SITELOCK

2025

SiteLock Annual Website Security Report

The Quiet Compromise: How 2025 redefined website threats - broader reach, stealthier malware, deeper persistence.

Table of Contents

Letter from SiteLock 4

Excutive Summary 5

The Five Defining Findings of 2025

Methodology & Data Scope 8

The Big Trends Shaping Website Security 10

Three Years. Three Shifts: 2023–2025 in Context

2023: Automation Accelerated Attack Creation

2024–2025: Scale, Then Optimization

Threat Volume & Bot Activity 13

Threat Volume & Historical Arc

Bot Traffic: Bots Didn't Retreat. They Got Smarter.

Why Bot Activity Matters

Malware Landscape 16

Infection Rates & The Quiet Compromise Pattern

Dominant Malware Families: Three-Year Trends

Multi-Family Infections: A Continuing and Deepening Pattern

The Redirect Collapse

The Backdoor Economy 20

Three-Year Backdoor Surge

The Reinfection Cycle

Malware Severity 22

All Four Tiers Rising: A Three-Year Pattern

What the Severity Shift Means for Remediation

CMS Risks & Vulnerabilities 24

CMS vs. Non-CMS: A Widening, Multi-Year Gap

The Plugin Problem

Application Vulnerabilities: Auth Bypass Is #1

Vulnerability Severity Distribution

Platform Alerts 28

When Alerts Peak and Why It Matters

The Value of Timely Action

The Economics of Cybercrime 30

Cheap Tools, Expensive Consequences

The Reinfection Economy

Emerging Threats: What's Around the Corner? 31

Final Thoughts & Recommendations 33

Letter from SiteLock

The Web Has Changed. Again.

The web threat landscape didn't just grow in 2025 - it changed character.

For several years, cyberattacks against small and midsize business websites have been driven by two forces: scale and automation. Attackers built industrialized systems to probe millions of sites simultaneously, deploy malware at volume and monetize compromised infrastructure with the efficiency of a legitimate technology business. In 2024, that model matured. In 2025, it evolved.

The shift we observed across more than 20 million monitored websites is not a story of louder, more visible attacks. It is the opposite. In 2025, attackers became quieter. More patient. More deliberate. The defining pattern of the year was not a surge in malware volume - it was the systematic replacement of noisy, visible compromise with stealthy, persistent access.

More websites were infected. Fewer files were detected per site. Backdoor infections surged 44% year-over-year and are now present on 70% of all infected sites - up from 46% in 2023. Redirect malware - once the dominant monetization vector at 57% of infected sites in 2023 - has all but vanished, collapsing to just 3% in 2025. These are not independent data points. They tell a single, consistent story: attackers are no longer optimizing for quick payouts. They are optimizing for durable control.

We call this the Quiet Compromise.

A compromised site no longer looks broken. It may load perfectly, rank well and convert customers - while simultaneously serving as a control plane for attacker operations. Without continuous, deep scanning that goes beyond surface-level file analysis, these infections go undetected for weeks or months. And the multi-family infection pattern we first highlighted in 2024 has not abated - in 2025, the sum of malware family prevalence across infected sites reached 239%, the highest in three years, confirming that layered, multi-payload infections continue to be the norm.

This year's report is built on data from real attacks across a network analyzing 38.4 billion files monthly. It is designed for two audiences. For small and midsize business owners, it explains what these threat patterns mean for your website, your brand and your customers. For hosting providers, it shows why proactive, root-cause security is no longer an add-on. It is a platform-health strategy.

The core message is simple: security can no longer be measured by whether a site is online. It must be measured by whether the site is clean, whether the root cause of any compromise has been eliminated and whether the mechanisms that enable reinfection have been removed.

Martin Fiegl
Head of Threat R&D

Meenu Randhawa
Product Marketing Manager

Executive Summary

The 2025 SiteLock Annual Website Security Report is drawn from one of the web security industry's largest real-world datasets:

20+ million websites monitored globally, 38.4 billion files analyzed monthly and 52 weeks of continuous threat telemetry. What the data reveals is not simply an escalation of familiar patterns - it is a fundamental shift in how website compromise works.
Attacks became continuous rather than occasional. Malware became quieter rather than more visible. Persistence became more valuable than disruption. And compromised websites increasingly became operational infrastructure - not just infected assets.

20M+
Website monitored
↑ 35% from 15M in 2024

38B+
Files scanned monthly
↑ 39% year-over-year

70%
Infected sites carry a backdoor
2023: 45.6% > 2024: 48.9% > 2025: 70.3%

504M
Threats blocked/month
126M/week

1.5M
Infections cleaned/week
78.8M total in 2025

19%
Files cleaned/infected site
414 avg (2023: 511 | 2024: 513 | 2025: 414)

658
Attacks/site/day
↑ 16%
2023: 611 > 2024: 568 > 2025: 658

9x
Bot vs human traffic ratio
5,303 bot probes/site/week
↑ 8% - per-site volume rising

252%
Multi-family infection index
Sum of malware family %: 285% (2023) > 248% (2024) > 252% (2025)

28%
More sites infected/week
4,765 avg/week
2023: 3,563 > 2024: 3,736 > 2025: 4,765

The Five Defining Findings of 2025

Severity Is Concentrating Upward

Critical-severity infections(those granting full command-and-control access) rose 133% year-over-year, from 16.6% to 38.7% of infected sites. Low-severity infections (defacement, SEO spam) fell 20%. Attackers are skipping the scaffolding phase. When compromise happens, it increasingly means full control.

The Quiet Compromise

Critical-severity infections(those granting full command-and-control access) rose 133% year-over-year, from 16.6% to 38.7% of infected sites. Low-severity infections (defacement, SEO spam) fell 20%. Attackers are skipping the scaffolding phase. When compromise happens, it increasingly means full control.

The Backdoor Surge

Backdoor infections rose 43.6% year-over-year. In 2023, backdoors were present on 45.6% of infected sites. In 2024, 48.9%. In 2025, 70.3%. This is now the defining characteristic of a compromised site and the primary engine of the reinfection cycle.

The Redirect Collapse

Redirect malware fell 82.7% year-over-year - the sharpest single-category decline in the dataset. Attackers are abandoning noisy, easily-detected techniques in favour of silent persistence. The redirect collapse and the backdoor surge are two sides of the same strategic shift.

CMS Risk Is Structural and Widening

WordPress sites are 3.46× more likely to be infected than non-CMS sites. Drupal 4.03×. Joomla 2.28×. Non-CMS infection rates fell 17% year-over-year. The gap is not closing - it is widening. CMS risk is driven by plugin sprawl and inconsistent patching, not by the platforms themselves.

