2023 SITELOCK ANNUAL WEBSITE SECURITY REPORT

SiteLock

A SECTIGO® COMPANY

TABLE OF CONTENTS

2023 SITELOCK ANNUAL WEBSITE SECURITY REPORT

EXECUTIVE SUMMARY

03

Remember when your biggest online worry was finding the perfect caption for your latest Instagram post?

Today, those concerns feel like relics of a simpler digital era. In 2024, the internet has become a battlefield where cybercriminals deploy sophisticated tools like AI to mimic voices, execute targeted attacks, and take down entire businesses faster than a speeding bullet. It's no longer just about keeping your website online—it's about defending it as the frontline of your security strategy.

This year's SiteLock Annual Website Security Report dives deep into the shifting cyber threat landscape, analyzing data from 14 million websites scanned daily and 2 billion files scanned monthly. The findings shine a floodlight on a stark reality for small and medium-sized businesses (SMBs): the digital predators are evolving faster than their prey can defend.

04 Key Findings and Implications

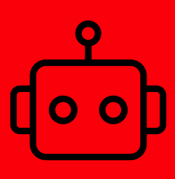
Threats are up

43%

from 2022

A Tsunami of Attacks

Imagine the entire population of Europe being targeted twice a month—every month. That's the scale of 2023's cyberattacks, which surged to 732 million threats monthly—a 43% increase from 2022. This dramatic rise underscores the urgent need for robust, multi-layered security measures. Attack frequency per site also grew by 24% daily. If your defenses aren't keeping pace, it's like fighting a wildfire with a garden hose.



Nearly

10x

more bot traffic than human

The Bot Invasion: Your Invisible Intruders

Bots have swarmed the internet. For every real visitor to your site, nearly ten bots sneak in—a 40% increase from 2022's ratio of seven bots per human. These aren't harmless spectators; they're silent thieves, scraping your data, testing your passwords, and choke systems. Malicious bots now make up over half of all bot traffic and without advanced detection and defenses, your website becomes an open buffet for these digital pests.

Joomla sites are

13x

more at risk of exploits

CMS Vulnerabilities: A Digital House of Cards

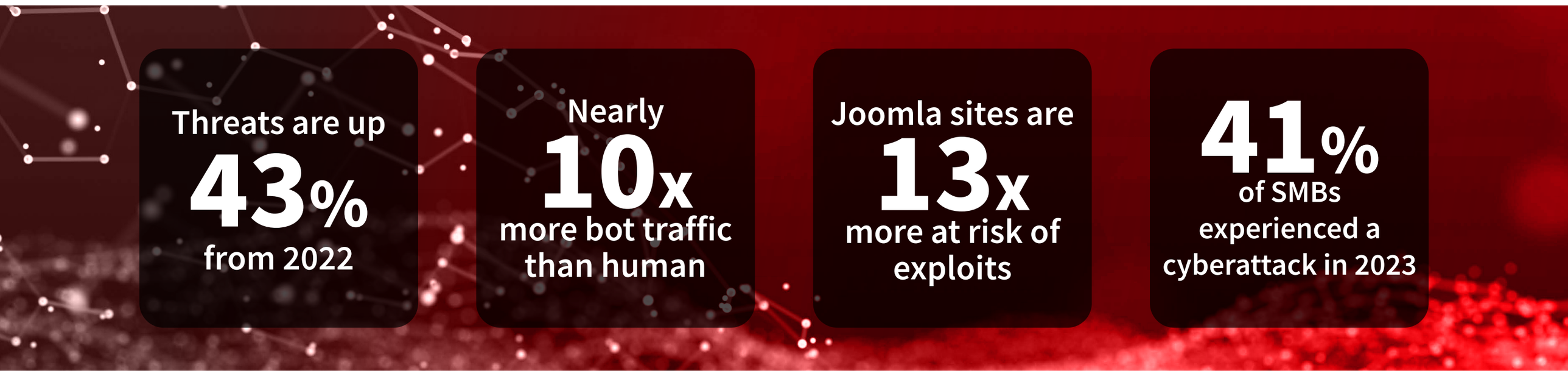
For SMBs relying on content management systems like WordPress, Joomla etc. vulnerabilities are a pressing concern. In 2023, WordPress sites were 10x more vulnerable to attacks compared to non-CMS platforms, and Joomla sites faced 13x the risk. Think of it like living in a high-crime neighborhood with unlocked doors and windows. Regular updates and security audits are no longer optional—they're essential for survival in the digital space.

05 **Key Findings and Implications** continued...

41%
of SMBs experienced a cyberattack in 2023

SMBs: The Knowledge-Action Gap

Small businesses are growing savvier about cybersecurity. Yet despite this increasing awareness, 41% still fell victim to cyberattacks- a stark reminder that knowing the risks isn't enough. This troubling gap between knowledge and action often stems from a dangerous misconception: "We're too small to be targeted." To bridge this gap, SMBs must shift from reactive to proactive measures, adopt multi-layered security strategies and foster a security-first culture.



AI: The Cybercriminal's New Best Friend

AI is reshaping cybersecurity as both a shield and a weapon. While it empowers defenders with advanced threat detection and prediction, cybercriminals are using it to devastating effect. AI-generated malware and phishing campaigns have seen a significant uptick, posing new challenges for traditional security measures.

Imagine receiving a video message from what appears to be your website hosting provider, asking you to approve urgent security updates. The voice and visuals seem authentic, but they're AI-generated, designed to steal credentials or inject malicious code into your website. In 2023, this went from an improbable scenario to an alarming reality.

The cybersecurity battlefield has become an arms race, with both defenders and attackers leveraging the same powerful tools. Staying ahead of this evolving threat is no longer optional—**it's essential.**

The implications for all

The cybersecurity battlefield has become an arms race, with both defenders and attackers leveraging the same powerful tools. Staying ahead of this evolving threat is no longer optional—it's essential.
The findings of this report have far-reaching implications for businesses of all sizes:

Increased Investment in Security
The rise in threats necessitates a proportional increase in security measures. Businesses must view cybersecurity not as an IT expense, but as a critical investment in their future—think of it as a digital insurance policy.

Adaptive Security Strategies
With threats evolving at an unprecedented pace, static security measures are no longer sufficient. Businesses need to adopt adaptive, data-powered security solutions that can keep pace with emerging threats, much like how our immune systems adapt to new viruses.

Education and Awareness
The persistent human factor in security breaches highlights the need for ongoing employee education and the cultivation of a security-first culture within organizations. Your team needs to be as cyber-savvy as they are job-skilled.

Proactive Rather than Reactive
Waiting for a breach to occur before taking action is no longer a viable strategy. Businesses must adopt a proactive stance, regularly assessing their security posture and addressing vulnerabilities before they can be exploited. It's the difference between preventing a fire and fighting one.

As we navigate this new frontier of digital threats, the insights provided in this report serve as a crucial roadmap for businesses looking to safeguard their digital assets. The subsequent sections delve deeper into each of these findings, offering detailed analysis and actionable recommendations to fortify your website security in 2024 and beyond.
Stay **vigilant**, stay **informed**, and most importantly, stay **secure**.

SMBS: GROWING AWARENESS, GROWING VULNERABILITIES

07

As we delve deeper into the evolving cyber threat landscape, the focus shifts to a group that is increasingly under siege: small and medium-sized businesses.

Although small and medium-sized businesses (SMBs) are becoming increasingly aware of cybersecurity risks, awareness alone is not enough. In 2023, 63% of SMBs identified themselves as cyber intermediates, while 4% claimed expertise in managing threats, according to data from the Hiscox Cyber Readiness Report. Yet, despite this growing knowledge base, 41% of SMBs experienced a cyberattack, up from 38% in 2022.

Adding to this alarming trend, the total number of attacks surged to 732 million per month in 2023, a 43% increase from 2022. For SMBs, this starkly underscores the widening gap between understanding cybersecurity risks and implementing effective defenses—a gap that cybercriminals are eager to exploit.

