imunify Security

WHITE PAPER

PROTECTING SITES FROM BEING BLACKLISTED IN GOOGLE USING SECURITY-FIRST WEB HOSTING

The last decade has seen some of the largest data breaches, and the cost to manage and remediate these breaches continues to increase. Google publishes a transparency report highlighting the massive rise in sites flagged as dangerous. Because shared hosting providers maintain thousands of websites, this makes them a primary target for hackers aiming to breach either individually hosted websites or the server hosting their customer sites.

In a web application environment, the first level of defense is the hosting infrastructure. This puts tremendous pressure on shared host providers to install the right cybersecurity appliances across the environment.

Shared hosting is unique from dedicated hosting or virtual private servers, as customer websites don't run in an isolated environment. Any compromise of one customer site could affect the physical server, and this affects the host's reputation and revenue.

Many shared hosting customers work with a popular content management system such as WordPress, Joomla or Drupal.

60%

WordPress owns over 60% of the content management software market

35%

35% of the Internet is powered by WordPress

WordPress owns over 60% of the content management software market and 35% of the Internet is powered by WordPress.

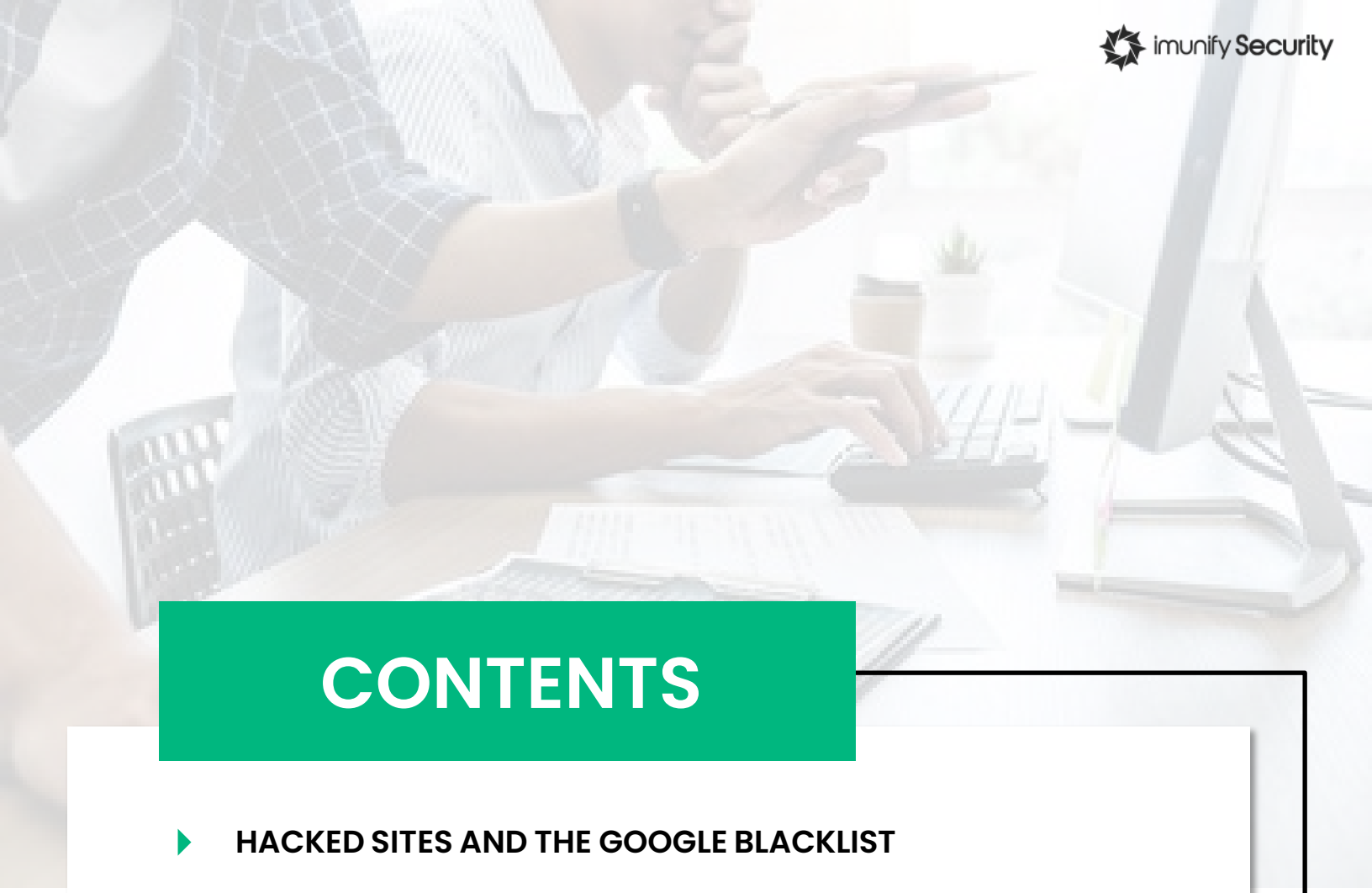
Because of its popularity, hackers write scripts that scan sites for WordPress hosting and then attempt to exploit undiscovered vulnerabilities. This issue makes it especially difficult for shared hosters responsible for protecting not only customer sites but the server itself.