2025 Signal	Three-Year Trend	Why It Matters
658 attacks/site/day	611 (2023) > 568 (2024) > 658 (2025): Resumed climb after methodology year	Layered infections are the norm; single-payload cleanup is structurally insufficient
70.3% of infected sites have backdoors	45.6% > 48.9% > 70.3%: Gradual build then sharp surge	Backdoor is now the primary infection objective, not a side-effect of it
414 files cleaned/infected site	513 > 513 > 414: Third-year divergence from rising infection count	Smaller payloads, harder detection - basic scanners miss more of what matters
Multi-family infection index: ~252%	285% > 248% > 252%: Dropped in 2024 driven by redirect collapse, recovered in 2025	Layered infections are the norm; single-payload cleanup is structurally insufficient
Redirect malware: 3.3% of infected sites	56.9% > 18.9% > 3.3%: Near-complete three-year collapse	Attackers abandoned noisy monetization in favour of silent persistence
Critical severity: 38.7% of infected sites	11.0% > 16.6% > 38.7%: Third consecutive year of escalation	Full C&C compromise is rising sharply - threat severity concentrating at the top
CMS gap: WP 3.46× vs Non-CMS	WP: 1.65× > 3.27× > 3.46× (widening); Non-CMS ↓17%	Structural CMS risk is not self-correcting; gap between CMS and non-CMS is growing

Methodology & Data Scope

The data presented in this report is derived from more than 20 million active websites monitored through the SiteLock global threat detection platform between January and December 2025.

Data sources include automated website scanners, malware remediation logs, threat alerts triggered by SiteLock's vulnerability detection systems and real-time telemetry from the SiteLock customer network.

Key Scanning Methods

SMART Scanning (Secure Malware Alert & Removal Tool)

Automates the detection and cleanup of malware across website files and databases. The primary source for malware family, severity and infection rate data in this report.

Malware Scanner

Front-end scanning layer that identifies threats not present in the SMART file layer, including redirect malware, phishing files and defacement. Combined SMART + Malware Scanner data provides the broadest view of site-level infection rates.

Web Application Firewall (WAF) Telemetry

Real-time threat blocking and bot traffic data across the WAF-protected site network.

Vulnerability Detection

Application-level vulnerability identification across CMS platforms, plugins and themes.

2025 Data Scope

38.4B
Files scanned monthly
Via SMART multi-scan methods - ↑39% from 2024

1.5M
Infections cleaned/week
78.8M total in 2025

1.07M
High & critical alerts issued
89,224 alerts/month average

27,581
Avg WAF-protected sites
504M threats blocked/month

Methodology Notes

Threat Reporting

Threats blocked figures represent verified malicious activity captured through SiteLock's WAF telemetry, excluding ambiguous or low-confidence traffic patterns. Bot traffic ratios are based on bot and human visit fields in the WAF dataset and reflect the full monitored network, not only WAF-enrolled sites.

Malware Family Percentages

Malware family statistics are expressed as a proportion of SMART-infected sites - not all monitored sites. Because a single infected site can carry multiple malware families simultaneously, these percentages sum to well over 100% in aggregate. This is not a data error; it reflects the multi-family infection reality documented throughout this report.

Malware Severity Percentages

Severity figures (Critical, High, Medium, Low) are expressed as a proportion of sites with file or malware detections. As with malware families, these percentages can exceed 100% because a single site can carry infections across multiple severity tiers at the same time.

Adjustments in 2025 Methodology

Year-over-year comparisons: 2024 figures have been recalculated using consistent methodology where pipeline changes were made, to ensure valid trend comparisons. The 2025 vs 2024 comparisons in this report reflect like-for-like methodology.

Scope Limitation

This report focuses exclusively on data observable through SiteLock's scanning and protection infrastructure. It does not account for websites not enrolled in active scanning. Findings represent attack behavior observed across SiteLock-protected environments, not the entirety of the global web threat landscape.

The Big Trends Shaping Website Security

Three Years. Three Shifts.

The web threat landscape has undergone three measurably distinct phases in three years.

Understanding the arc connecting 2023, 2024 and 2025 is essential to understanding why the security priorities for website owners and hosting providers must shift in 2026.

2023

Automation Accelerated Attack Creation

The widespread adoption of publicly accessible AI tools dramatically lowered the barrier to entry for cybercrime. Attackers gained the ability to generate phishing campaigns at scale, automate vulnerability discovery and produce more convincing social engineering content. The economics of attack creation changed fundamentally: what previously required technical skill and time became accessible, fast and cheap. Attack volume per site reflected this - reaching 611 attacks per day, up from 491 in 2022.

Multi-family infections were already visible in the 2023 data, with the sum of malware family prevalence across infected sites reaching 220% - clear evidence that layered, multi-payload attacks were already the dominant infection pattern.

2024

Automation Industrialized Attack Scale

By 2024, attackers had operationalized automation at industrial scale. Bot traffic surged to 12.6× the volume of human traffic - a 28% year-over-year increase and the highest bot ratio recorded in the SiteLock dataset. Multi-family infections continued, with the family prevalence sum at 217%. Critical malware severity rose 51% year-over-year as attackers escalated beyond simple infections to persistent, control-oriented compromise.

The dominant pattern of 2024 was escalation - broader, more automated and more layered than anything seen previously. Attack volume dipped slightly in absolute terms to 568 attacks per day due to methodology refinements, but when recalculated on a consistent basis, the underlying pressure continued to intensify.

2025

Attackers Optimized Compromise

In 2025, the data reveals the third phase of this evolution. Attackers stopped simply scaling attacks. They began optimizing the quality of compromise - making it stealthier, more persistent and harder to fully eliminate. Every major data signal points in the same direction:

- More websites were infected (**+28% week-on-week**) while fewer files were compromised per site (**-19%**).
- Critical-severity malware reached **38.7%** of infected sites - up **133%** from 2024's 16.6% and up **252%** from 2023's 11.0%.
- Backdoors surged from 45.6% (2023) to 48.9% (2024) to **70.3%** (2025): Persistence became the primary infection objective.
- Redirect malware - the most visible monetization indicator - collapsed from 56.9% (2023) to 18.9% (2024) to **3.3%** (2025).
- Multi-family infection index reached **252%** in 2025, confirming layered infections deepened rather than abated.

Compromise Is No Longer an Event. It Is an Operational Condition.

