COMPREHENSIVE GUIDE TO PROTECTING YOUR WEBSITE FROM MALWARE ATTACKS

Prepared By: www.unitedseo.ae

WHAT IS MALWARE?

Malware is a collective term for any software intentionally designed to cause harm or exploit vulnerabilities in computer systems. It includes various malicious programs and code that can be used for a variety of nefarious purposes. Malware can infect devices, steal sensitive data, disrupt operations, and serve as a platform for other cyberattacks.

GLOBAL MALWARE INFECTIONS

- In 2020-2023, there were over 560 million malware attacks globally.
- The cost of global cybercrime reached approximately $1 trillion in 2020.

Ransomware Attacks:

- Ransomware attacks increased by 485% in 2020.
- The average ransom demand surged to over $220,000 in 2020.

Data Breaches

- Over 37 billion data records were exposed in data breaches in 2020.
- The average cost of a data breach in 2020 was $3.86 million.

Business Impact

- Approximately 60% of small businesses go out of business within six months of a cyberattack.
- Large enterprises spend an average of $1.3 million to remediate a malware attack.

WHAT ARE THE MOST COMMON TYPES OF MALWARE ATTACKS?

VIRUSES

A virus infects other programs and can spread to other systems, in addition to performing its own malicious acts. A virus is attached to a file and is executed once the file is launched. The virus will then encrypt, corrupt, delete, or move your data and files. Viruses will often be attached to phishing emails and lead to larger attacks like business email compromise (BEC) attacks.

BOTS

A computer with a bot infection can spread the bot to other devices, creating what's known as a botnet. This network of bot-compromised machines can then be controlled and used to launch massive attacks — such as DDoS attacks or brute force attacks — often without the device owner being aware of its role in the attack. Bots are also used for crypto mining on specific hardware. One way to control bots is to use tools that help determine if traffic is coming from a human user or a bot.

SPYWARE

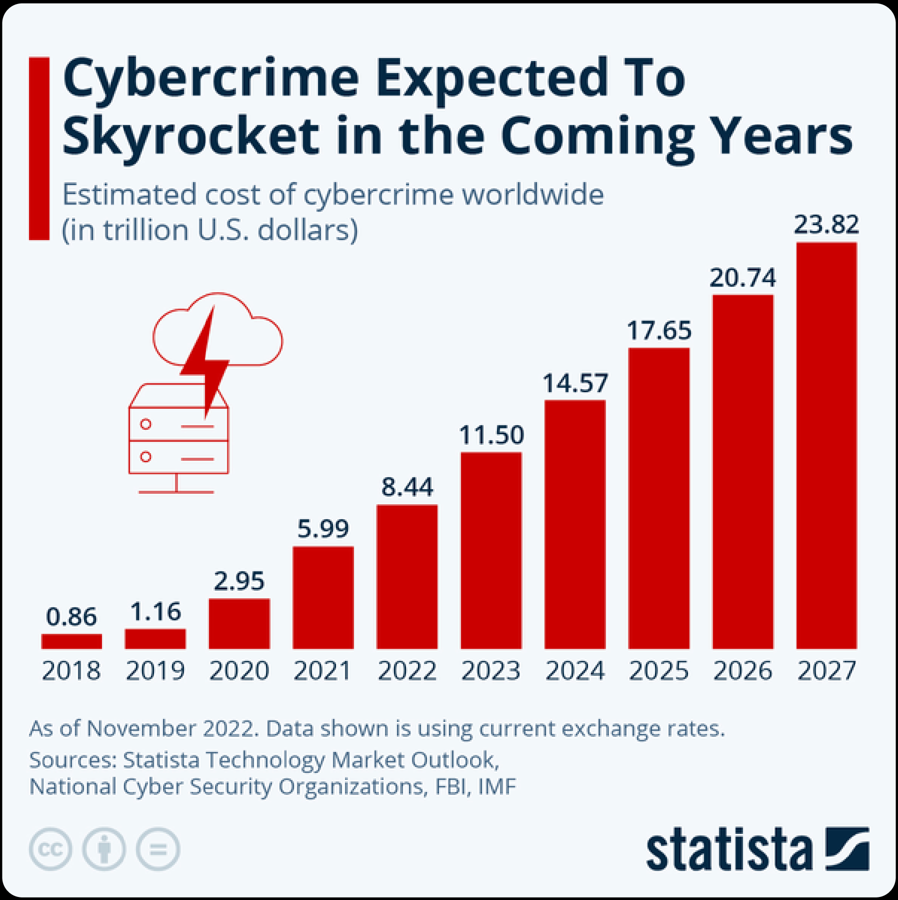
Cybercriminals use spyware to monitor the activities of users. Spyware often leads to credential theft, which in turn can lead to a devastating data breach. It often originates in corrupt files, or through downloading suspicious files.
Keyloggers are a common kind of spyware that monitors and records users' keystrokes. With this kind of spyware, hackers can steal credentials as well as credit card numbers and other data that may be entered into a system through typing.