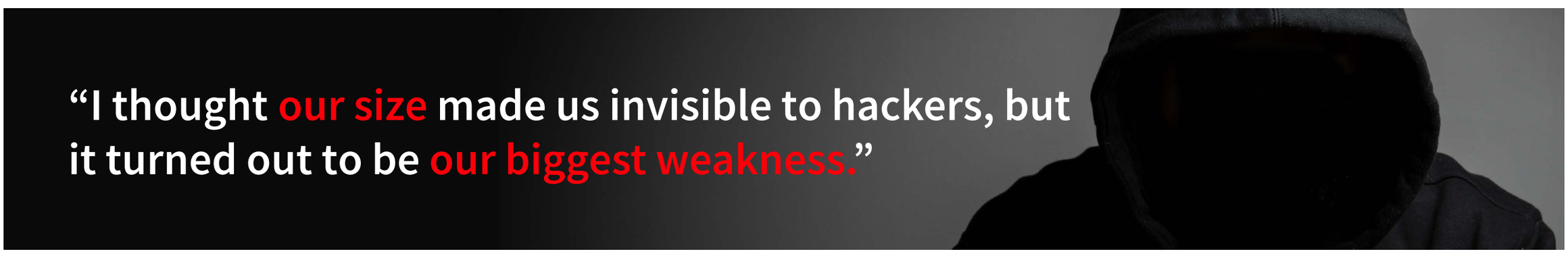
08 The Perception Problem

A dangerous misconception continues to persist among SMBs: “We’re too small to be targeted.”

This misconception is not only misleading but dangerous. In fact, over 60% of small businesses believe they are too small to be a target, and among sole proprietors, this number rises to 73%, illustrating just how widespread—and risky—this belief is. (Source: IBC’s 2023 Cyber Security Survey)

For Kaila Uli, owner of the jewelry business Brillies, this mindset came at a devastating cost. As highlighted in a recent Marketplace report, her company fell victim to repeated ransomware attacks. Brillies lacked an IT department, and although Uli was tech-savvy, she quickly found herself overwhelmed as the attacks persisted.

Unable to stop the breaches, Kaila faced months with almost no sales and no income. In desperation, she attempted to recreate Brillies under a new URL, but the attackers followed her there, targeting her new site with the same intensity. Ultimately, the financial and emotional strain forced Uli to shut down Brillies altogether. Reflecting on her experience, she admitted:



This story underscores a harsh truth for SMBs: attackers don’t overlook smaller businesses—they exploit them because they’re seen as easier targets. The belief that SMBs are too small to matter not only increases vulnerability but magnifies the consequences when a breach occurs.

Why SMBs Are Prime Targets:
The perfect mix of value and vulnerability

- **Lower Defenses:** Smaller budgets often mean limited resources for advanced tools or regular updates.
- **Valuable Data:** Even small businesses hold sensitive customer and financial information, making them appealing to ransomware campaigns
- **Gateway Attacks:** SMBs frequently serve as entry points to larger supply chains, enabling attackers to breach enterprise partners

09 Adding to the Challenge

While stories like Kaila's highlight the devastating consequences of misguided assumptions, they are far from isolated incidents. SMBs face an escalating threat landscape, with challenges compounded by a mix of technical vulnerabilities, human errors, and resource limitations:

Overconfidence in Basic Tools: Many SMBs rely solely on antivirus software or simple firewalls, which are no match for the sophisticated tactics employed by today's attackers.

The Human Factor: Weak passwords, phishing attacks, and misconfigured settings remain leading causes of breaches. In 2023, AI-powered phishing campaigns became increasingly polished, tricking even vigilant employees with convincing, professional language.

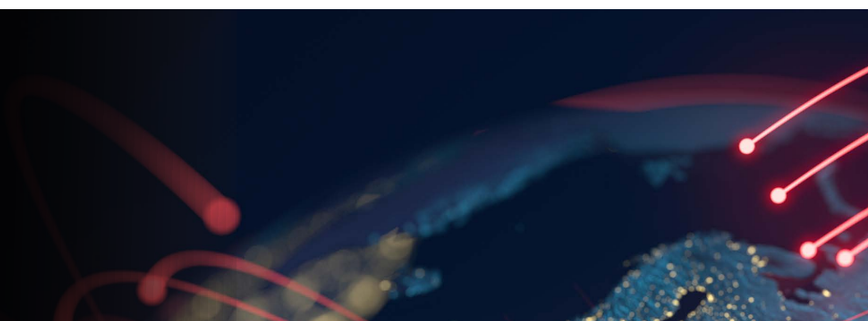
CMS and Custom Website Risks: Websites built on platforms like WordPress or custom-coded solutions face significant risks from outdated plugins, themes, or inadequate security practices

These vulnerabilities collectively expose SMBs to higher infection rates and more severe consequences when attacks occur. The stakes are high: operational downtime, loss of customer trust, and financial repercussions that can cripple even the most resilient businesses.

These vulnerabilities collectively expose SMBs to higher infection rates and more severe consequences when attacks occur. The stakes are high: operational downtime, loss of customer trust, and financial repercussions that can cripple even the most resilient businesses.

Bridging Awareness and Action: SiteHealth

For SMBs, bridging the gap between awareness and action is critical to defending against today's sophisticated cyber threats. SiteLock's SiteHealth tool offers a comprehensive, real-time evaluation of a website's vulnerabilities, empowering businesses to act before issues escalate.



How It Works

SiteHealth consolidates insights from over 10 critical security scans, generating an actionable status ranging from Healthy to Compromised. By evaluating factors like detected malware, misconfigurations, and outdated software, it provides dynamic recommendations tailored to address specific vulnerabilities.

Think of SiteHealth as a **routine wellness check-up** for your website. Just as a doctor identifies and treats health risks before they worsen, SiteHealth helps SMBs **detect and resolve vulnerabilities** before they lead to devastating breaches.

Why It Matters

The urgency of adopting tools like SiteHealth cannot be overstated. In 2023:

HIGH-RISK WEBSITES WERE **60X** MORE LIKELY TO BE INFECTED, A **48%** INCREASE FROM 2022

MEDIUM-RISK SITES SAW THEIR INFECTION RATE SURGE BY **116%** WHILE HIGH-RISK SITES EXPERIENCED A **47%** INCREASE IN INFECTIONS YEAR-OVER-YEAR

These figures underscore the growing danger SMBs face, where even slight delays in addressing vulnerabilities can have severe consequences.

What Sets SiteHealth Apart

Unlike traditional tools that merely identify risks, SiteHealth provides SMBs with a clear status (Healthy, At Risk, or Compromised) and tailored security actions to-do list to mitigate those risks. This ensures businesses can act decisively, safeguarding their digital assets in an ever-evolving threat landscape.

Key Takeaway

Believing “it won’t happen to us” is not just a misconception—it’s an open invitation for cybercriminals. SMBs must move beyond awareness, taking proactive steps to protect their businesses from the escalating threat landscape. Tools like SiteHealth empower businesses to understand, monitor, and mitigate risks, ensuring their websites remain operational and secure.

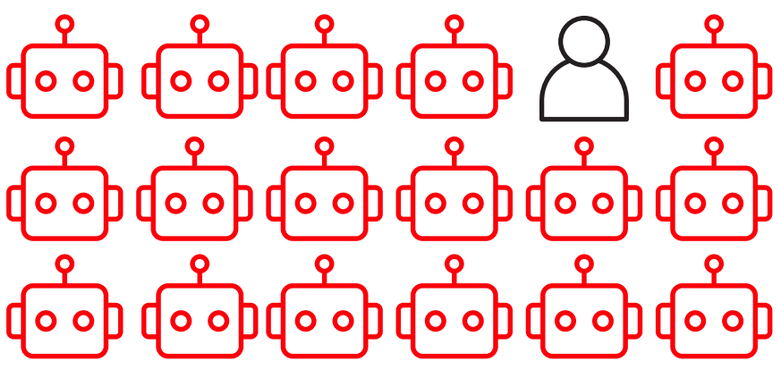
THE FAST AND THE MALICIOUS: BOT ARMAGEDDON

11

In 2023, cyber threats reached unprecedented heights, with websites encountering an average of 732 million threats monthly—a dramatic 43% increase from 2022's 512 million. At the core of this escalation lies a silent yet formidable adversary: bots. These automated programs dominate the digital battlefield, reshaping the threat landscape with their scale, precision, and sophistication.

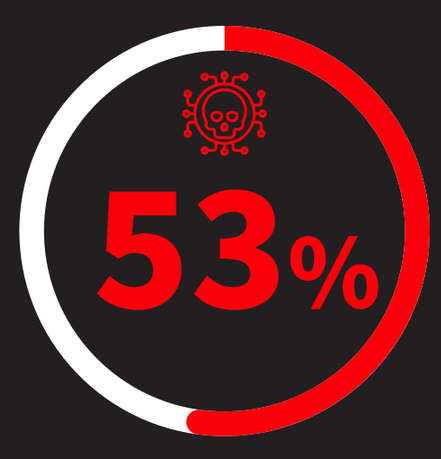
Prevalence and Malicious Intent: The Twin Trends of Bot Activity

At the heart of the bot surge are two interlinked trends:
Prevalence and Malicious Intent



Prevalence: In 2023, websites faced an average of **4,258 bot visits** per week, with bots outnumbering human visitors by a staggering ratio of **9.9 to 1**- a **40% increase** from 2022.