Cross contamination of sites is common in shared hosting where cybersecurity defenses fail.

Harvesting tools allow attackers to get a list of sites hosted on a single IP, which then gives them a list of potential targets. Using the harvested list (which could be thousands of sites on a shared host), the attacker then attempts to read the **wp-config.php file**, which contains credentials for the database and possibly FTP.

With just one compromised site, an attacker could potentially have access to databases, FTP servers, and the hosting physical server in a sophisticated attack across an environment.

To protect the entire environment, it's important that webmasters and digital agencies responsible for customer sites have the tools necessary to monitor and defend customer sites.



imunify Security

CONTENTS

HACKED SITES AND THE GOOGLE BLACKLIST

For any webmaster, keeping a site indexed and performing well in Google is always a main concern. Google published a list of webmaster guidelines, and one item includes "monitoring your site for hacking and removing hacked content as soon as it appears." They detail the types of hacked content that will get the site owner's domain flagged. It's a clear guideline but difficult to follow as most webmasters are not familiar with common web-based attacks that can affect a site.

When a domain is flagged for hacked content, it's removed from the index, meaning it no longer shows in results when a user performs a search query. In some scenarios, Google simply places a warning that the site is hacked in search results.

Both outcomes will greatly affect a corporate website organic search results and ultimately its revenue.

HACKED SITES AND THE GOOGLE BLACKLIST

60 trillion URLs
the Google search bot crawls every day

10K websites
daily Google flags as hacked

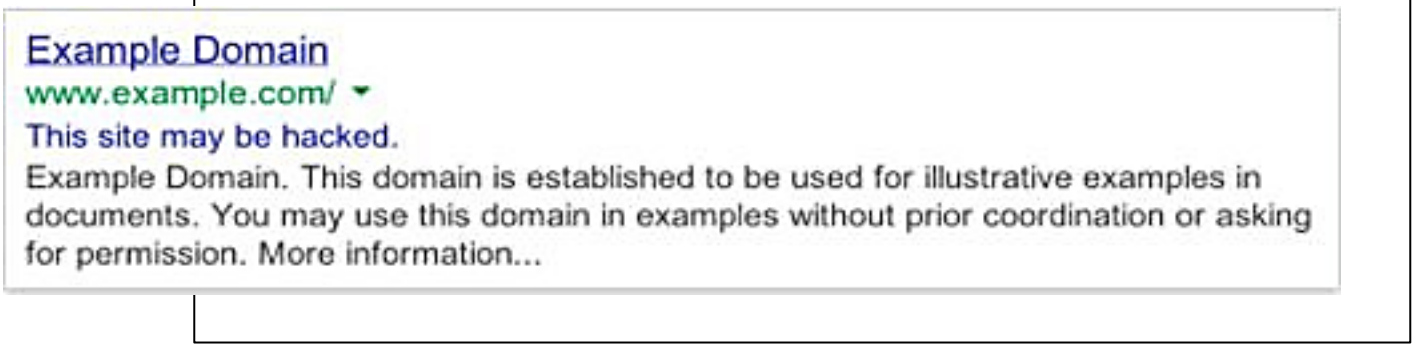
90%
Google owns almost 90% of the market for Internet search

It's estimated that Google flags 10,000 websites daily as hacked of the 60 trillion URLs the search bot crawls.

Google does not refer to the process as blacklisted, but the aftermath can be devastating to the website owner and a tremendous amount of overhead and stress for the webmaster in charge of troubleshooting and remediating the issue.

The effects of being blacklisted are almost immediate. The site owner will see a drop in traffic, as both Bing and Google display a red interstitial message in the user's browser warning them that the site contains malware. Google owns almost 90% of the market for Internet search, so a website flagged by Google Safe Browser will receive almost no organic search traffic. With this drop in search traffic, the site owner will see residual effects in revenue, lead generation, and customer loss.

HOW DOES THE GOOGLE BLACKLISTING PROCESS WORK?



Most website owners are familiar with Googlebot and indexing crawlers, but Google has crawlers that search sites for hacked content often with undisclosed IP addresses so malware site owners cannot avoid detection and cloak malicious files.