RANSOMWARE

Arguably the most common form of malware, ransomware attacks encrypt a device's data and holds it for ransom. If the ransom isn't paid by a certain deadline, the threat actor threatens to delete or release the valuable data (often opting to sell it on the dark web).

TROJANS

A Trojan program pretends to be a legitimate one, but it is in fact malicious. A Trojan can't spread by itself like a virus or worm but instead must be executed by its victim, often through social engineering tactics such as phishing. Trojans rely on social engineering to spread, which puts the burden of defence on users.



Cybercrime Expected To Skyrocket in the Coming Years

Estimated cost of cybercrime worldwide (in trillion U.S. dollars)

As of November 2022. Data shown is using current exchange rates.

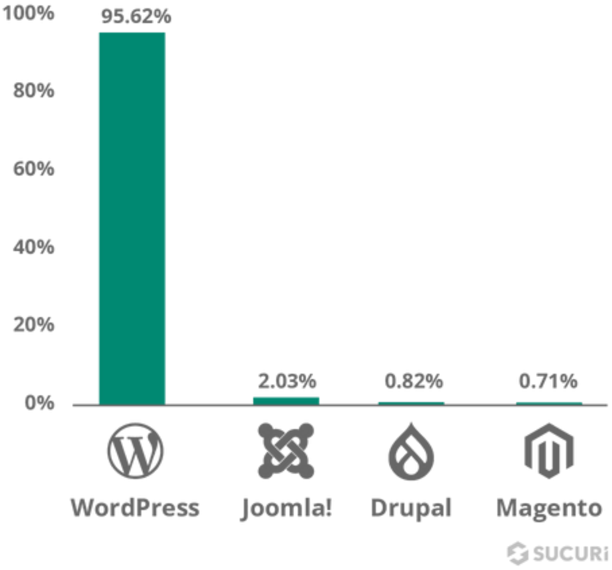
Sources: Statista Technology Market Outlook, National Cyber Security Organizations, FBI, IMF

According to estimates from Statista's Cybersecurity Outlook, the global cost of cybercrime is expected to surge in the next five years, rising from $8.44 trillion in 2022 to $23.84 trillion by 2027. Cybercrime is defined by Cyber Crime Magazine as the "damage and destruction of data, stolen money, lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, post-attack disruption to the normal course of business, forensic investigation, restoration and deletion of hacked data and systems, and reputational harm.

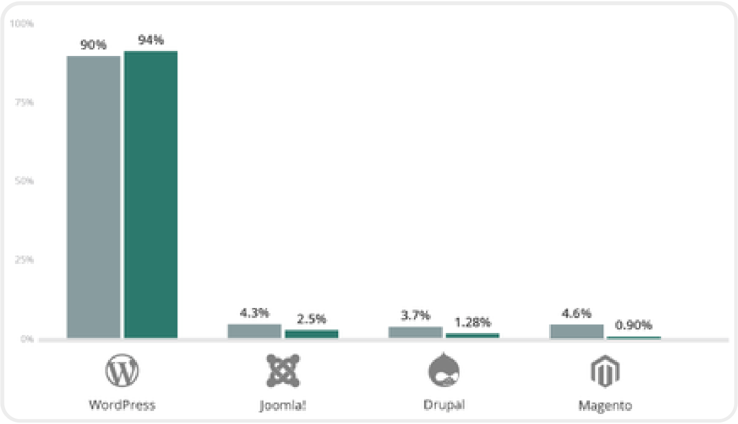
Read more on the costliest cyber attacks here.