Malicious Intent: Among this torrent of automated traffic, **53%** of bots were malicious, transforming them into the **primary drivers of cyber threats** and leaving legitimate traffic in the minority



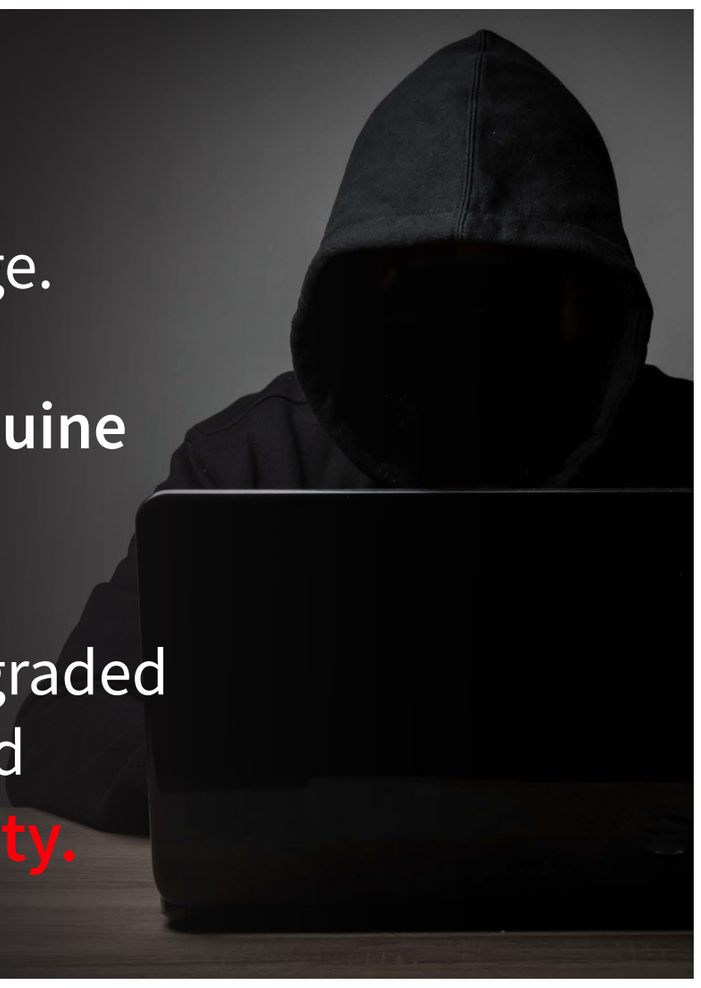
These trends underline the growing dominance of bots in online ecosystems, posing unique challenges for businesses of all sizes, particularly SMBs.

A Daunting Challenge for SMBs

For SMBs, these trends represent a formidable challenge.

Imagine running a physical store where, for every genuine customer, ten others enter to disrupt or steal.

The consequences are immediate and far-reaching: degraded website performance, stolen customer data, and eroded trust—all amplified by the **growing scale of bot activity.**



12 Driving the Surge: Automation, Machine Learning, and AI

The driving force behind these trends are advancements in automation, machine learning, and AI, that have transformed bots into faster, smarter, and more evasive entities. Once the domain of sophisticated hackers, the ability to design and deploy bots is now widely accessible, even to non-technical actors thanks to tools like generative AI and large language models (LLMs), amplifying the scale and precision of cyberattacks.

AI-powered bots can now replicate human-like interactions, making them harder to detect. Powered by LLMs, bots can now respond to emails, text messages and chat with contextually aware input. Tasks that earlier required human intervention can now be easily automated, blurring the lines between legitimate and malicious activity.

Advanced bots can evade traditional defenses like firewalls and CAPTCHA systems with ease, using AI to adapt to security protocols in real time.

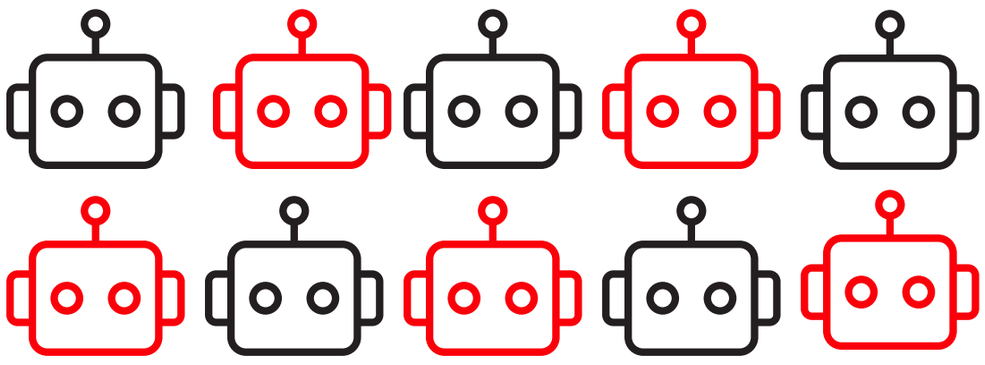
Bots are capable of conducting multi-layered attacks, targeting vulnerabilities with unprecedented efficiency.

Consider this scenario: A contact form under siege by AI-driven bots submitting entries that **appear human.** On the surface, these entries look real but include harmful links, spam, or even malicious scripts designed to **bypass basic validations.**
In no time, a simple communication tool is **weaponized** into a portal for cyber threats that can - overwhelm support teams with fake inquiries, **exploit vulnerabilities** in the form handling process to steal data or inject malicious scripts designed to compromise backend systems or redirect users to phishing sites.

For SMBs, these developments create a perilous environment. AI-powered bots have thrust them on the frontlines of an automated onslaught, often outgunned and unprepared to defend against such sophisticated threats.

13

Malicious Bots: The Backbone of Modern Cyber Threats



FOR EVERY **10 BOT VISITS**
~
ARE MALICIOUS

From simple disruptions to large-scale attacks, bots are now core tools in the cybercriminal arsenal. Today, they are omniscient, omnipresent, and indispensable for cybercriminals carrying out activities that overwhelm SMBs and large organizations alike.

It's no exaggeration to call them the backbone of modern cyber threats, as they execute a range of attacks including:

- **Credential Stuffing:** Testing stolen login credentials at scale
- **DDoS Attacks:** Overwhelming servers with traffic, rendering websites inaccessible
- **Data Scraping:** Extracting sensitive customer or proprietary information

For SMBs, malicious bots represent a relentless adversary, probing for vulnerabilities and exploiting weaknesses at scale.

High-Risk Sites: The Multiplier Effect

The high-risk status of a website acts as a beacon for bots, drawing automated threats like moths to a flame.

Earlier in this report, we highlighted that high-risk sites are **60 times more likely to face infections**—a statistic that takes on even greater significance when viewed through the lens of bots' growing dominance.

60x

This number isn't just a warning—it's a reflection of a broader truth: vulnerabilities act as magnets for malicious bots.

- **Prime Targets:** Bots are programmed to exploit low-hanging fruit, and high-risk sites offer exactly that
- **The Vulnerability Loop:** Each bot-driven attack compounds existing flaws, deepening the site's risk profile and attracting even more malicious activity
- **Exponential Exposure:** As weaknesses deepen, bots flock to these sites, compounding the damage and perpetuating the cycle of vulnerability

A high-risk status signals not only immediate danger but also the likelihood of repeated exploitation, making proactive mitigation critical.

14 The Cost of Bot-Driven Cybercrime

For SMBs, bots represent an existential threat and the consequences are immediate and far-reaching:

Website Disruptions: DDoS attacks overload servers, causing downtime and frustrating customers.

Data Theft: Bots scrape sensitive customer information, leading to breaches.

Revenue Loss: Slow website performance drives potential customers away.

Reputation Damage: A compromised website erodes trust and credibility.

Case In Point

Remember Kaila Uli and Brillies. Her story exemplifies the catastrophic impact of unchecked bot activity. Despite migrating her website, the relentless onslaught of bot-driven attacks continued and forced her to close her business. Her experience is a stark reminder of how bots can dismantle SMBs, highlighting the urgent need for proactive defenses.

