wordpress programming company, writes for Forbes: "20 plugins is a pretty good number," and many websites exceed that, creating a major security risk. While it's not always possible to avoid installing plugins, it's important to keep track of how many are added and to routinely audit the plugins installed on a website.**

> “Utilizing open-source applications is a great way for businesses to quickly add new functionality to their website. Unfortunately, the use of unmanaged plugins, themes and CMS’ can reduce a website’s security posture and potentially allow Critical Vulnerabilities to be exploited by attackers.”

— **Martin Fiegl**
**SiteLock Research Sr. Manager**

## UPDATE PLUGINS AND CMS CODE FOR PROACTIVE PROTECTION

**To protect your website from being hacked, it is important to take a proactive approach and ensure that your CMS and plugins are up-to-date, and that you only install plugins from reputable sources. Additionally, it is essential to have a comprehensive website security solution in place that can detect and prevent threats.**




# SEARCH ENGINES AREN'T PROTECTING YOU, AND OFTEN NOT YOUR CUSTOMER EITHER

Search engines are the front door to the internet for many website visitors and customers, so it's not surprising that search engines are a significant source of traffic for websites. From search result rankings to local listings and online maps, website visitors and customers rely on search engine results to show only trusted links.

However, search engines often miss widespread malware infections, leaving website owners and their visitors vulnerable to attack. Website visitors and customers who rely on search engines to identify malware-infected websites are particularly at risk, as 92% of all malware-infected websites are not flagged or blacklisted by common search engines. And when a business' website contains or spreads malware to visitors, it is the business that faces the blame and loss of reputation from customers, not the search engine.

Not only that, but getting a website removed from a search engine blacklist can take up to 30 days or more, depending on the severity of the malware and how many times that site was blacklisted historically. This leaves businesses with an infected website struggling to remove the infection and protect their customers, as well as their online reputation. SiteLock prevents sites from being blacklisted by search engines, so businesses can keep their website up and running.

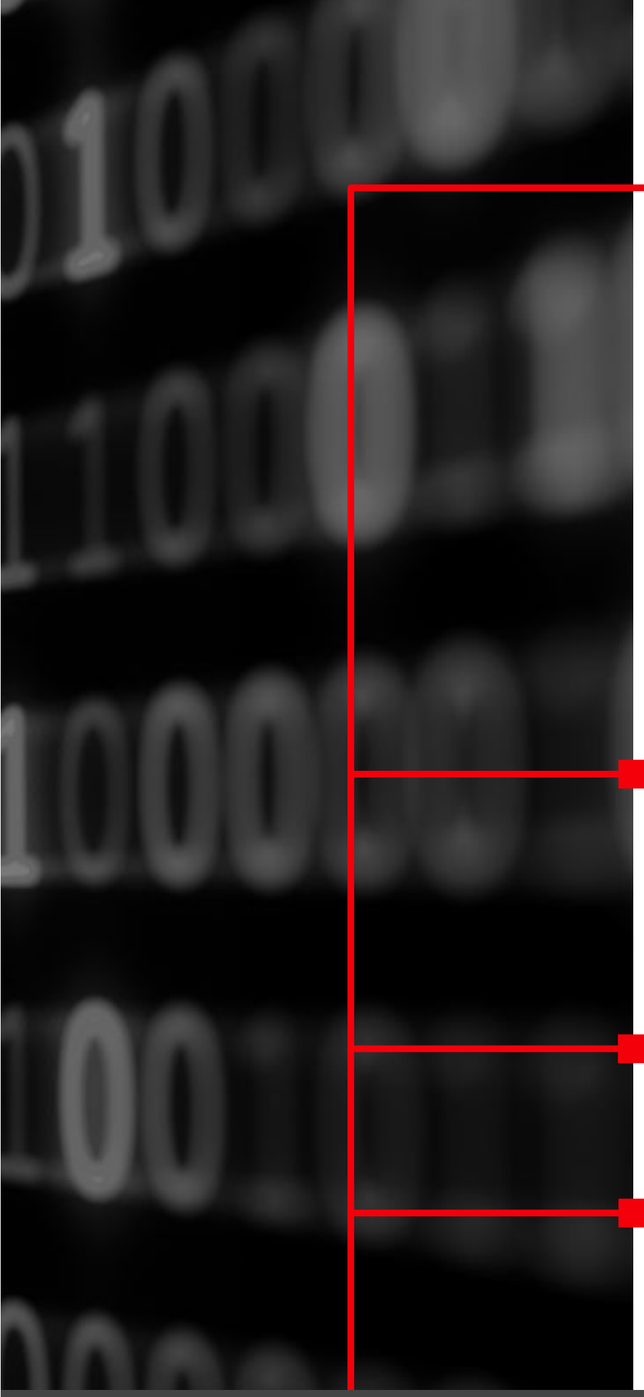
# GUIDANCE: A COMPLETE SECURITY SOLUTION IS NEEDED