Compromise is no longer simply an event. It is increasingly an operational condition. A website can appear clean - loading at full speed, ranking well, processing transactions - while simultaneously hosting a backdoor, serving phishing content to visitors, acting as a bot command-and-control relay, or providing resold access to multiple threat actors. The absence of visible symptoms is no longer reassurance. The defining challenge of 2025 is not stopping attacks. It is identifying and eliminating persistence before it becomes operational control.

This is the Quiet Compromise: broader reach, smaller traces, deeper footholds.

2025 vs. Traditional Attack Patterns

Traditional Attack Patterns	2025 Threat Patterns
Broad attack distribution	Targeted, optimized operational pressure
Large, visible malware payloads	Smaller, stealthy, low-footprint compromise
Single-family infections	Multi-family, layered infections (239% index)
Redirect & defacement for rapid monetization	Backdoor persistence for long-term infrastructure control
High file counts - easy to detect	Low file counts per site - harder to detect
Cleanup resolves the compromise	Cleanup without root-cause removal creates a reinfection countdown

For SMBs

The shift to the Quiet Compromise means visible symptoms - redirects, defacements, browser warnings - are no longer reliable indicators that your site is infected. The absence of obvious malware is not the same as a clean site.

Continuous, deep scanning that covers both files and the database is the only way to keep pace with this model.

For Hosting Providers

Proactive, layered scanning at the platform level breaks this cycle.

The optimisation shift means attackers are now more efficient at extracting value from every compromised site. Most infected sites carry multiple malware types simultaneously. Surface-level cleanup without root-cause removal generates the next support ticket.

For your infrastructure, this translates to more reinfection cycles, more persistent support burden and more complex remediation requirements.

Threat Volume & Bot Activity

658 **Attacks per site, per day in 2025**

↑ 16% from 568/day in 2024 - approximately one attack every two minutes, around the clock.

In 2025, SiteLock blocked an average of 126 million verified threats per week across its network of protected websites - equivalent to 504 million blocked threats per month. On a per-site basis, websites experienced 658 attacks per day, resuming the multi-year escalation after a 2024 methodology adjustment year.

Attack Volume: Eight-Year Historical Arc

Year	Avg Attacks/Site/Day	YoY Change	Context
2018	63	-	Pre-automation baseline
2019	94	↑ 49%	Early bot scaling
2020	82	↓ 13%	Pandemic disruption to attack patterns
2021	172	↑ 110%	Post-pandemic automation surge
2022	491	↑ 186%	Attack automation industrialization
2023	611	↑ 24%	AI-assisted tooling accelerates attack creation
2024	568	↓ 7%	Methodology recalibration - like-for-like shows continued increase
2025	658	↑ 16%	Optimization phase: more targeted, more persistent attacks

~126M

Avg threats blocked per week

Most blocked: exploit attempts, script injections, shell activity

4,579

Avg threats blocked per WAF site per week

↑ 15% year-over-year

Bots Didn't Retreat. They Got Smarter.

The 2025 bot-to-human ratio - 9 bot visits for every one human visit - declined from 13× in 2024. Read in isolation, this might appear to be an improvement. It is not.

The data tells a more nuanced story. Per-site bot probe volume actually rose from 4,914 per week in 2024 to 5,303 in 2025 - an 8% increase. The ratio shifted because human traffic grew as SiteLock's monitored network expanded 35%. The bots did not retreat. They became more selective. And the absolute bot visit count remained at 146 million per week across the network.

9×

Bot to human traffic ratio in 2025

Down from 12.6× in 2024 - but absolute probe volume per site ↑ 8%

5,303

Avg bot probes per site per week

One automated probe every 2 minutes - ↑ from 4,914 in 2024 and 4,257 in 2023

146M

Total Bot Visits / Week

Network-wide

733M

Avg Monthly Bot Visits

Bot Traffic Trend: 2019–2025

Year	Bot:Human Ratio	Per-Site Probes/Week	YoY Change in Ratio
2019	2.52×	N/A	Early bot scaling phase
2020	4.34×	N/A	Pandemic automation surge
2021	4.59×	N/A	↑ 6%
2022	7.07×	N/A	Attack automation industrialization
2023	9.86×	4,257	↑ 39%
2024	12.6×	4,914	Peak ratio year in dataset
2025	9.44×	5,303 ↑ 8%	↑ 25% in ratio - but per-site probe volume still rising

What the bot ratio decline actually means

A lower ratio does not mean fewer bots. It means human traffic grew faster than bot traffic due to SiteLock's expanded network coverage. The per-site probe volume rising 8% is the operationally relevant figure: each monitored website received more automated attack attempts in 2025 than in 2024.

Why Bot Activity Matters

Bot activity matters because it is the opening move in most infection chains. Automated systems operate continuously, scanning for:

- Outdated plugins, themes and CMS versions with known CVEs published in the last 24–48 hours.
- Exposed administrative endpoints and login panels susceptible to credential stuffing.
- Configuration weaknesses, abandoned staging environments and forgotten scripts.
- Forms and input fields susceptible to injection and upload attacks.

For SMBs, the practical consequence is that a vulnerable plugin will be found. The question is only whether it gets patched before it gets exploited. At 5,303 probes per site per week, that window is measured in hours.

The Bottom Line

Bot traffic is now a primary vector for initial access that leads to persistent compromise. Each website in the monitored network received more than 5,300 automated probes every week in 2025. Most were rejected. The ones that were not - the probes that found an unpatched plugin, an exposed admin path, a weak credential - are the ones that resulted in the 4,765 infections tracked per week. Real-time WAF-based pre-execution blocking is the only defense that operates at the speed automation demands.

For SMBs

Your website received approximately 5,303 automated probes last week - scanning for the same vulnerabilities exploited in the majority of SMB infections. Most were blocked. The ones that were not are the reason continuous scanning, fast patching and WAF protection are non-negotiable.

For Hosting Providers

Bot filtering at the network edge is protecting your customers whether they know it or not. At 126M threats blocked per week across the WAF network, platform-level pre-execution blocking is the only operationally viable defense at shared hosting scale. The per-site probe increase of 8% shows the pressure on your customer base is not easing.

Malware Landscape

Infection Rates and the Quiet Compromise Pattern.

In 2025, SiteLock observed the clearest expression yet of the trend first emerging in 2023:

The number of infected websites grew significantly while the average malware footprint per site shrank. This divergence defines the year.