Proactive Defense: Shielding SMBs from Bots

Combatting bots requires robust, proactive defenses:

Bot Management Tools: Leverage advanced tools like SiteLock's Web Application Firewall (WAF) to block malicious bots before they reach your website.

Keep Software Updated: Keep CMS, plugins, and themes updated to mitigate vulnerabilities.

Traffic Analysis: Regularly monitor website traffic for unusual patterns or spikes.

Rate Limiting: Restrict the number of requests from a single IP within a set timeframe.

CAPTCHA Implementation: Use CAPTCHA challenges to distinguish bots from human users.

By adopting these strategies, SMBs can safeguard their websites, ensuring seamless access for legitimate users while keeping bots at bay.

Spotting the Signs: Recognize Bot Attacks Early

Watch for:

1. **Sudden Traffic Spikes:** Unusual surges in website visitors, especially at odd hours.
2. **High Bounce Rates:** Visitors leaving after viewing only one page.
3. **Server Strain:** Slower website performance or frequent crashes.
4. **Abnormal User Behavior:** Rapid, repetitive actions like login attempts or form submissions.
5. **Unusual Geographical Traffic:** Visits from regions unrelated to your business.

Key Takeaway

The adoption of AI and automation is only accelerating, and bots will continue to grow in scale and sophistication. Malicious bots are no longer just an annoyance—they are a dominant force in the cyber threat landscape. For SMBs, the fight against bots is crucial for protecting data, maintaining performance, and ensuring business survival. By implementing modern defenses and leveraging tools like SiteLock's WAF, small businesses can reclaim their digital spaces and stay ahead in the battle.

16 Insights From The SiteLock Platform

As bots dominate the cyber threat landscape, another equally dangerous partnership emerges: malware and vulnerabilities. In the modern cyber threat landscape, malware and vulnerabilities are co-conspirators, amplifying each other's impact in ways that leave websites—and their owners—dangerously exposed.

Attackers no longer wait for weaknesses to emerge; they actively seek out and exploit vulnerabilities, evolving their methods with every breach. Malware infections are no longer just frequent; they are precise, persistent, and alarmingly difficult to detect

A Symbiotic Relationship

Malware and vulnerabilities thrive together, forming a self-reinforcing cycle of exploitation:

Vulnerabilities Provide Entry Points

Outdated plugins or misconfigured settings, act as open doorways , inviting malware to infiltrate and wreak havoc.

Malware Creates New Weaknesses:

Once inside, malware embeds itself, often generating additional vulnerabilities that attackers can exploit to escalate their foothold.

An Endless Loop

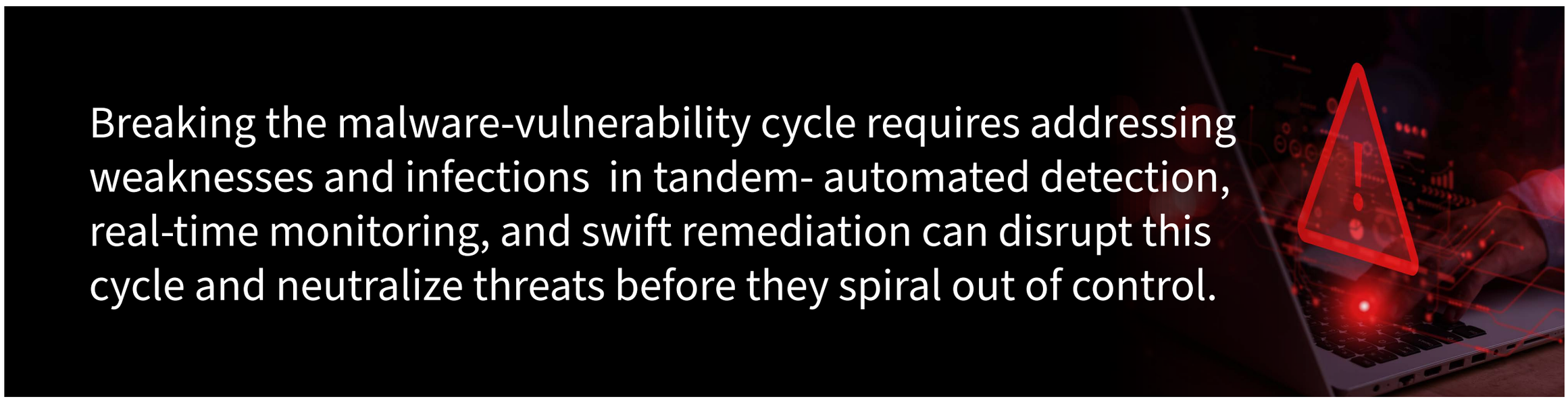
This cycle amplifies risk, complicates remediation, and leaves websites in a persistent state of exposure.

The Case for Swift Action

Breaking this cycle hinges on swift, decisive action. The longer vulnerabilities and malware remain unaddressed, the greater the risk of escalation. Attackers capitalize on delays, embedding deeper into systems and making recovery exponentially harder. By identifying and remediating threats early, website owners can significantly reduce their long-term impact, preventing minor breaches from escalating their foothold or exploiting additional vulnerabilities and snowballing into major crises.

THE MALWARE AND VULNERABILITY NEXUS

17



A Year of Escalating Threats

In 2023, the intersection of malware and vulnerabilities emerged as a critical concern for website security, with attackers leveraging both weaknesses in code and advanced malware to compromise digital assets.

Data from the SiteLock platform, which monitors and protects websites globally, offers unparalleled insights into these emerging trends. Millions of attempted attacks were recorded and mitigated, painting a vivid picture of the cyber threat landscape. The metrics from 2023 highlight the escalating volume of attacks, the growing complexity of malware, and the dynamic nature of vulnerabilities.

Here are the standout findings:

Rising Attack Frequency

DAILY ATTACK INCREASE

THE SITELOCK PLATFORM TRACKED AN ALARMING **24%** INCREASE IN DAILY ATTACK ATTEMPTS, REFLECTING THE RELENTLESS PERSISTENCE OF CYBERCRIMINALS TARGETING WEBSITES

ESCALATING THREATS

WEEKLY AVERAGE THREATS BLOCKED JUMPED BY **41%**, WITH **PER-SITE THREATS BLOCKED** SKYROCKETING BY **79%**, EMPHASIZING THE GROWING INTENSITY OF BOTH AUTOMATED AND **TARGETED ATTACKS**

Escalation of Critical Malware

FILE HACKER MALWARE

DETECTED IN **2/3** OF COMPROMISED SITES, A **68% INCREASE** FROM °˛°°, REMAINS THE MOST PREVALENT MALWARE ACROSS **MONITORED WEBSITES**

REDIRECT MALWARE

AFFECTING OVER HALF OF INFECTED WEBSITES SAW A WHOPPING **133%** INCREASE YEAR-OVER-YEAR, MARKING IT AS THE **FASTEST-GROWING THREAT**

THE MALWARE AND VULNERABILITY NEXUS

18

EVAL REQUESTS DETECTED

IN **39%** OF INFECTED SITES, GREW BY **73%,** TARGETING SERVER-SIDE VULNERABILITIES WITH STEALTH AND PRECISION

BACKDOORS PRESENT IN 46% OF INFECTED SITES (+17% YOY), AND SHELL SCRIPTS, **FOUND IN 32% (+33% YOY),** EXEMPLIFY THE PERSISTENT NATURE OF MODERN CYBERATTACKS REINFORCING THE CRITICAL **NEED FOR CONSTANT VIGILANCE**

Severity on the Rise

HIGH-SEVERITY MALWARE INFECTION RATES

MORE THAN DOUBLED, SURGING BY **107%,** AS SITELOCK MITIGATED INCREASINGLY **COMPLEX AND IMPACTFUL THREATS**

The Rise of Targeted Exploitation

WHILE SQLi VULNERABILITIES DECREASED BY 30%, THEIR INFECTION RATE INCREASED BY 6%.

SIMILARLY, CROSS-SITE SCRIPTING (XSS) VULNERABILITIES DROPPED BY 33%, BUT INFECTION RATES CLIMBED BY 12%.

The simultaneous decrease in vulnerabilities and rise in infection rates shows that attackers are shifting toward more targeted, strategic exploitation. The use of AI and automation allows cybercriminals to identify and exploit weak points more efficiently, maximizing their impact.