Should these crawlers find malicious content, a Safe Browsing flag is triggered against the URL and sometimes the domain itself. Google's Chrome browser uses the Safe Browsing API to detect if a domain is blacklisted and displays a message to users when they type the domain into Chrome.

A message also displays in Google's search results under the website link warning users about the site's current hacked status.

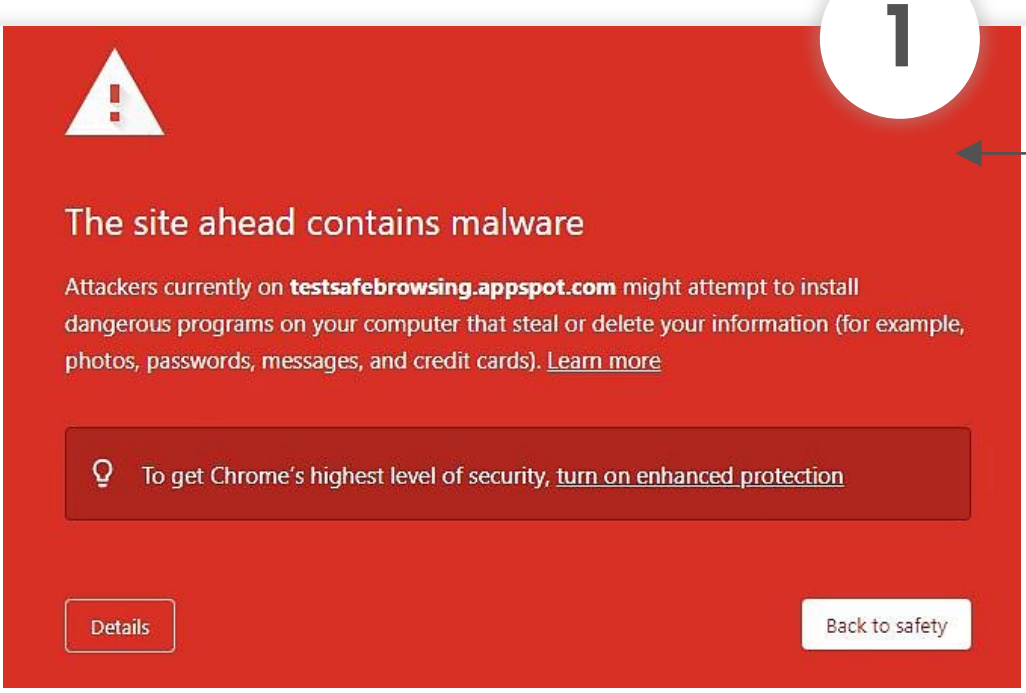
Not every site is hacked when Google flags them. Some sites contain malware or facilitate phishing attacks. Google Safe Browsing detects sites with malicious intent and flags them as well.

When a user types the URL into Chrome or FireFox (which also uses the Safe Browsing API), they are met with a red warning interstitial.

HOW DOES THE GOOGLE BLACKLISTING PROCESS WORK?

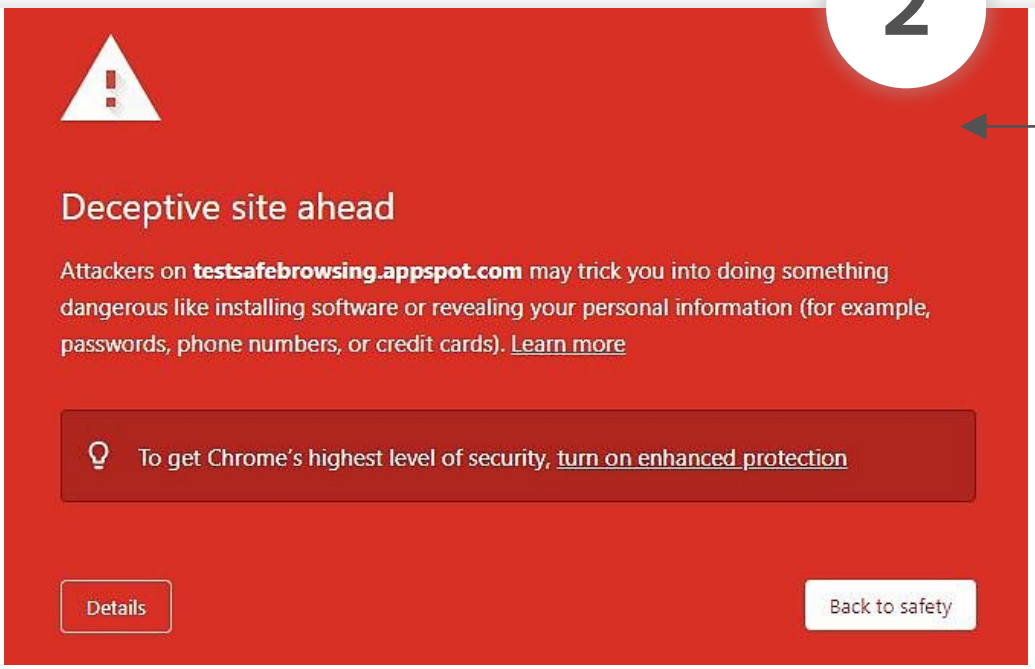
Google has two main red interstitials shown below.