4,765

Infected sites/week

2023: 3,563 | 2024: 3,736 | 2025: 4,765

414

Avg files cleaned/site

2023: 511 | 2024: 513 | 2025: 414 (↓19%)

1.5M

Files cleaned per week

78.8M total cleaned in 2025

The divergence is consistent and confirmed by three years of data. In 2023 and 2024, files cleaned per site held steady at approximately 511 - 513 per week per infected site. In 2025, that figure dropped 19% to 414 -even as the number of infected sites grew 28%. This is not random variation. Attackers are deploying smaller, lower-noise payloads that do more operational damage with less detectable surface area.

Key Takeaway

More infections, fewer files per infection. Attackers are deploying smaller payloads that achieve the same or greater operational impact - persistent access, C&C capability, reinfection mechanisms - with less detectable evidence. Basic file scanners that flag large infection clusters will miss an increasing share of what matters. Depth of scanning is no longer optional - it is the primary differentiator between detection and dwell.

Dominant Malware Families: Three-Year Trends

The malware family data below shows the percentage of SMART-infected sites carrying each type - quarterly average for each year. Because a single infected site typically carries multiple malware types simultaneously, these percentages sum to well over 100%. This multi-family reality is addressed in the following section.

Malware Type	2023	2024	2025	3-Yr Trend	Role in Attack Chain
Filehacker	67.0%	72.2%	71.5%	— Stable at ~70%	Primary file manipulation - overwrites core files, enables payload delivery
Backdoor	45.6%	48.9%	**70.3%**	↑ **54% over 3 yrs**	Persistence mechanism - survives cleanup, enables reinfection, can be resold
Eval Request	39.3%	37.0%	34.4%	↓ Steady decline	Remote execution - fetches and runs malicious content dynamically
FileManager	15.4%	17.3%	23.2%	↑ Rising 3 yrs	Admin control - upload, edit, delete capability; enables ongoing file control
Shell Script	32.4%	24.7%	22.7%	↓ Steady decline	Server-level command access - hidden inside image or config files
Malicious JS	17.1%	12.1%	12.4%	— Stabilizing	Client-side attacks - targets visitors through injected scripts
Phishing	3.6%	4.7%	4.3%	— Stable	Credential/data harvesting targeting site visitors
Redirect	**56.9%**	**18.9%**	3.3%	↓ **94% over 3 yrs**	Near-extinction - visible monetization abandoned for stealthy persistence
Defacement	N/A	12.2%	10.5%	↓ Declining	Reputation damage - declining as stealth-first strategies dominate
SEO Spam	4.2%	4.8%	4.7%	— Stable	Link injection for search rank manipulation

Two trends define the 2025 malware family picture and they are two sides of the same coin. Backdoor prevalence reached 70.3% - up 44% in a single year and up 54% across three years. Simultaneously, redirect malware - once present on 57% of infected sites in 2023 - has effectively vanished, present on just 3.3% of infected sites in 2025. Both reflect the same strategic shift: attackers are moving from visible, quick-monetization techniques to silent, durable access mechanisms.

Multi-Family Infections: A Continuing and Deepening Pattern

In 2024, SiteLock first documented the widespread prevalence of multi-family infections. Compromised websites carrying multiple distinct malware types simultaneously. In 2025, this pattern not only continues, it remains a defining characteristic of modern website compromise.

Year	Multi-Family Index (sum of family %)	What It Confirms
2023	~285%	Multi-family infections already the dominant pattern; Redirect malware at 56.9% was a major contributor
2024	~248%	Index fell as redirect collapsed 38 percentage points not fewer layers
2025	~252%	Redirect near-zero, backdoor now near-equal to filehacker

The multi-family index tells a story that numbers alone can obscure. The drop from 285% in 2023 to 248% in 2024 was not evidence of simpler infections. It was almost entirely a redirect artefact. Redirect malware fell from 56.9% to 18.9%, shedding 38 percentage points from the index, while every other major family held steady or grew. Strip out redirect and the underlying layering barely moved.

In 2025, the index recovered to approximately 252% -effectively the same level as 2024. The backdoor surge added back roughly what redirect lost: backdoor grew 21 percentage points while redirect shed another 16. Across all three years, the degree of infection layering has remained structurally consistent. What changed is not how many families are present on a compromised site -it is which ones.

That compositional shift is the real story. Three years ago, a typical infected site carried filehacker, redirect and a backdoor. Today it carries filehacker, backdoor and FileManager. Backdoor's rise to 70.3%,combined with a filehacker rate that held near 70%, means a typical infected site in 2025 is almost certain to carry at least two high-capability malware families simultaneously. Both are operationally dangerous. Neither is visible to a casual observer or a basic file scanner.

The net result is a multi-family picture that has remained structurally consistent across three years, even as its composition shifted fundamentally from a landscape anchored by a visible, noisy monetization payload to one dominated by silent, persistent access mechanisms.

What multi-family infections mean for cleanup

If a website carries three malware families simultaneously as the majority of infected sites now do, cleanup that removes two and misses one leaves an attacker with a functional foothold. The missed component can regenerate the others. Root-cause remediation that scans for and removes all malware types across both files and the database is the only approach that breaks this pattern.

The Redirect Collapse: Three Years in Context

No trend in the 2025 data is more dramatic than the near-extinction of redirect malware - and few trends are more revealing about the direction of attacker strategy.

Year	Redirect Malware: % of Infected Sites	YoY Change	Context
2023	57%	↑ 133%	Second largest malware family -major monetization vector at its peak
2024	19%	↓ 67%	Significant decline as stealth-first approaches gain
2025	3%	↓ 83%	Near-complete collapse - visible monetization abandoned

Redirect malware is visible. It triggers immediate customer complaints, search engine warnings and hosting abuse reports. It generates cleanup requests quickly. It is, from an attacker's perspective, operationally noisy.

What the three-year arc reveals is that redirect actually peaked in 2023 surging 133% from 2022 as attackers scaled traffic monetization before the strategic reversal began. The rapid ascent and near-total collapse within three years is not a gradual trend. It is a deliberate pivot. The systematic abandonment of redirect malware replaced by silent, persistent backdoors and file manager tools is the clearest single signal that the attacker community has made a strategic choice: durable access is worth more than quick monetization.

For SMBs

Today's infected site rarely looks infected. The absence of browser redirects, defacements or spam does not mean your site is clean. Backdoors and eval-request scripts operate silently - below what any human observer or basic scanner notices. Continuous, deep automated scanning is the only reliable detection method.

For Hosting Providers

The collapse of redirect malware removes one of the most reliable customer-reported infection signals. More infected sites in your customer base will go undetected because the obvious symptoms are gone. Platform-level scanning that actively looks for backdoors, FileManager installations and persistent access mechanisms - not just visible payloads - is what now makes the difference.