Positive Trends in Infection Rates and Cleanup

WEEKLY AVERAGES REVEALED AN
11% DECLINE IN INFECTED SITES
AND A 12% DROP IN INFECTED FILES,
DEMONSTRATING THE VALUE OF
PROACTIVE DEFENSES

SiteLock's automated SMART File Cleanup addressed 6% fewer files weekly, reflecting advancements in detecting and blocking threats before they caused harm.

Data in Context: Building Resilience

The dual narrative emerging from the SiteLock data highlights both the evolving tactics of cybercriminals and the advancements in defensive strategies.

On one hand, proactive defenses have successfully reduced infection rates and cleanup needs. On the other, cybercriminals are refining their tactics, leveraging fewer vulnerabilities with greater precision and impact. The decreasing volume but increasing exploitability of vulnerabilities highlights a shift toward maximizing damage with targeted, high-severity attacks. The reduction in cleanup requirements reflects the effectiveness of proactive detection measures, exemplified by tools like SiteLock that intercept threats early.

This underscores the critical need for adaptive, layered defenses. By leveraging proactive defenses like automated scanning, real-time remediation, and layered security measures, businesses can reduce their risk and ensure long-term digital resilience.

20 Key Malware Insights

A Snapshot of 2023's Malware Landscape: A Growing Arsenal of Threats

The trends reveal not only an increase in the frequency and sophistication of attacks but also underscore the diverse nature of the threats websites face. Here's a closer look at the top malware categories and their implications:

MALWARE TYPE	% OF INFECTIONS	YEAR-OVER-YEAR CHANGE
File Hacker	67%	+68%
Redirect	56%	+133%
Backdoor	46%	+17%
Shell Script	32%	+17%
Eval Request	39%	+73%
File Manager	15%	-4%
Defacement	15%	-9%
Phishing	10%	+35%
SEO Spam	4%	-28%

Dominant and Rapidly Growing Threats

These malware types saw substantial growth in prevalence, reflecting their effectiveness and attackers' growing reliance on them:

File Hacker (67%, +68%)

The most prevalent malware type, found in two-thirds of infected websites.

Impact

Alters or steals server files, often serving as the entry point in multi-stage attacks.

Interpretation

This sharp rise indicates attackers increasingly rely on File Hacker malware to manipulate server files, making it a top priority for remediation.

Redirect Malware (56%, +133%)

The fastest-growing threat of 2023, redirect malware saw explosive growth.

Impact

Diverts website traffic to malicious sites, damages SEO rankings, and erodes user trust.

Interpretation

The sharp increase highlights a shift toward user-focused exploits designed to disrupt operations and damage reputations.

Eval Requests (39%, +73%)

Embedded malicious code targeting server-side vulnerabilities surged significantly.

Impact

Compromises operations, evades detection, and opens pathways for more sophisticated attacks.

Interpretation

The rise in Eval Requests signals a trend toward stealthier and harder-to-detect server-side exploits.

Persistent Threats

Malware types designed for long-term control remained a critical concern in 2023:

Backdoors (46%, +17%)

A persistent issue, backdoors allow attackers to maintain unauthorized access and reinfect sites even after remediation.

Impact

Enables long-term control, repeated malware injections, and data theft.

Interpretation

The steady increase underscores the difficulty of eradicating threats that leverage backdoors for recurring attacks.

Shell Scripts (32%, +17%)

Versatile tools for executing unauthorized server commands, shell scripts continued to rise.

Impact

Facilitates server compromise, enabling attackers to execute malicious commands undetected.

Interpretation

Their growing presence highlights attackers' focus on server-side exploits to maintain control and execute operations.

Declining but Not Obsolete Threats

While these threats saw reduced prevalence, they still pose risks for specific attack scenarios:

File Manager Malware (15%, -4%) and SEO Spam (4%, -28%)

These threats saw declines due to improved detection mechanisms or shifts in attacker priorities.

Impact

File Manager malware enables unauthorized file access, while SEO spam targets search rankings to redirect traffic.

Interpretation

Although declining, their presence highlights the need for vigilance against targeted campaigns.

Defacement Malware (15%, -9%)

Slightly less common in 2023, this threat disrupts website appearance and credibility.

Impact

Primarily used for reputational harm and to undermine user trust.

Interpretation

Despite a decline, defacement malware remains a favored tactic for attackers seeking to cause visible damage.

Emerging and Targeted Tactics

Attackers are increasingly leveraging advanced tactics to target users directly.

Phishing Malware (10%, +35%)

A significant rise in phishing malware reflects attackers' success with exploiting user trust.

Impact

Delivers convincing, AI-generated attacks designed to harvest credentials or financial data.

Interpretation

This trend signals the rising sophistication of phishing campaigns, leveraging automation and AI for greater impact.

Malware's Multi-Layered Assault:

Critical Threats Putting Websites Under Siege

Malware rarely acts alone—it operates with multiple layers of infection, amplifying its destructive potential. In 2023, critical malware such as File Hacker, Redirect Malware, and Eval Requests dominated the cyber landscape, leaving websites under relentless siege.

A single breach often begins with file hacks compromising server files, progresses to backdoor installations that allow persistent unauthorized access, and culminates in redirect malware that diverts user traffic to malicious sites. This multi-pronged strategy demonstrates how cybercriminals deploy overlapping tactics to maximize damage and maintain long-term control over compromised websites.

The sharp rise in these critical threats reflects a dangerous evolution- Malware is no longer content with short-term disruption; it seeks to maintain persistent control and maximize impact.

24 Threat Severity: Understanding the Spectrum

Building on the earlier discussion, it's important to understand the different levels of malware severity to better protect against their combined effects.

Malware operates across varying levels of severity and its severity determines its role in a coordinated attack -from breaking into a system to taking long-term control. SiteLock classifies malware into four severity levels from low-severity nuisances like SEO spam to critical threats capable of crippling entire businesses. Lets explores the varying levels of malware severity.

	CHARACTERISTICS	EXAMPLE TYPES	°¸°″ TRENDS AND IMPLICA TIONS
THREAT LEVEL	Immediate action needed; disrupts business operations	File Hacker, Shell Scripts, Backdoors	**Small Group, Big Impact:** Critical malware may represent only a small fraction of vulnerabilities (3%), but they are disproportionately represented in high-impact infections These threats, such as File Hacker and Redirect Malware drove some of the largest infection increases in 2023.
	Targets sensitive data, user credentials, and trust.	Redirects, Phishing, Malware Injections	**Targeting Trust:** High-severity malware infection rates rose by 107%, with attackers leveraging the explosive growth of redirect malware (+133%) and the targeted sophistication of phishing campaigns.
	Exploits vulnerabilities to expand attack surface.	Cryptominers, Mailer Malware	**Gateway to Escalation:** These may seem less threatening on the surface, but they account for a substantial 55% of all vulnerabilities, making them the most prevalent category. Their widespread presence lays the groundwork for attackers to escalate their activities.
	Minimal impact but damages user experience.	SEO Spam, Defacement	**Fading but Not Gone:** Account for 31% of the threats and although declining in prevalence (-28% for SEO spam and -9% for defacement), it doesn't mean they can be ignored. These threats still degrade user trust and experience.

25 Why Every Threat Level Demands Attention

The severity spectrum isn't just about categorizing risks—it's a roadmap for prioritizing action. While critical threats demand immediate remediation, medium and high-severity vulnerabilities pose an equally insidious danger by serving as gateways for more destructive attacks. Medium and high-severity threats exploit smaller gaps leading to larger breaches when left unresolved. Addressing these threats proactively is key to breaking the escalation cycle.

Understanding Vulnerabilities: The Open Door for Attackers

Lastly, while malware often takes center stage in discussions of cybersecurity, vulnerabilities remain the root cause of most compromises.

Concentrated in CMS plugins, themes, and core applications, vulnerabilities act as the gateways that cybercriminals exploit to launch attacks. These weak points amplify the damage of every breach, making them critical to address.