CMS INFECTIONS

As per Sucuri data sets, that indicate WordPress continues to be the most popular CMS among our user base, accounting for 95.62% of clients in 2021-2022. As seen in past years, Joomla (2.03%) followed in second place with Drupal (0.82%) taking third.



In fact, 94% of hacked websites we cleaned last year ran on WordPress, a statistic highlighted in the Sucuri 2021-2022 Hacked Website Threat Report. It not only looks at WordPress security but at the threat landscape as a whole.



COMMON MALWARE ATTACKS ON WORDPRESS WEBSITES

WordPress is a popular content management system (CMS) used by millions of websites worldwide. Unfortunately, its widespread use makes it a prime target for various types of malware attacks. Here are some common types of malware attacks that target WordPress websites:

BRUTE FORCE ATTACKS

The simplest form of attack that targets one of the potentially weakest links in security – your password! A Brute Force Attack involves a cyber criminal attempting a gigantic number of password combinations over and over again until the correct combination is found.

This form of attack is far from elegant but has proven to be very effective against weak passwords and usernames like ‘123’, ‘password’, and ‘admin’.

WORDPRESS CORE VULNERABILITIES

WordPress is open source, allowing your business to reduce cost and provides extensive innovation opportunities.

But since the source code is easily obtainable, potential cyber criminals can identify core vulnerabilities and exploit them.

One of the easiest ways of exposing your WordPress site to attack is to continue to use updated WordPress versions as well as running older versions of WordPress’s scripting language, PHP.

SQL INJECTION ATTACKS

One of the most common WordPress attacks, an individual may cause damage or gain access to your WordPress admin by injecting malicious SQL queries or statements to manipulate your MySQL database.

Any user input section of your WordPress site such as a contact form or search box may be susceptible to a SQL Injection attack.

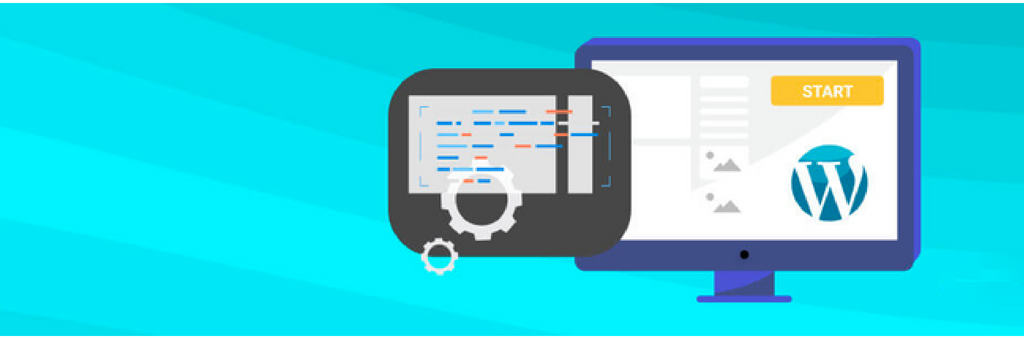
Themes and Plugins may be your weak link to SQL Injection attacks so make sure anything installed comes from a reliable and trusted developer.

As your MySQL Database software is vulnerable to this form of attack it is important to make sure you keep up with software updates and never allow access to your MySQL credentials.

PLUGIN AND THEME VULNERABILITIES

Plugins and Themes are a fantastic way to add functionality to your WordPress pages or create a unique look. But plugins are a frequent entry point of WordPress attacks owing to their reliance on developers to keep up to date with security weaknesses and exploits.