1



Sites that contain malware or harmful code display the warning "This site contains malware."

2



Sites determined to be phishing or a part of a social engineering attack display the warning "Deceptive site ahead."

HOW DOES THE GOOGLE BLACKLISTING PROCESS WORK?

> *Google blacklists sites for several other reasons, and each warning interstitial and notification can be seen here.*

Receiving any one of these alerts requires immediate action, and the first step is troubleshooting the problem. Not every warning means the local website is hacked. These warnings display when Google flags third-party assets such as JavaScript, CSS or a dynamically loaded image (e.g., malicious ads).

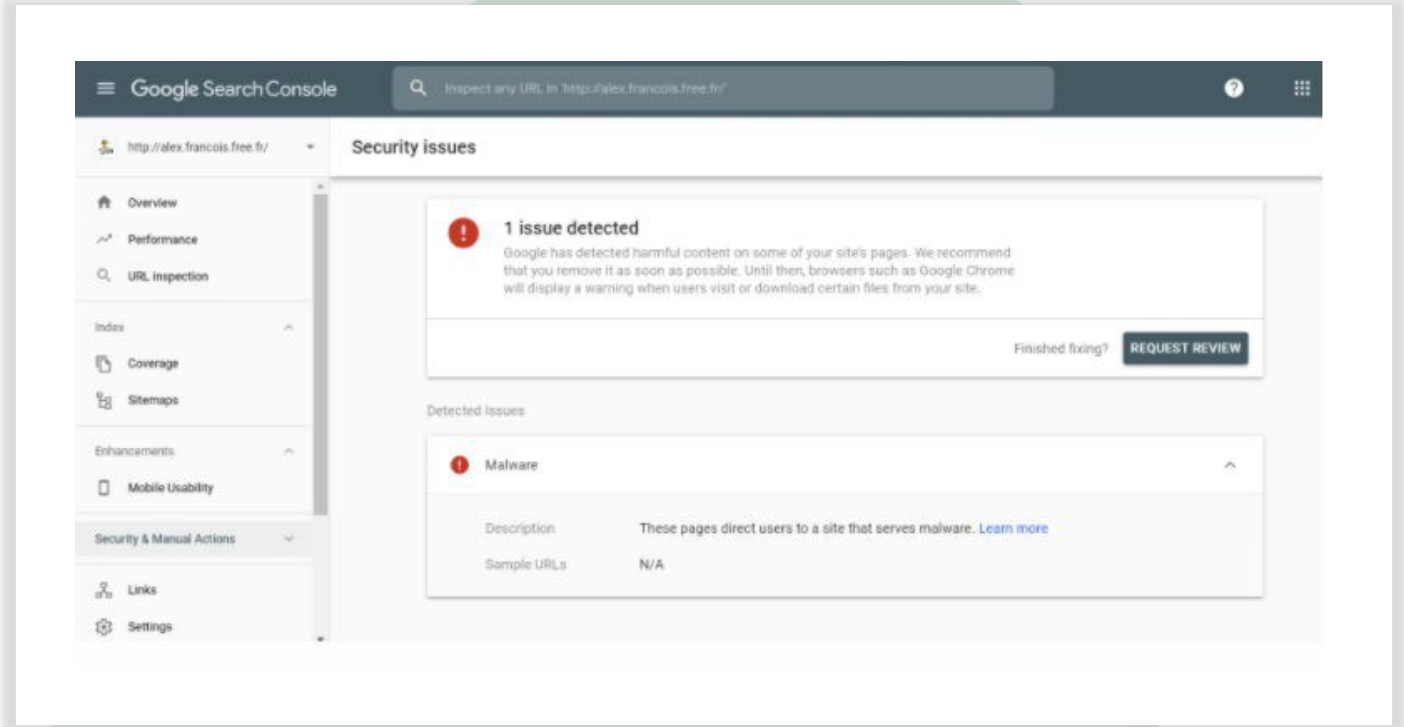
Other Google products can also be affected after being flagged in Safe Browser.