The Backdoor Economy

70% **of all infected websites carried a backdoor in 2025**

Up from 49% in 2024 and 46% in 2023 - a 44% single-year surge and a 54% rise across three years

Backdoors are not simply persistence mechanisms. They are infrastructure. Once installed, a backdoor transforms a compromised website from a one-time victim into a durable, attacker-controlled asset that can be reused, repurposed and resold.

The three-year trajectory makes the shift unmistakable: 46% in 2023, 49% in 2024, 70.3% in 2025. Backdoor installation has become the primary objective of modern website compromise - not a side effect of it. The 2024 report noted backdoors as a rising concern. The 2025 data shows they have become the defining characteristic of an infected site.

What a Backdoor Actually Does

A web backdoor is code - planted in files, databases or both - that creates a persistent, hidden access point into a compromised website. Unlike visible malware, a backdoor sits dormant until activated by the attacker. It provides:

- **Persistent re-entry:** Survives password resets, plugin updates and surface-level cleanup that does not address root cause
- **Remote command execution:** Allows the attacker to run arbitrary server-side code on demand - even months after initial compromise
- **Database persistence:** Backdoors planted in the database rather than the filesystem are invisible to file-only scanning tools
- **Resale value:** Dark web markets allow compromised site access to be sold, meaning multiple threat actors can monetize the same site simultaneously and independently

The Reinfection Cycle

The backdoor is the engine of the reinfection economy that creates recurring costs for hosting providers and recurring frustration for website owners. Every incomplete cleanup - one that removes visible malware but leaves a backdoor intact - simply resets the infection clock.

Key Takeaway

More infections, fewer files per infection. Attackers are deploying smaller payloads that achieve the same or greater operational impact - persistent access, C&C capability, reinfection mechanisms - with less detectable evidence. Basic file scanners that flag large infection clusters will miss an increasing share of what matters. Depth of scanning is no longer optional - it is the primary differentiator between detection and dwell.

The Reinfection Chain

1. Attacker gains access via vulnerable plugin, weak credential or exposed endpoint
2. Backdoor is planted - in files AND the database
3. Surface-level malware is deployed (redirect, spam, phishing page)
4. Customer or scan tool removes visible malware - site appears clean
5. Backdoor survives - attacker returns, or sells access to another actor
6. Reinfection occurs - new support ticket, repeat cleanup, customer frustration
7. Cycle repeats until root cause - including the backdoor - is fully removed

For SMBs

Today's infected site rarely looks infected. The absence of browser redirects, defacements or spam does not mean your site is clean. Backdoors and eval-request scripts operate silently - below what any human observer or basic scanner notices. Continuous, deep automated scanning is the only reliable detection method.

For Hosting Providers

The collapse of redirect malware removes one of the most reliable customer-reported infection signals. More infected sites in your customer base will go undetected because the obvious symptoms are gone. Platform-level scanning that actively looks for backdoors, FileManager installations and persistent access mechanisms - not just visible payloads - is what now makes the difference.

Malware Severity

SiteLock classifies malware into four tiers based on behavior and potential business impact.

In 2025, the data shows something that demands attention: all four severity tiers rose significantly in prevalence across infected sites - for the third consecutive year. The pattern is not a spike. It is a sustained, multi-year escalation.

Severity Tier	What It Includes	2023	2024	2025	3-Yr Change
Critical (Command & Control)	Shell scripts, filehackers, file managers - grants full attacker control	11.0%	16.6%	**38.7%**	↑ **252%**
High	Redirects, phishing, downloaders targeting visitors	42.6%	33.2%	62.5%	↑ **88% from 2024**
Medium	Obfuscated scripts, cryptominers, mailers	16.5%	38.9%	71.0%	↑ **330%**
Low	SEO spam, link injections, comment spam	15.4%	34.7%	52.5%	↑ **241%**

Note: Percentages represent the share of infected sites carrying at least one instance of each severity level. As with malware families, these figures can and do exceed 100% in aggregate because a single site can carry infections across multiple severity tiers simultaneously.

Critical severity infections - which grant full command-and-control access - rose 133% in a single year and 252% across three years.

The 2024 report noted critical severity at 17% as a concern. In 2025, it stands at 39%. This is the most alarming single severity trend in the dataset: **Nearly four in ten infected sites now carry malware that gives an attacker complete control of the server.**

The broad rise across all severity tiers reflects the same multi-family infection dynamic. A site infected in 2025 is increasingly likely to carry low-severity SEO spam and high-severity phishing and critical-severity backdoor components simultaneously. Severity should guide remediation urgency - but the presence of low-severity malware cannot be used as a signal that the infection is limited in scope.

What the Severity Shift Means for Remediation

The severity escalation changes how infections must be approached. In earlier years, a low-severity SEO spam detection could reasonably be treated as a minor hygiene issue. In 2025, the same infection is statistically likely to co-exist with critical C&C malware. Treating severity tiers as mutually exclusive - cleaning the spam without investigating for backdoors - is an increasingly costly assumption.

Key Takeaway

Attackers are starting quiet and finishing loud - or more precisely, they are embedding multiple severity tiers simultaneously. Low-severity malware is often the opening foothold or the SEO spam layer sitting on top of a critical C&C infection. Catching a low-severity alert and remediating comprehensively is how you stop an escalation. Ignoring it because it looks minor is how you arrive at a critical compromise.

For SMBs

Critical-severity malware gives attackers full command-and-control of your server. This is beyond data theft - it means your infrastructure can be weaponized for spam, phishing distribution, DDoS participation and malware delivery to your visitors. Any critical-severity alert requires immediate, comprehensive remediation.

For Hosting Providers

Critical C&C infections at 39% of infected sites are the primary source of abuse complaints, email blacklisting and shared IP reputation damage. The 133% single-year rise directly increases your infrastructure risk surface. WAF-level pre-execution blocking prevents the initial compromise that enables critical-tier infections from establishing.

CMS Risks & Vulnerabilities

Content Management Systems power the majority of SMB websites.

The plugin-driven flexibility that makes CMS platforms accessible also creates an attack surface that grows with every component added and requires active maintenance to remain secure. In 2025, the CMS risk picture continued a multi-year pattern: structural vulnerability exposure remained elevated across all major platforms, while non-CMS site infection rates improved.