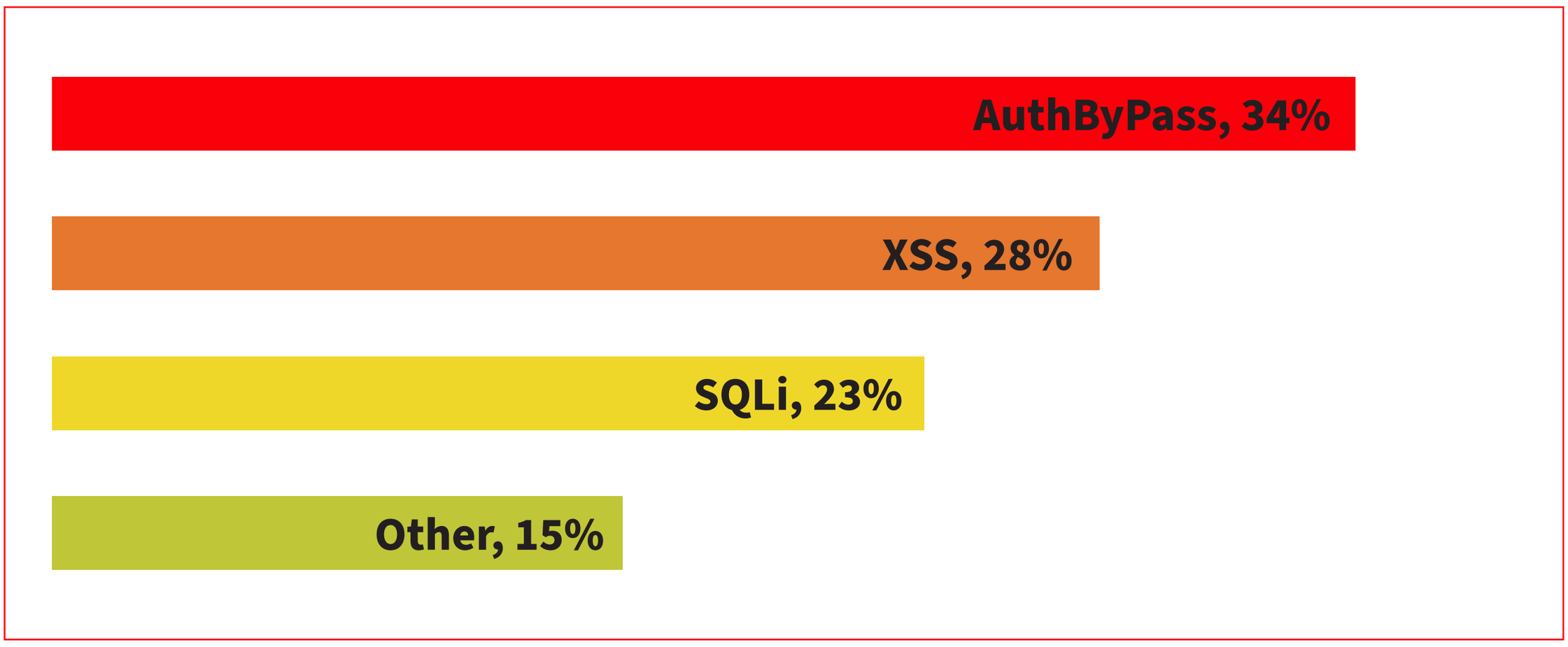
In 2023, the most common vulnerabilities included:

- **Authentication Bypass (AuthByPass):** Allowed attackers to bypass security mechanisms and gain unauthorized access.
- **SQL Injection (SQLi):** Enabled attackers to execute malicious SQL commands to access sensitive data.
- **Data Scraping:** Allowed the injection of malicious scripts to hijack user sessions or steal data.

The Distribution of Vulnerabilities

Plugins, themes, and core CMS applications accounted for the majority of vulnerabilities.

The **Vulnerabilities in Applications Distribution Chart** illustrates how these risks manifest across CMS plugins, themes, and core applications :



The Ripple Effect of Vulnerabilities

Every unpatched vulnerability leaves a website one step closer to compromise. Often concentrated in CMS plugins, themes, and core systems, vulnerabilities play a central role in enabling sophisticated cyber threats. Addressing these weak points is the first line of defense against malware and ensures a safer online presence.

Even a single vulnerability can have cascading consequences. Once exploited, vulnerabilities often pave the way for layered attacks, enabling more sophisticated threats like backdoors or redirect malware which amplify damage and make recovery harder.

Breaking the Cycle

Proactive management is critical. By regularly updating plugins, themes, and core systems, website owners can close critical gaps before they are exploited. This is especially crucial for CMS-based and custom websites, where vulnerabilities can vary widely based on configurations and usage. Closing these gaps early is not just about prevention—it's about breaking the cycle that enables increasingly sophisticated attacks.

Next Steps

With CMS and custom websites being frequent targets, understanding their unique vulnerabilities is crucial for building stronger defenses. The next section delves deeper into these risks and how they can be mitigated effectively.

CMS PLATFORMS: A POPULAR YET RISKY CHOICE

27

Content Management Systems (CMS) have revolutionized website development allowing anyone to quickly and easily create a fully functioning website. CMS platforms thrive on their modular nature, enabling website owners to customize and extend functionality through third party tools like plugins and themes that help enhance usability, visual appeal and overall performance. This flexibility and convenience have driven their incredible popularity, with CMS platforms now powering an estimated 67% of websites globally.

WordPress the dominant player in the space alone accounts for 63% of the CMS market, with over 810 million websites built on the platform. However, this widespread adoption paints a target on their back – the reliance on third party plugins and themes introduces vulnerabilities that cyber criminals are only too eager to exploit. With such a massive user base, CMS platforms present an attractive and expansive target for attackers, making security challenges inevitable.

According to SiteLock data, in 2023:

Joomla websites were **13x more vulnerable** than non-CMS websites

WordPress sites were **10x more vulnerable** than non-CMS websites

Drupal websites were **1.14x more vulnerable,** indicationg that even niche CMS platforms are not immune

28 Plugins: The Trojan Horse of CMS Websites

While plugins and themes are the cornerstone of CMS platforms, due to their unparalleled flexibility and functionality, yet this very advantage often conceals a significant flaw: security risks. These seemingly helpful tools can serve as Trojan Horses, introducing hidden vulnerabilities that attackers exploit to compromise websites.

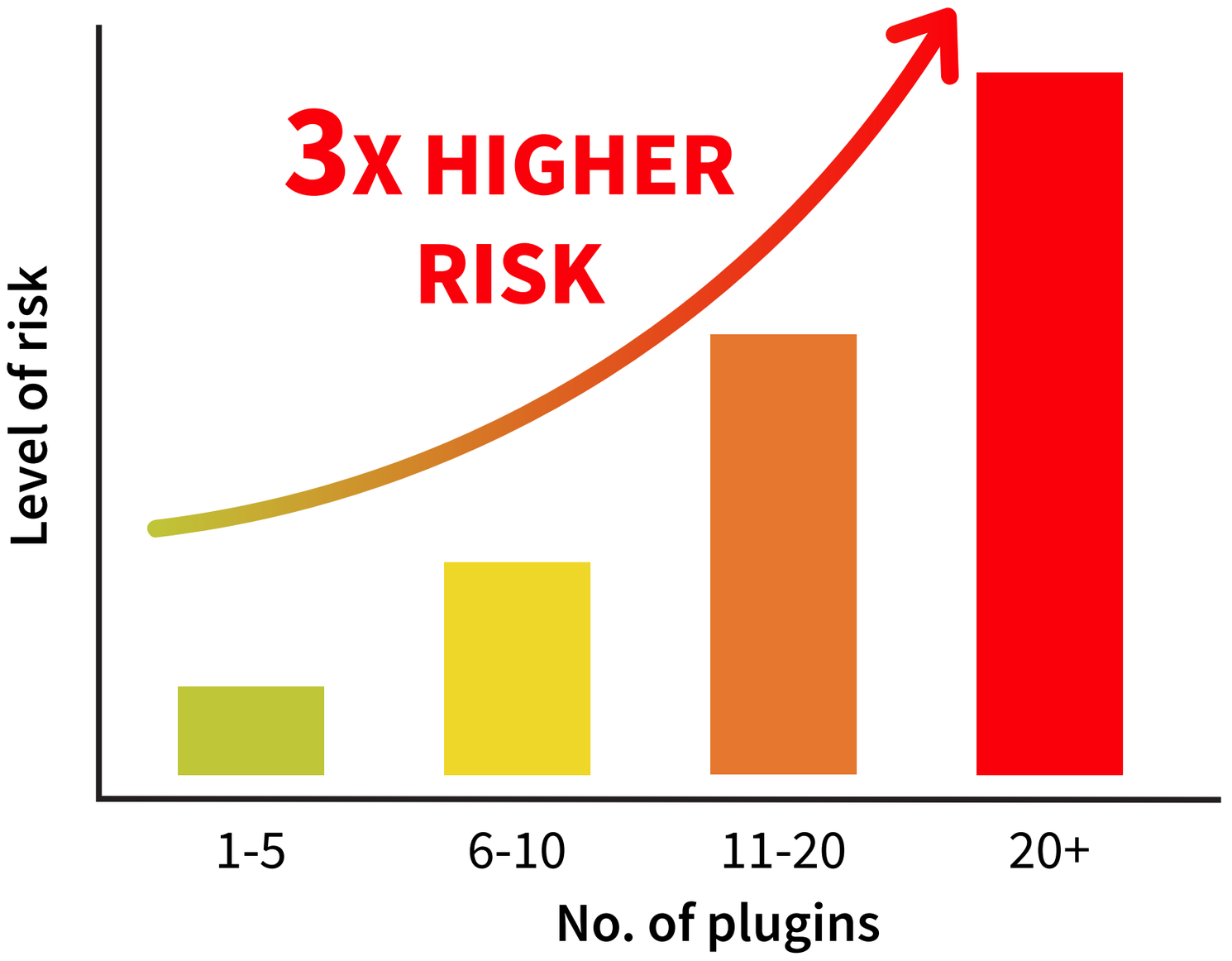
Plugin Vulnerabilities: Breaking Down the Risks

The risks associated with plugins are as varied as they are critical.