For example, any Adwords ad campaigns pointing to sites determined to host malware will be suspended if the issue is not resolved quickly.

Some website owners see long-term organic traffic loss even after the issue is resolved. If Gmail accounts are found to send phishing emails to the site, the Google Suite or personal Gmail account could be suspended as well.

IDENTIFYING A BLACKLISTED WEBSITE

In any one of the blacklistable attack scenarios, the malicious content is hidden from the site owner, so webmasters must rely on alerts in Google Search Console. Before receiving notifications, the webmaster must first register the site in the Search Console.



After the site is registered, it can take a few days to collect and display data, but a notification about the compromised content should show quickly in the "Security and Manual Actions" page.

WHAT TRIGGERS THE MALWARE WARNINGS?

Google flags sites where it can detect malware or malicious intent, but relying on a simple Google warning should not be the only way a webmaster monitors for malicious content. A site that does not display a warning message in Search Console could still be compromised. To help fight against cyber-criminals, Google does its best to help webmasters be proactive such as notifying them of an outdated WordPress version running on a registered site.

A few reasons why a site gets flagged include:

INJECTED CONTENT

If attackers are able to add content to a site's existing pages, the malicious code can be used to steal data from users or trick them into sending data in attacks such as clickjacking. JavaScript files can also be used to inject malicious content if an attacker can add them to site files.

ADDED CONTENT

Attackers with write access to a server's directories can upload malicious files unknown to the site owner. Links to the files are then sent to an attacker's targeted victims. The newly created files can go unnoticed until Google crawlers find them and flag the domain as an attack site.

HIDDEN CONTENT

In spam attacks, attackers inject hidden links into a site page that points to their malicious content. The links can be hidden using CSS and JavaScript, or attackers could display them far down the page so that the site owner does not notice them. This attack is commonly used for pharma spam where hacked sites host hidden links to drug-related sites.

REDIRECTS

Conditional redirects send users to a malicious website when users click the website link in Google but not when the site URL is directly entered into a browser. When the website owner or webmaster checks the site by directly typing the URL into Chrome, the site acts normally. These conditional redirects help keep the hacked content hidden from the site owner but redirect users to another page when finding the site in a search engine.

WHAT TRIGGERS THE MALWARE WARNINGS?

1. INJECTED CONTENT

Injected content can be anything from a malicious third-party JavaScript file or persistent XSS where the attacker adds links to your site. Persistent XSS content is usually stored in the site database, which means that tables must be cleaned from the malicious content and the offending code snippet remediated.

External files should be stored locally. Should the third-party host be compromised, the scripts included in the site code would be controlled by the attacker.

2. ADDED CONTENT

Attackers with access to directories can upload malware for the site owner to host. By uploading malicious files to numerous compromised sites, an attacker can then use phishing emails to trick users into thinking they are downloading files from a legitimate website.

Attackers that aim to inject links and malicious downloads on a site server often work with a mesh of hacked sites instead of just one compromised server. In this scenario, the files are hidden from view when the site owner browses the site, but Google's crawlers are able to detect them while analyzing site content

WHAT TRIGGERS THE MALWARE WARNINGS?

3. HIDDEN CONTENT

Hiding malicious content is one component of compromising a site.

Hackers like to keep their actions hidden from the site owner so that injected and uploaded content will persist. They do this by using conditional coding such as displaying malicious content based on the user agent or the REFERER header value. The hidden content is placed in a div or other HTML element with CSS properties (e.g. the div contains the “display: none;” directive). When users view the web page, they do not see the hidden links, but crawlers detect them.

Cloaked links are an example of hidden content. Pharmaceutical links, referred to as a “pharma hack,” are often injected as cloaked links. Cloaked content refers to web page content that does not display to human users but is injected into a page where crawlers can process the links as backlinks to a specific site. By using cloaked links, the attacker can manipulate search results to better rank sites in Google’s index.

WHAT TRIGGERS THE MALWARE WARNINGS?

4. REDIRECTS

Google detects phishing content meant to steal credentials and financial information from targeted users. When sites get caught hosting phishing pages, Google flags them as suspicious. Hackers use third-party sites in several ways to facilitate phishing. The first one is hidden redirects. The redirects are usually configured in the httpd.conf file to conditionally send users to a phishing page based on the REFERER value to avoid detection.

The second way attackers use redirects is based on vulnerabilities on the website. It's not uncommon for developers to redirect users based on query string values. If the redirects are not whitelisted to ensure that users are only redirected to defined sites, then attackers can use them for their own phishing pages.

For instance, the following URL could be used to redirect users:
https://site.com/?redirect=anypage.com

The redirect query string variable should be whitelisted, or an attacker could use it to launch a phishing attack.