CMS vs. Non-CMS: A Widening, Multi-Year Gap

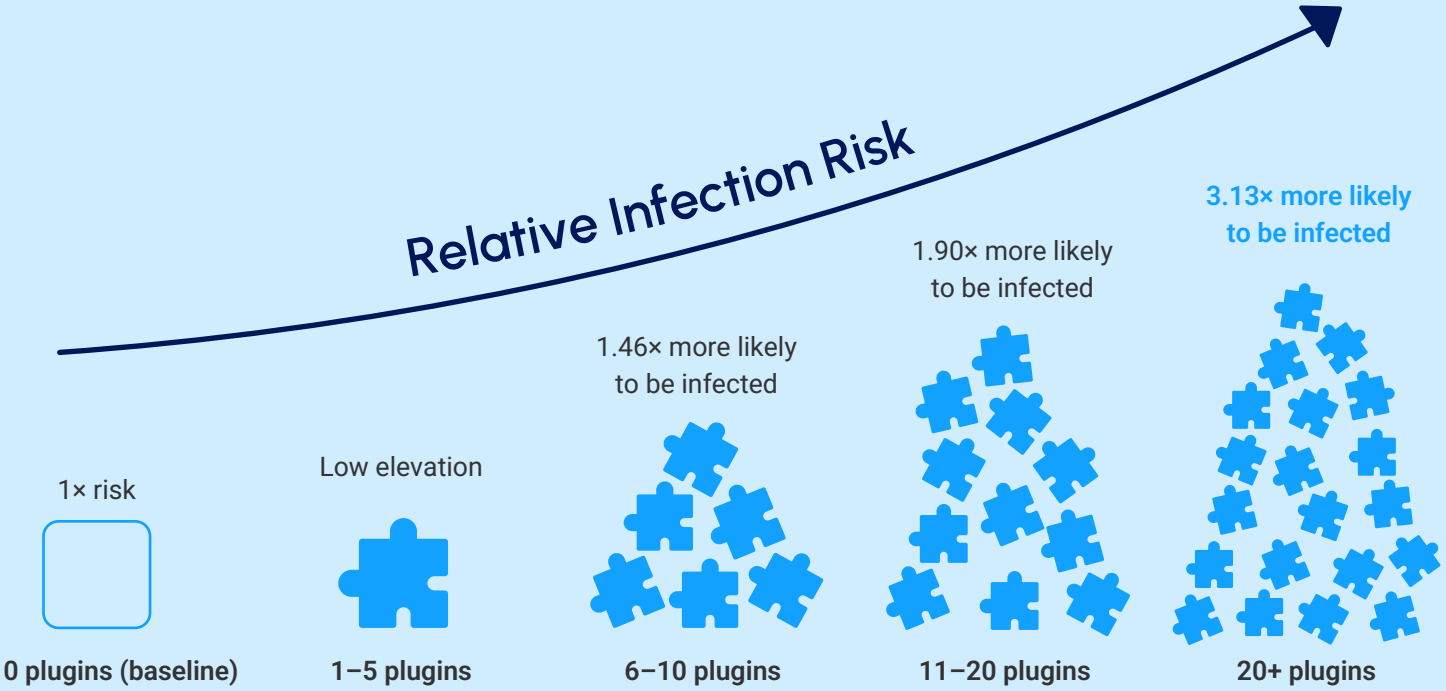
Platform	2023 (vs Non-CMS)	2024 (vs Non-CMS)	2025 (vs Non-CMS)	3-Yr Trend
WordPress	1.65×	3.27×	3.46×	↑ Gap widening
Drupal	2.20×	3.88×	4.03×	↑ Gap widening
Joomla	1.10×	1.80×	2.28×	↑ Fastest growth
Non-CMS	Baseline	Baseline	↓ 17% YoY	Improving - gap vs CMS widening

The non-CMS improvement - a 17% year-over-year decline in infection rate - is particularly telling. Custom-coded sites, typically maintained by developers with more consistent patching discipline and fewer third-party dependencies, are demonstrably getting safer. CMS sites are not improving at the same rate. This is a structural gap driven by plugin ecosystem complexity and the three-year data shows it is widening, not closing.

WordPress represents 18.2% of all monitored sites with an average of 24,300 infected sites per week. The core update rate is high at 85.6%, but as the 2024 report identified, core updates alone are insufficient. The risk resides in the plugin and theme ecosystem, a finding that Patchstack's 2025 data confirms: 91% of new WordPress ecosystem vulnerabilities were found in plugins, with just 9% in themes and 6 in WordPress core.

The Plugin Problem: A Multi-Year Recurring Weakness

Plugins are the primary attack surface on CMS platforms, a finding consistent across all three years of SiteLock data. The more plugins a site runs - especially unmaintained or outdated ones - the higher its infection risk. The 2025 data confirms these multipliers are unchanged from 2024, holding steady while the absolute infection rate environment worsened:



Every unused plugin is an open door. A deactivated but not deleted plugin still contains code that can be exploited. The 20+ plugin risk multiplier rising 5% to 3.13× in 2025 while the underlying environment worsened means high-plugin-count sites are moving into increasingly dangerous territory. Patchstack reported the median time to first exploit for heavily targeted WordPress vulnerabilities at just 5 hours in 2025 - the patching window is not measured in days.

Application Vulnerabilities: Auth Bypass Is #1

Beyond the malware and CMS picture, SiteLock also captures application-level vulnerability distributions across the monitored network. In 2025, authentication bypass vulnerabilities are the dominant type - larger than SQL injection and cross-site scripting combined.

Vulnerability Type	% of Total	What It Enables
Auth Bypass	33.3%	Unauthorized access to admin areas - attackers bypass authentication entirely
SQL Injection (SQLi)	21.1%	Database extraction, credential theft, content manipulation
Cross-Site Scripting (XSS)	21.1%	Session hijacking, script injection into visitor browsers
CSRF	8.1%	Unauthorized actions executed on behalf of authenticated users
Unrestricted Upload	7.5%	Malicious file upload enabling remote code execution
Redirect	4.4%	Open redirect enabling phishing and traffic hijacking
Multi-vector	2.8%	Combined attack surfaces
Other	~15%	RFI, LFI, XXE, DoS and other types

Authentication bypass at 33.3% is larger than SQLi and XSS combined. This is significant because auth bypass directly enables unauthorized administrative access without requiring credential compromise or a complex exploit chain. Auth bypass vulnerabilities are predominantly found in plugins - the same plugin ecosystem that the CMS infection data identifies as the primary risk surface. Keeping plugins updated is the direct mitigation.