SMBs today are under constant attack. And while they face an explosive rise in attacks and the broad range of threats, there are steps that can be taken to make a business more secure. A complete security solution that includes technologies like SSL certificates, CDNs, and WAFs is crucial. Further, the security solution must be automated to be always on, always updated, and failover protected to guard against threats before they have a chance to reach the website. And in the event of malware infection, automation also helps to remediate the threat immediately before irreparable damage can be done. This comprehensive, automated approach to website security provides peace of mind for organizations of all sizes.

Although being "100% safe" may remain impossible, SMBs can and should invest in solutions and partnerships that will grow and evolve along with the threats and attack vectors they face. In order to stay ahead of the curve, SMBs need a partner that is capable of providing that level of support. This gives SMBs the best of both worlds, allowing them to take advantage of both the depth of expertise and the ability to stay up-to-date on security threats that a leading vendor provides, while fitting within the comparatively limited budget and skill profile of most SMBs.

## 2022 WEBSITE SECURITY CHECKLIST

- ☐ Stay up-to-date on the specific security threats of your website.
- ☐ Plan ahead. It's not a matter of if you will experience an attack but when. Know what to do in the event of a cyberattack.
- ☐ Leverage automation in your favor with tools that automatically detect security risks and can patch vulnerabilities.
- ☐ Implement a various methods to block attacks (Firewall, SSL certificates, CDN, etc). Bad actors continuously evolve and their attack strategies will change.
- ☐ Conduct regular website audits and file reviews for unusual file names or content.
- ☐ Remove outdated and unused plugins and themes.



# SMBs NEED A TRUSTED SECURITY PARTNER

SiteLock is one such provider. A comprehensive website security platform, SiteLock helps protect SMBs from a variety of online threats, including malicious bots, attacks of all kinds, while addressing bandwidth and resource hassles. Using SiteLock can help you ensure that your site is protected and functioning reliably, giving you peace of mind and allowing you to focus on what you know best: your business.

SiteLock's proprietary Risk Assessment tool analyzes over 500 variables to determine a website's risk level. The three main categories that account for a site's risk include website complexity, site popularity, and site composition.

**Website Complexity:** The size of the website, the number of files it contains, and the number of directories are all factors that contribute to website complexity. The more complex a website is, the more opportunities there are for something to go wrong and for a hacker to exploit vulnerabilities.

**Site Popularity:** A website's popularity also contributes to its risk level. The more traffic a site receives, the more opportunities there are for hackers to attempt an attack.

**Site Composition:** The software, content management system, plugins, and themes used to build a website can also make it more susceptible to attack. Out-of-date software and plugins can leave websites vulnerable, as can using popular themes with known security holes.

Additionally, site speed is a critical indicator of a reliable, well-maintained website. Consumers are increasingly impatient—a one-second delay can lead to a 7% loss in conversions, 11% fewer pageviews, and a 16% decrease in customer satisfaction. It's clear that website speed is essential for a positive user experience, high rankings in search engines, and good conversion rates. That's where SiteLock TrueSpeed Content Delivery Network (CDN) comes in. It works by caching static files like images, JavaScript, and CSS so that they can be served quickly and without delay. When a request is made for one of these files, the cached copy is intelligently delivered instead. This saves the server from having to generate the file on-the-fly, resulting in a faster loading website.