When users see the URL, they see an innocuous link to "site.com," but open redirects allow an attacker to trick users into going to a malicious page.

The link would look similar to the following:
https://site.com/?redirect=maliciouspage.com

In the above example, the user would be redirected to the attacker's phishing page allowing them to trick users into thinking they went to a familiar site

WEB HOSTING WITH SECURITY IN MIND

Web hosts offer several advantages that help webmasters manage their clients' sites, but security is the most critical component in protecting site owners from long-term effects after a compromise and to protect the site from being blacklisted in search engines. An attacker with complex stealth access to server resources can persist for months.

Create.com takes a security approach to the creative website management experience. Most hosting services focus primarily on user tools, but Create.com combines user tools with advanced security so that webmasters can ensure the safety of their customer websites.

There are several Content Management Site (CMS) applications on the market, but WordPress is a primary target for attackers.

WordPress itself is secure and allows users to quickly create a website, but the plugins and settings used on the site often lead to a compromise. It's easy to find simple scripts that can be used to find vulnerable WordPress sites, so exploiting WordPress doesn't even require advanced hacking skills. It's critical that any hosted WordPress site has the right security in place to protect against threats.

For many webmasters, using WordPress alleviates much of the site management overhead compared to coding a site from scratch. Because of the ease of use with WordPress, the software owns over 30% of the market followed by Joomla and Drupal. The popularity of WordPress makes it great for creatives, but bad for cybersecurity. If WordPress isn't configured and managed properly, it's often hacked.

As new vulnerabilities are found, a WordPress site and its plugins must be patched quickly.

WEB HOSTING WITH SECURITY IN MIND

With Create.com, webmasters have two options for secure hosting

MANAGED WORDPRESS

In a managed WordPress environment, the hoster helps with updates, monitoring, and security for the site. This option leaves the cybersecurity of the site in the hands of the hoster, which is beneficial for webmasters unfamiliar with the way hackers work.

SHARED HOSTING

With shared hosting, the webmaster has full control over the website but leverages the hoster's server. The hoster's server security protects the site from a compromise, and provides 99.9% uptime, a 50-day money-back guarantee, solid state drive backup storage, and free unlimited migrations.

In either one of the above scenarios, it's still important for users to keep auto-updates turned on. With automatic updates to WordPress, the system will install the latest version of the software without any interaction from the user. This will eliminate many of the issues where users abandon sites or don't log into their main dashboard, and the software never gets updated.
These sites are perfect targets for attackers.

In addition to automatically updating WordPress, the site owner should always take regular backups and keep these backups for at least two weeks (30 days are preferable). Backups are critical for disaster recovery and incident response. If malware cannot be removed from a site, backups can be used to restore the database and files.

Note though that should malware persist on the site for months, these backups could contain malware and must be properly audited.

THE SOURCE OF MOST VULNERABILITIES: WORDPRESS PLUGINS

The WordPress software itself is generally safe, but it has frequent updates that must be installed as they are released. It's not uncommon for sites to have dozens of plugins installed, and it's often these coded widgets that leave sites vulnerable to exploits. Most plugin creators keep their code patched against the latest vulnerabilities, but some authors abandon their projects leaving the code open to the latest exploits.

In widespread compromises, the plugin author hands over their project to an unknown party who injects malicious code into the plugin code repository. Injected code in a popular plugin can leave hundreds of thousands of WordPress sites open to hackers.

As an example of a widespread compromise, the All In One SEO Pack plugin — installed by over 2 million users — was found to have a medium-level security vulnerability affecting any site that allowed authenticated authors or contributors to upload content to the site.

The plugin did not sanitize input in the SEO title and SEO description fields, so an authenticated user could inject their own crafted malicious HTML or JavaScript into title and description fields in an effort to take over the site. With this Cross-Site Scripting (XSS) vulnerability, an attacker could perform any number of activities in the context of an administrator account when the administrator views a page with these fields.

THE SOURCE OF MOST VULNERABILITIES: WORDPRESS PLUGINS

The vulnerability required an immediate update to the newer version, but many webmasters are unaware of CVE notices and leave WordPress sites unattended. When vulnerabilities are made public, attackers scan the web for these specific vulnerabilities and exploit them. After sites are exploited, they host malicious content that Google's crawlers collect and potentially flag the site in Safe Browsing.

Plugin developers often use the same open-source libraries, so a vulnerability in just one library can affect several plugins. In a large-scale WordPress attack, a single bad actor can affect hundreds of thousands of sites. In April 2020, researchers saw a large spike in scans against WordPress sites for several existing vulnerabilities.