Vulnerability Severity Distribution

Vulnerability Severity	% of Total	What It Enables
Critical	2.7%	Q4 spike: 25.1M (vs Q1: 13.9M)
High	10.5%	Q4 spike: 103.3M
Medium	68.3%	Dominant share all year
Low	18.5%	Q1 elevated at 124M

Medium-severity vulnerabilities dominate at 68% reflecting the volume of known, catalogued issues across widely-deployed plugins and themes.

For SMBs

If you are running WooCommerce, you are handling payment data on one of the most targeted platforms on the web. Every unused plugin is an attack surface and auth bypass, the most prevalent vulnerability in the dataset, means an attacker can gain admin access without ever needing your password. Audit your plugin stack quarterly, remove everything inactive, and treat high-severity vulnerability alerts as business-critical action items, not notifications.

For Hosting Providers

Non-CMS sites are improving while CMS risk grows and the gap widens. On shared hosting, an auth bypass exploit in a widely-deployed plugin can affect thousands of customer sites simultaneously making platform-level vulnerability alerting before exploitation the most operationally efficient response available to you. CMS-specific alerting, automated plugin update assistance and targeted outreach to customers running 20+ plugins are the highest-value interventions in your security portfolio.

Platform Alerts

Early Warning at Scale

1.07M

High & critical alerts in 2025

↓ 3.5% from 2024 - but ↑ 115% from 2023

+313%

Paid-tier alert growth since 2023

2,886/month (2023) > 11,921/month (2025)

In 2025, SiteLock issued an average of 89,224 per month. Every one of these alerts represents a specific, actionable signal: a high or critical severity vulnerability detected on a monitored website, sent to the site owner before it becomes an active infection.

The Value of Timely Action

Alert volume matters only insofar as alerts are acted on. In 2025, AI-assisted vulnerability discovery tools have compressed the exploitation timeline to hours for popular plugins with large install bases. An alert acted on within 24 hours dramatically reduces infection risk. An alert that sits unaddressed for 72 hours or more faces exponentially higher exploit probability.

When Alerts Peak and Why It Matters

The 2025 monthly data reveals a consistent seasonal pattern that has direct implications for how website owners and hosting providers should prioritise their security attention.

Period	Pattern	What Drives It
May–July	Peak alert volume (105K–110K/month)	Summer CVE disclosure cycle - plugin vendors and security researchers publish significant volumes of new vulnerabilities
August–September	Moderate decline	Post-peak, patching activity catches up
October	Secondary spike (paid scan alerts particularly elevated)	Pre-holiday plugin update cycle; new CVEs ahead of high-traffic ecommerce period
November–December	Significant drop	Reduced scan activity and disclosure volume

The May–July peak is not a coincidence. It aligns with the period in which the largest volume of WordPress plugin CVEs are typically published annually. For website owners running WooCommerce or high-traffic sites, this is the highest-risk window of the year - and the period when acting on alerts within 24 hours matters most.

Key Takeaway

AI-assisted vulnerability discovery is compressing the time between a CVE being published and the first automated exploit attempt. In 2025, this window is measured in hours for high-profile vulnerabilities not days. An alert acted on within 24 hours dramatically reduces infection risk. An alert left unresolved for 72 hours faces exponentially higher exposure as automated scanners probe continuously.

For SMBs

High and critical alerts are action prompts, not notifications. When a high or critical alert lands in your inbox, the vulnerability it's flagging is already being tested by automated scanners Assign ownership, track completion and treat them with the same urgency as a payment system outage. The window between a CVE publication and the first automated exploit attempt can be as short as five hours.

For Hosting Providers

The platform surfaces the alerts - your role is ensuring your customers are enrolled, receiving them and equipped to act. The May–July window is the highest-risk period of the year -the point at which CVE disclosure volume peaks and the exploitation window is shortest. Providers with broad customer enrolment going into that window see fewer infections, fewer support tickets and less churn than those relying on customers to self-select into protection.

The Economics of Cybercrime

Cheap Tools, Expensive Consequences

Cybercrime has become disturbingly efficient.

Attackers launch high-impact campaigns using low-cost, widely available toolkits that often require no technical skill to deploy. The return on investment for attackers is enormous and asymmetric.

Attacker Economics	SMB Victim Economics
Malware kits & exploit frameworks: $20–$100	Avg website malware attack cost: $5,000–$20,000
Infostealer-as-a-Service: As low as $12/month	Breach response cost: $120,000–$1.24M per incident
Backdoor reinfection: Near $0 - access already exists	1 in 3 affected businesses incur fines significant enough to damage their financial health
AI-powered phishing kit: Deployable in minutes	SEO recovery after blacklisting: Weeks to months
Failed attack cost: Negligible - automation absorbs failure	Incomplete cleanup: Full cost repeated on next reinfection

The after-effects of a cyberattack go well beyond the initial cleanup. According to the Hiscox Cyber Readiness Report 2025, one in three affected businesses incurred fines significant enough to damage their financial health. Many also reported lower business performance (30%), higher customer notification costs (29%) and greater difficulty attracting new clients (29%). For SMBs, these are not recoverable line items — they are existential risks.

For hosting providers, the economics of incomplete remediation are equally direct. Each compromised site that is not fully cleaned generates a predictable cost chain: support ticket, cleanup, reinfection, second ticket, abuse complaint, potential IP reputation impact and ultimately churn. The customer who has been infected three times in a year does not blame their plugins. They blame their host.

The Bottom Line

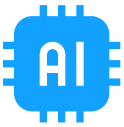
Cybercrime is a numbers game and the odds favor attackers who can automate failure. An attacker only needs one campaign to succeed in thousands to profit. An SMB has to successfully defend every attack. The economics are unforgiving in one direction — prevention costs a fraction of remediation, and incomplete remediation simply defers the full cost to the next reinfection.
Proactive investment - scanning, alerting, WAF protection, root-cause remediation - is not an expense. It is the lowest-cost way to avoid a far larger one.

Emerging Threats

What's Around the Corner?

The threat landscape continues to evolve faster than traditional defenses adapt.

Three emerging patterns from 2025 will define the operating environment for website owners and hosting providers in 2026.

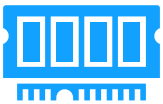


AI in the Attack Chain

Artificial intelligence is now embedded across the modern attack lifecycle - not as a theoretical capability but as standard operational tooling:

- **Vulnerability discovery:** AI-assisted scanning tools match CVE disclosures to vulnerable site populations within hours of publication - compressing the patch window to its absolute minimum
- **Payload mutation:** Machine-learning-powered payloads mutate dynamically to evade signature-based detection, reducing the effectiveness of static scan databases
- **Social engineering at scale:** AI-generated phishing campaigns produce convincing impersonation of trusted brands and individuals, making traditional phishing identification increasingly unreliable for end users
- **Adversarial AI:** Tools are emerging that probe and attempt to mislead machine-learning-based security detection systems - creating an arms race at the detection layer itself

The practical implication for SMBs is not that they need to become AI experts. It is that the response window for known vulnerabilities is now measured in hours - and only automated, continuous scanning and real-time alerting operate at the required speed.