- **Outdated Plugins:** A leading cause of vulnerabilities, providing easy entry points for attackers.
- **Configuration Weaknesses:** Poorly configured plugins expose sensitive functions to exploitation.
- **Unmaintained Plugins:** Abandoned or unsupported plugins create persistent security gaps.

Breaking Down the Data on Plugins and Malware

Data from SiteLock highlights the relationship between plugin usage and infection risk:



- **1–5 Plugins:** Represent 67.8% of WordPress sites but account for 58.33% of infections, showing that even minimal setups require consistent maintenance.
- **6–10 Plugins:** Sites with this range face an infection rate 1.5x higher than those with 1–5 plugins.
- **11–20 Plugins:** Infection rates double, as managing more plugins increases the attack surface.
- **20+ Plugins:** These rare sites experience an infection rate nearly 3x higher than those with fewer plugins.

29

The Cost of Plugin Overload

Risk Grows with Plugin Count

The data shows a clear correlation: as plugin count increases, so does the likelihood of malware infection. This underscores the dangers of plugin overload, where unmaintained or outdated plugins create vulnerabilities that attackers exploit.

Exponential Risk for High Plugin Counts

Sites with 20+ plugins might be a smaller part of the overall WP population, but their 3x higher infection rate illustrates the compounded risk of maintaining too many plugins. Each additional plugin increases the attack surface, often overwhelming website owners' ability to manage and secure their installations.

False Sense of Security

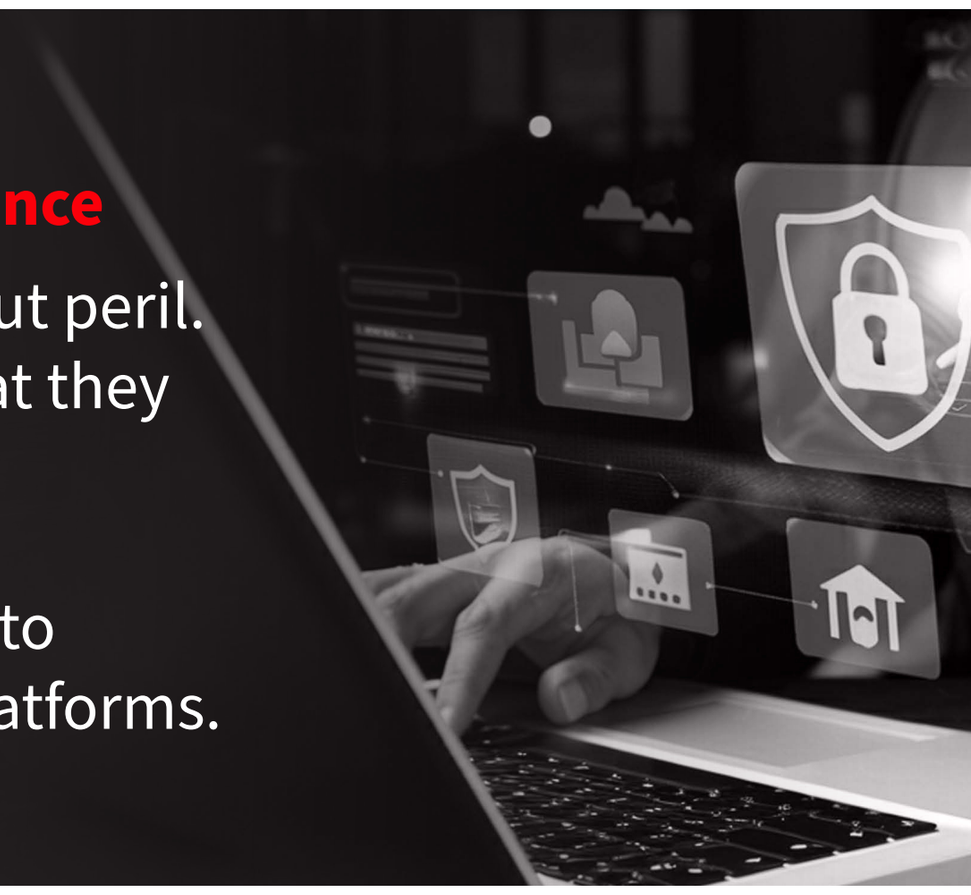
Sites with 1–5 plugins may seem secure, but the high infection rates among these sites highlights the importance of consistent maintenance, even for minimal setups.

Beyond Plugins

Even sites without plugins are not immune. Core systems, themes, and misconfigurations extend the metaphor of the Trojan horse—risks can originate internally, not just from external add-ons.

Functionality vs. Security—Striking the Right Balance

Plugins offer incredible utility, but they are not without peril. Like the original Trojan horse, their danger lies in what they bring within. By managing plugin usage carefully, maintaining updates, and leveraging robust security measures, website owners can keep the gates closed to malicious actors while reaping the benefits of CMS platforms.



30

Strengthening CMS Defenses

CMS-based websites, can reduce security risks by:

1. **Regular Updates:** Themes, and CMS core systems updated ensures that known vulnerabilities are patched promptly.

2. **Plugin Hygiene:** Limit the number of installed plugins, prioritizing quality and security over quantity.

3. **Use Trusted Plugins:** Vet plugins carefully for quality and security support.

4. **Audit and Remove:** Regularly review and remove unnecessary or outdated plugins to reduce potential attack surfaces.

5. **Monitor Website Health:** Employ automated tools, like SiteLock's SiteHealth and Prioritized Security Action Queue to detect and remediate threats in real-time.

6. **Backup Strategies:** Maintain regular backups to recover quickly in the event of an infection.

Key Takeaway

While CMS platforms offer unmatched flexibility, their popularity makes them a prime target for cyberattacks. Plugins, themes, and core vulnerabilities represent critical weak points. Proactive management and advanced security tools are essential to harness CMS capabilities without falling victim to their inherent risks.

CUSTOM WEBSITES: A GROWING TARGET

While CMS platforms often dominate the conversation, custom websites face their own unique set of challenges. **Infection rates** for custom websites **rose by 69% in 2023,** highlighting that attackers are diversifying their focus and and finding growing value in breaching them.

Why Are Custom Websites at Risk?

- **Weaker Update Cycles:** Custom sites often lack automated update mechanisms, leaving vulnerabilities unpatched and increasing exposure to malicious attacks.
- **Unregulated Third-Party Tools:** Custom websites often use custom libraries, third-party add-ons or integrations that lack the collective oversight, frequent updates and vulnerability awareness commonly seen in community-driven CMS projects making them a significant security risk.
- **Diverse Architectures:** Custom configurations create inconsistencies in security practices, making them harder to secure.

Lifecycle Security Practices for Custom Websites

Custom websites offer unparalleled flexibility and uniqueness, but these benefits come with a heightened security burden. To safeguard these sites robust lifecycle security is non-negotiable:

Regular Code Audits
Conduct frequent security reviews to identify and address vulnerabilities in custom code.

Third-Party Risk Management
Vet third-party plugins and libraries thoroughly before integration.

Standardize Updates
Establish and maintain a consistent schedule to apply updates and security patches.

Advanced Security Measures
Deploy advanced security tools like SiteLock's automated scanning and malware remediation to detect and neutralize hidden threats.

Comprehensive Backup Plans
Regularly back up website data to ensure quick recovery and minimize downtime in case of a breach or malware infection.