A single bad actor used 24,000 distinct IP addresses to scan 900,000 WordPress sites searching for known vulnerabilities in popular plugins. The attacker then attempted to inject third-party hosted JavaScript code into vulnerable pages that would run when an administrator is authenticated into the WordPress dashboard.

CREATE.COM CYBERSECURITY FOCUS

Create.com offers a creative experience but with a focus on security. They leverage Imunify360 to minimize and mitigate threats allowing webmasters and other site administrators to defend WordPress and other CMS sites without the added requirement of knowing cybersecurity and configuration management of infrastructure. WordPress security is enhanced with several layers of security that protects from several threats in the wild.

STOP OUTGOING SPAM

Compromising a server to send outgoing spam emails is common for bad actors looking for ways to send phishing emails without having them blocked by filters. Email servers commonly used by spammers are already blocked by filters, so spammers must find alternative ways to send malicious content. When an email provider is added to spam blacklists, all other customer emails sent from the same server will be blocked by spam blockers. For this reason, it's important for webmasters and host providers to protect from outgoing spam.

Create.com leverages "rspamd," which is an email spam filter that analyzes outgoing email, determines if it's spam, and forwards it to an additional anti-spam layer named MailChannels. Email is then sent to the recipient only if the email passes validation. This double validation and anti-spam layers protect the site owner, the provider, and any other customers on Create.com servers.

CREATE.COM CYBERSECURITY FOCUS

SECURE MIGRATION

During migration, Imunify360 scans the site as files are transferred to the new host server. Imunify360 performs an antivirus scan on all site elements and automatically fixes issues as the site migrates.

Customers searching for better security often already have hacked sites. Attackers use several techniques to stay hidden from detection, so many customers are unaware that their sites have been compromised.

Create.com leverages Imunify360 to help new customers securely migrate their sites from their current host to the local Create.com host servers. Migration is fully automated for customer convenience so that webmasters unfamiliar with the steps to move a site from one host to another can rely on Create.com tools.

This unique Create.com migration component is just one example of focusing on security to protect site owners on a shared hosting server.

SIX LAYERS OF SECURITY IN IMUNIFY360

Imunify360 helps webmasters in a number of ways and integrates directly with Create.com cyber-defenses. By keeping security as a primary focus, webmasters no longer need to find their own tools, install them, and ensure that configurations are correctly set up. Imunify360 has six layers of security.

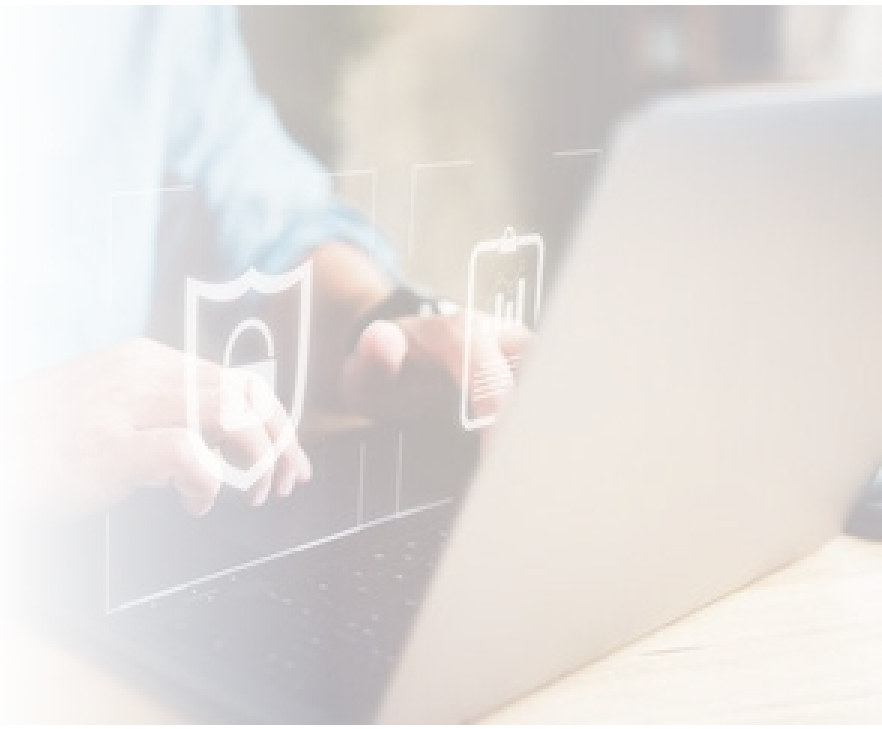
ANTIVIRUS

It's estimated that ⅛ of new files stored on a server are malicious. Antivirus is a basic component in cybersecurity but often overlooked in web application hosting. Most webmasters know that desktop antivirus is necessary for local device security, but they are unaware that antivirus is also necessary for web application security. Imunify360 identifies and cleans malicious content so that site owners do not need to manually find hacked files.