Using SiteLock enables SMBs to take proactive steps toward protecting their business and ensuring a reliable online presence. SiteLock's malware scanning and detection capabilities can help to uncover hidden malware infections and identify vulnerabilities that could be exploited by hackers. While its remediation services proceeds to clean websites of these malicious codes, the Web Application Firewall (WAF) can help to block future threats at scale.

# APPENDIX

## Key Statistics

- 27% of infected websites have more than one type of malware infection
- 8.42% of websites infected with malware were blacklisted by search engines
- The average website receives 2,306 bot visits per week.
- Total Sample Size: 14,117,997 Million sites
- 37 billion files scanned every month
- Bot traffic is 5.5x more than human visitors
- High severity Threats increased 86% in 2021 from 2020
- 93% of infected sites were not flagged or blacklisted in google.
- Average number of attacks per day per site: 172
- 210% increase in attacks from 2020
- 18% of infected websites are infected with Critical Severity Threats
- 237% increase in files cleaned

## Scan Statistics

- Average infected sites per week: 2,713
  - SMART file infection rate: 0.02%
- Average number of files cleaned per week: 1,229,385
  - Average number of files cleaned per week per site: 637

## Risk Score

- Low risk sites infected: 0.06%
- Med risk sites infected: 0.02%
- High risk sites infected: 2.43%
- High risk sites are 41 times more likely to be infected

## Malware Statistics

- Sites impacted:
  - 27% of websites had more than one malware infection type
  - 35.84% of file infections had at least 1 filehacker
  - 31.62% of file infections had at least 1 backdoor
  - 28% of file infections had at least 1 malicious eval request
  - 9.14% of file infections had at least 1 filemanager
  - 28% of file infections had at least 1 shell script
  - 5.87% of infected sites had at least 1 SEO spam file
  - 24% of infected sites had at least 1 redirect
  - 5% of infected sites had at least 1 defacement
  - 6.35% of infected sites had at least 1 phishing file

## XSS Vulnerabilities

- Sites with XSS vulnerabilities: 1.35%
- Sites w/ XSS vulnerabilities that were infected: 1.96%
- Total pages with XSS vulnerabilities: 1,003, 985
- Vulnerable pages per site: 294

## SQLi Vulnerabilities

- Sites with SQLi vulnerabilities: 1.57%
- Sites w/ SQLi vulnerabilities that were infected: 1.85%
- Total pages with SQLi vulnerabilities: 332,657
- Vulnerable pages per site: 486

## CSRF Vulnerabilities

- Total Sites with CSRF: 82,760
- Sites with CSRF vulnerabilities: 0.37%
- Sites w/ CSRF vulnerabilities that were infected: 2.17%

## WordPress Statistics

- Percentage of WP Population with Malware: 0.83%
- Sites that had at least one vulnerability (XSS, SQLi, or CSRF): 8.96%
- Sites running WooCommerce: 13:68%
- Sites that are infected with WooCommerce installed: 0.92%

## WordPress Plugins:

- Sites that had 1-5 plugins installed that were infected: 0.73%
- Sites that had 6-10 plugins installed that were infected: 1.00%
- Sites that had 11-20 plugins installed that were infected: 1.24%
- Sites that had 20+ plugins installed that were infected: 4.43%
- Sites that were infected that had no plugins installed: 0.03%

## Joomla! Statistics

- Percentage of Joomla Population with Malware: 0.60%
- Percentage of Joomla Population with Vulnerability and Malware: 1.26%
- Sites that had at least one vulnerability (XSS, SQLi, or CSRF): 9.56%

## Drupal Statistics

- Percentage of Drupal Population with Malware: 0.98%
- Percentage of Drupal Population with Vulnerability and Malware: 9.42%
- Sites that had at least one vulnerability (XSS, SQLi, or CSRF): 0.98%

## Non-CMS Statistics

- 0.23% of non-CMS sites were infected with malware.
- Sites that had at least one vulnerability (XSS, SQLi, or CSRF): 0.035%