If a plugin has not been updated in over 6 months, the developer may have abandoned it. These plugins are most vulnerable to exploits and it is best to avoid them entirely.



HOW TO PROTECT THE WEBSITE FROM MALWARE ATTACK?

WEBSITE
OWNER'S RESPONSIBILITIES

KEEP SOFTWARE AND PLUGINS UPDATED

Regularly updating your content management system (CMS), themes, and plugins is essential. Outdated software can contain vulnerabilities that hackers exploit to gain access to your website. To update, log into your CMS admin dashboard, navigate to the updates section, and apply the available updates promptly. Repeat this process at least once a week for optimal security.

How to do it:

- For content management systems (CMS) like WordPress, log in to your admin dashboard and look for available updates. Apply them promptly.

- For plugins and themes, regularly check for updates in the admin panel and update as needed.

Frequency: Check for updates at least once a week and apply them immediately.

USE STRONG PASSWORDS

Strong passwords are your first line of defense. Create complex, unique passwords that include a mix of uppercase and lowercase letters, numbers, and special characters. Utilize a reputable password manager to generate and securely store these passwords. Change your passwords every 3-6 months or immediately if you suspect any compromise.

How to do it:

- Use a password manager to generate and store complex passwords.

- Ensure passwords are a mix of uppercase, lowercase, numbers, and special characters.

Frequency: Change passwords every 3-6 months or immediately if you suspect a breach.

IMPLEMENT TWO-FACTOR AUTHENTICATION (2FA)

2FA adds an extra layer of security by requiring a secondary verification step, typically involving a mobile app or text message. To enable 2FA, go to your account settings and follow the setup process. Once enabled, it provides continuous protection against unauthorized access

How to do it:

- In your account settings, enable 2FA and follow the setup process.

Frequency: Enable 2FA once, and it remains active.

BACKUP YOUR WEBSITE

Regular backups are your safety net in case of an attack or data loss. Use backup plugins or your hosting provider's backup feature to schedule automated backups, ideally on a daily or weekly basis. Store these backups securely in offsite locations or cloud storage to ensure their availability when needed.

How to do it:

- Use a backup plugin or your hosting provider's backup feature.
- Schedule automated backups to run daily or weekly.
- Store backups in secure, offsite locations or cloud storage.

Frequency: weekly automated backups are recommended.

REGULARLY SCAN FOR MALWARE

Use reputable security plugins or online scanners to regularly scan your website for malware and vulnerabilities. Schedule automated scans, ideally on a weekly basis, to detect and address potential threats promptly

How to do it:

- Use security plugins or online scanners.
- • Schedule automated scans.

Frequency: Perform scans weekly or after major updates.

HOW UNITEDSEO CAN HELP YOU

PROVIDE ONGOING MAINTENANCE

UnitedSEO can offer website maintenance packages that encompass regular updates, backups, and security scans. These tasks should be performed on a scheduled basis, ideally weekly or as specified in the client's agreement.

EDUCATE CLIENTS

We educate clients on security best practices, including password management and recognizing phishing attempts. Initial training should be supplemented with periodic updates and reminders to ensure clients remain vigilant.

MONITOR WEBSITE PERFORMANCE

We set up performance monitoring tools to detect both performance issues and potential security breaches in real-time. This entails configuring alerts for unusual activity or performance drops and continuous monitoring.

REGULAR SECURITY AUDITS

Conduct periodic security audits of website to identify and address vulnerabilities that could indirectly affect client websites.

REPORTING

we will provide you with monthly reports with each month what work has been carried forward and also a monthly audit checklist.

LOOKING FOR WEBSITE MAINTENANCE CONTRACTS?

WE'VE GOT YOU COVERED!

Your website is your online identity. Ensure it's always up and running smoothly with our expert website maintenance services. Whether you're a business owner, blogger, or e-commerce store owner, our team of professionals is ready to take care of all your website needs. From regular updates and security checks to performance optimization, we've got the expertise to keep your online presence in top shape.

Call us: +971 4 442 6518