Proactive Defense in Action

In 2023, **SiteLock issued a monthly average of 41,402 alerts for High and Critical Severity vulnerabilities in web applications.** These alerts served as an essential early warning system, helping website owners—whether CMS-based or custom—to address potential risks before they could be exploited.

Key Takeaway

CMS and custom websites may differ in architecture, but attackers exploit both with increasing precision. The rise in vulnerabilities across plugins, themes, and bespoke configurations highlights the urgent need for proactive security measures and advanced monitoring tools, regardless of the platform

Aritficial Intelligence

In 2023, Artificial Intelligence (AI) transformed the cyber threat landscape, becoming both a weapon of choice for attackers and a vital defense mechanism for businesses. As AI tools become increasingly accessible, they have not only lowered the entry barriers for cybercriminals but also ignited a technological arms race, reshaping the way we think about and combat cyber threats.

Advanced Cybercrime in Everyone's Hands

AI has democratized cybercrime, empowering even non-technical actors to wield elite-level capabilities. What was once the domain of highly skilled hackers is now accessible to anyone with access to generative AI tools.

DIY Malware Kits

Imagine shopping for a hacking tool that requires no expertise in cybersecurity—fully developed, managed, updated, and ready to use. This is the reality of exploit kits. Exploit kits are sophisticated software tools designed to automatically identify and exploit vulnerabilities with minimal effort from the user. Exploit kits can be used to target vulnerabilities in CMS platforms, plugins, and website code, enabling attackers to execute attacks like injecting malicious scripts, redirecting traffic, or even installing backdoors.

Phishing Simplified

Say goodbye to poorly written scam emails. AI now generates flawless phishing emails, professional-grade landing pages, and convincing social engineering scripts, drastically boosting success rates.

Automation at Scale

Tasks like replying to phishing bait or executing brute-force attacks are automated, enabling attackers to amplify their campaigns without significant effort.

This "democratization of cybercrime" has led to an explosion in the volume and sophistication of attacks. Small-time hackers now have access to capabilities that rival even the most well-funded organizations.

34 The Rise of AI Arms Dealers

In the dark corners of the internet, a shadow industry has emerged—essentially an arms market for cybercriminals, equipping them with AI-driven tools that make their attacks more efficient, adaptable, and devastating.

- **Dynamic Malware Generation and Evolution:** AI enables criminals to generate malware variants rapidly, creating diverse attacks with similar core functionalities continuously evolving to evade the latest detection technologies. This overwhelms traditional detection systems, leaving defenders scrambling to keep up.

- **AI-as-a-Service:** The dark web has embraced the "as-a-Service" model, offering plug-and-play AI services that automate attacks, scan for vulnerabilities, and craft highly tailored phishing campaigns. Cybercriminal forums openly advertise RaaS packages, complete with downloadable features, bundled offers, and even 24/7 customer support. Prices range from $50 to $5000 depending on what you are looking to achieve.

- **Custom AI Models:** Attackers train AI systems on stolen data to target specific organizations or industries, creating tools that are highly personalized and harder to counter.

- **Exploit Development:** AI streamlines the process of identifying and exploiting vulnerabilities in target systems. Once weaknesses are discovered, AI crafts precise exploits and optimized attack sequences, turning potential gaps into guaranteed breaches.

- **Evasion Techniques:** : By analyzing malware against security software, AI learns detection mechanisms and modifies malware to bypass them, creating an ongoing cycle of stealth and adaptation.

This underground ecosystem has supercharged the scale and impact of cybercrime. As attackers gain access to increasingly powerful tools, defenders face an uphill battle to effectively combat and neutralize these advanced threats.

35 AI vs AI: When Offense Meets Defense

The battle between attackers and defenders has become a high-stakes game, with AI driving both offense and defense. Cybersecurity can no longer employ just a static line of defense of fortifying systems—it's now a fast-paced, ever-evolving chess match.

Attackers' AI

Scanning for vulnerabilities, mimicking human behavior, and rapidly adapting malware to bypass defenses.

Defenders' AI

Detects patterns, predicts attack vectors, and neutralizes threats in real time.

An Escalating Tug-of-War: This battle is a constantly evolving arms race, with attackers and defenders continuously upgrading their AI models to outsmart each other. The cycle of innovation is relentless where only those who adapt fastest can prevail

This dynamic has redefined cybersecurity as a test of speed, constant vigilance and cutting-edge solutions to stay ahead of attackers.

AI-Driven Threats in Action: Real-World Impacts

A recent survey from Nationwide revealed that **25% of small businesses** have already fallen victim to AI-generated scams, underscoring the growing scale and precision of AI-powered attacks.

Hyper-Realistic Impersonations

AI-generated deepfakes, both video and audio, make social engineering attacks nearly impossible to distinguish from legitimate communications.

Phishing 2.0

AI enables attackers to craft personalized campaigns that mimic trusted colleagues, suppliers, or clients, making scams even more convincing and dramatically increasing success rates.

Continuous Learning

Cybercriminals are using AI to backfeed data from failed attacks, improving their tools with every attempt and making future breaches more precise and harder to detect.

35 Securing the Future in a Complex Digital World

The findings of this report reveal a troubling picture. The digital landscape is no longer just a battleground of malware and vulnerabilities; it is now an intelligence war, where attackers leverage AI, automation, and precision tactics to exploit every weakness.

The Trends Shaping Security Strategies

- **AI-Powered Cybercrime on the Rise:** Attackers are leveraging AI and automation to launch faster, more sophisticated, and highly evasive cyber threats, making traditional defenses.
- **Vulnerabilities Continue to Serve as the Gateways for Infection:** Unpatched plugins, misconfigured settings, and outdated systems remain prime targets, allowing attackers to exploit weaknesses and perpetuate cycles of reinfection.
- **Bots-the workhorses of cybercrime:** Malicious bots now act as the backbone of modern cyber threats.
- **Proactive Security as a Necessity:** Whether on CMS platforms or custom websites, early detection and swift remediation of vulnerabilities are crucial to preventing long-term damage and disruption.

A new imperative: Pre-empt don’t just respond

The era of patching after an attack, mitigating only after damage occurs, and responding instead of anticipating is over. Organizations must transition from reactive security to predictive resilience—leveraging real-time intelligence, automation, and proactive defense mechanisms to stay ahead of threats rather than just contain them.

Cyber threats will not slow down, nor will they become less sophisticated. The key to long-term protection is not just stronger technology but a mindset shift—security must be continuous, adaptive, and deeply integrated into every digital touchpoint.

Businesses that treat security as an afterthought will remain vulnerable. But businesses that embed security into their operations, workflows, and digital strategy will not only survive but thrive in this new cyber era. Security is no longer just about defense—it is a core business enabler. The organizations that recognize this will position themselves for sustainable growth, trust, and resilience in an increasingly hostile digital environment.

35 A Security Manifesto: Guiding Principles for the Digital Age

Proactive Protection Over Reactive Responses:

- Utilize real-time monitoring, AI-driven threat intelligence, and automated remediation to stay ahead of attackers.
- Detect vulnerabilities before they can be exploited and take swift action to prevent cascading threats.

A Multi-Layered Approach to Defense

- Ensure continuous security assessments to adapt to emerging threats.
- Employ a multi-layered approach that combines tools like Web Application Firewalls (WAF), automated scanning, and robust backup systems to secure every layer of the digital stack.

Awareness and Educations as the First Line of Defense

- Simplify website security with guided fixes, actionable guidance, and automated workflows, empowering users to make informed decisions about their website's protection.
- Provide clear, actionable insights that help website owners and teams make informed security decisions.

Security is Shared Responsibility

- Promote best practices across the digital ecosystem, ensuring that security isn't just an afterthought but a foundational element of online operations.
- Strengthen website defenses through collaboration with hosting providers, developers, and technology partners.

Agility and Adaptability in an Evolving Threat Landscape

- Cyber threats evolve—so should security strategies. Ensure defenses are dynamic, continuously updated, and able to counter new attack vectors.
- Use smart scoring and prioritized security actions to guide remediation based on real-time threat levels.

AI-Driven Threat Prevention & Rapid Responses

- Leverage AI and machine learning to analyze patterns, detect anomalies, and automate threat mitigation.
- Prioritize security actions based on real-world risk, ensuring the most critical threats are addressed first.

SiteLock

A SECTIGO® COMPANY

GET IN TOUCH

sales@sitelock.com

(877) 846 6639

+1 (415) 390 2500 *(International)*