SIX LAYERS OF SECURITY IN IMUNIFY360

FIREWALL

In simple applications, blocking all incoming traffic protects the internal network. This configuration is common for home firewalls, but it's not feasible in a hosting environment that needs advanced analysis for incoming and outgoing traffic. Imunify360 includes an advanced firewall that uses cloud heuristics and artificial intelligence (AI) to detect threats and block brute-force attacks often used to guess a user's credentials.



WEB APPLICATION FIREWALL (WAF)

A standard firewall analyzes and filters all traffic, but a WAF targets HTTP traffic. By targeting
HTTP traffic, a WAF can block specific attacks against web applications such as XSS, SQL injection, file inclusion and several others. These attacks are commonly misunderstood and often hidden to webmasters who do not know how to monitor them. Traffic passes through the Imunify360 WAF that then analyzes its content to determine if it's malicious. If the request passes validation, it's forwarded to the web application.

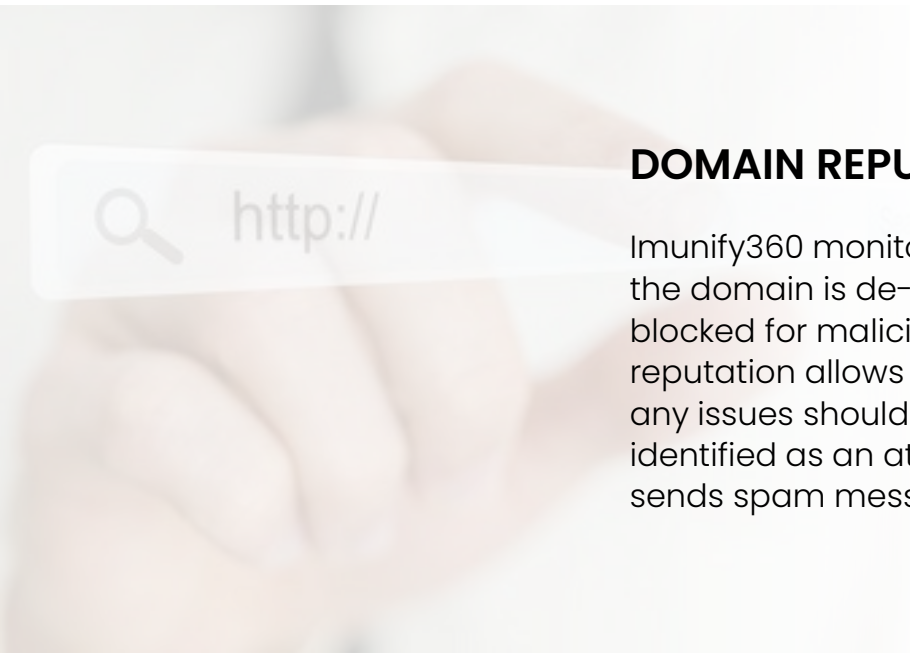
SIX LAYERS OF SECURITY IN IMUNIFY360

PHP SECURITY LAYER

Web security is more than blocking incoming traffic. It also means identifying content on the site that could be silently performing malicious actions. For example, a PHP script injected into the site could be used to send spam emails to targeted recipients. Imunify360 is a proactive defense that adds an extra PHP Security Layer of protection, prevents malware execution in real-time, and ensures multi-level access blocking to malicious PHP files.

PATCH MANAGEMENT

Cybersecurity of any application is never a "set it and forget it" event. Software vendors including plugin developers frequently deploy patches to remediate newly found vulnerabilities. To continue protecting a CMS, all plugins and the CMS software must be patched every time a new update is published. Imunify360 provides proactive cyber-defenses by patching software after developers deploy an update. By quickly patching the CMS, the webmaster reduces the window of opportunity for an attacker.



DOMAIN REPUTATION

Imunify360 monitors various blacklists to find out if the domain is de-listed from search engines or blocked for malicious activity. Monitoring domain reputation allows webmasters to quickly remediate any issues should the site be compromised and identified as an attack site that distributes malware, sends spam messages, or hosts phishing content.

SECURE HOSTING WITH CREATE.COM

With Imunify360, Create.com offers the most secure environment for webmaster sites, especially preferred CMS applications such as WordPress.

Monitoring for hacked content takes a lot of professional experience, but just one oversight can result in numerous website issues including blacklisted in search engines, reduced incoming organic traffic and revenue, and potential for suspension of other Google product accounts.

We're all about layering security services for a cleaner internet and customer experience. Are you with us?

Adam Farrar,

CEO of Create.com

Join Create.com now!