Fileless and In-Memory Malware

An emerging pattern in 2025 is the growth of fileless attack techniques - malware that executes entirely in memory without writing persistent files to disk. This is operationally significant because basic file scanners are entirely blind to these attacks. The 19% decline in files cleaned per infected site in 2025 is consistent with - though not solely attributable to - a growing proportion of infections that operate without leaving a file-level trace.

Basic file scanners are blind to fileless attacks. Database-level scanning, behavioral traffic analysis and memory anomaly detection are required to identify fileless infections. This is a direct extension of the 2025 Quiet Compromise pattern -the logical end state is compromise with zero file-level evidence.

Quantum: The Horizon Threat

Quantum computing remains a planning-horizon risk rather than an immediate operational threat for SMBs. However, credible research in 2025 confirmed that current RSA-2048 and similar encryption standards face a long-term risk from near-term quantum hardware development. NIST has finalized its first post-quantum cryptography standards.

For organizations handling sensitive customer data - payment information, personal records, health data - the quantum timeline is now a strategic planning input. The migration to post-quantum encryption will not happen overnight and organizations that begin monitoring NIST's guidance now will not be caught unprepared when the transition becomes operationally necessary.

Final Thoughts & Recommendations

Cyberattacks in 2025 were more calculated than in any previous year in this dataset. Malware became quieter. Persistence became the primary objective. Backdoors reached 70% of infected sites. Multi-family infections deepened and the visible, noisy compromise techniques that once made infections detectable are being systematically abandoned in favour of silent, durable access.

For small businesses, the security baseline has changed. It is no longer sufficient to know your site is online. You need to know whether it is clean, whether any previous compromise has been fully resolved at the root cause and whether the mechanisms that enable reinfection have been removed. For hosting providers, the same logic applies at scale: customer sites that appear healthy can be actively compromised, generating the reinfection cycles that drive your support costs and erode customer trust.

The Bottom Line

Security isn't about locking everything down - it's about being prepared when (not if) someone tries the door. The goal isn't perfection. It's persistence. Small, consistent actions - patching quickly, scanning continuously, remediating completely - shrink risk dramatically. And in 2026, speed is the differentiating factor. Attackers are exploiting vulnerabilities in hours. Your defenses need to match that pace.

Recommendations for SMBs

The threat landscape is automated and relentless. Small businesses do not need enterprise budgets to build effective defenses. They need a focused strategy that keeps pace with how attacks actually operate today.

Patch Everything - Immediately and Continuously

- Update CMS core, all plugins, all themes and all third-party integrations as soon as updates are available
- Prioritize vulnerabilities flagged in known exploited vulnerability lists - the exploitation window can be as short as
- Enable auto-updates where possible; set calendar reminders where not
- Audit your plugin stack quarterly: remove everything not actively in use - deactivated is not the same as safe

Enable Continuous, Deep Scanning

- Run automated malware scanning at least weekly - daily if you operate e-commerce
- Ensure your scanner covers database tables, not just files - backdoors increasingly live in the database
- Enable real-time alerts and treat high and critical alerts as 24-hour action items, not notifications

Demand Root-Cause Remediation - Not Just Cleanup

- Seven in ten infected sites carry a backdoor - cleanup that misses it creates a reinfection countdown
- Verify that any remediation process addresses both the file system and the database
- Change all admin passwords and audit all admin accounts after any confirmed infection
- Address the vulnerability that enabled initial access - otherwise the next infection is a matter of time, not chance

Deploy WAF Protection and Bot Mitigation

- A Web Application Firewall blocks malicious requests before they reach your application code
- Enable login rate limiting and monitoring to reduce brute-force and credential stuffing exposure
- At 5,303 bot probes per site per week, WAF-level filtering is not optional - it is the primary first line

Back Up - and Test Your Backups

- Maintain regular, clean backups stored independently from your live hosting environment
- Test restoration quarterly - an untested backup is not a backup
- Document your recovery path and assign responsibility before you need it

Recommendations for Hosting Providers

Own the Security Conversation Before Your Customers Do

Customers who understand their risk posture act on it. When a customer discovers their site is infected, the first call goes to their host — regardless of who is responsible. The providers that win on security in 2026 are those that surface threats before customers encounter them, not those that react fastest once they do. Clear, timely, jargon-free alerts that tell customers what was found, why it matters and exactly what to do next are the difference between being seen as a trusted partner and being blamed for a breach.

Treat Root-Cause Remediation as the Standard, Not the Escalation

The 2025 backdoor data confirms what the 2024 report warned: cleanup without root-cause removal generates the next support ticket. 70% of infected sites now carry a backdoor. That means the majority of cleanups that address only visible malware will fail — and the failure surfaces as a second ticket, usually within weeks. Remediation that does not check both the file system and the database is not remediation. It is deferral and every incomplete remediation is a recurring cost. Make full root-cause removal the default workflow rather than the exception reserved for repeat cases, and verify before closing.

Close the Enrolment Gap

Protection only works on sites that are covered. The customers least likely to opt into security are consistently the ones most likely to need it — high plugin counts, outdated CMS versions, no WAF. Default-on coverage removes the self-selection problem, shrinks the blast radius of infected sites across shared infrastructure and gives customers a defensible compliance position under NIS2, GDPR and PCI DSS.

Monitor for the Reinfection Signal

Sites that generate multiple security support tickets within 90 days are almost certainly experiencing the backdoor-driven reinfection cycle. Identifying these sites proactively - through platform telemetry, not just ticket history - and prioritizing root-cause remediation for them reduces your support queue and improves customer outcomes before churn becomes the result.

Get Ahead of the May–July Window

CVE disclosure volume peaks between May and July, and the exploitation window is shortest precisely when volume is highest. Broad customer coverage and clear alerting going into that period materially reduces infections, tickets and abuse complaints during the year's highest-risk stretch.

The web will keep changing. Attackers will keep automating.

The path forward is the same as it has been: detect earlier, remediate completely, protect proactively - and treat every clean, secure website as the business asset it is.

Get In Touch

sales@sitelock.com

(877) 846-6639

sitelock.com