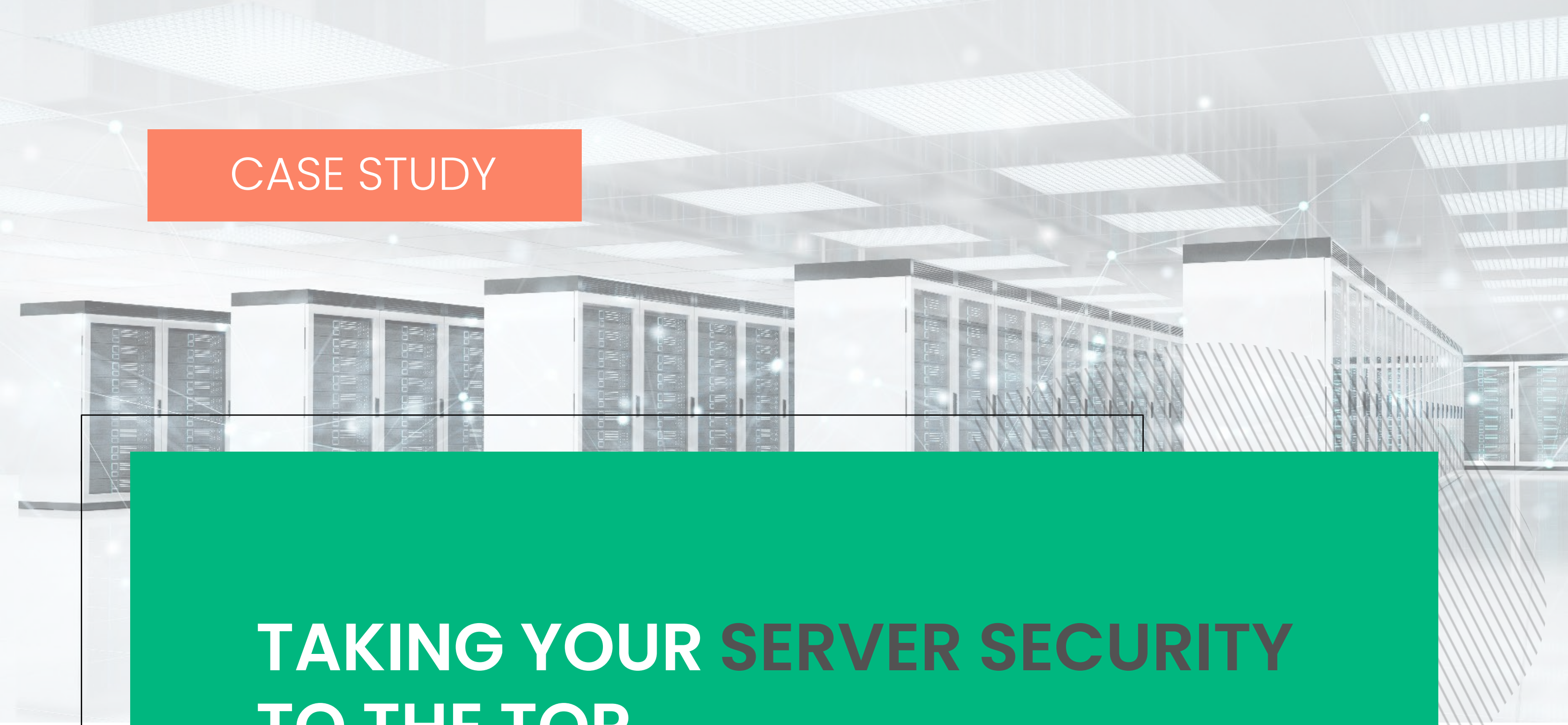
imunify Security



CASE STUDY

TAKING YOUR SERVER SECURITY TO THE TOP

Every site owner wants to avoid malware, but they don't have the skills to monitor threats and mitigate attacks should their website be a target. In a shared hosting environment, most sites hosted on the server run on common software such as WordPress or Joomla. While this makes it easy for site owners to build a site with little web development knowledge, it's also beneficial for hackers. Hackers prey on small sites with little security, and then these sites become a burden on server resources.

An increase in server resource usage affects the server as a whole, which means that all customers running sites in the shared hosting environment are affected. This phenomenon can increase cost of server maintenance, decrease revenue, and harm the host's reputation. Eventually, it can mean the loss of customers and a reputation for poorly performing host servers.

THE IMPACT OF HACKED SITES ON A SERVER

Hacking is a business, and the market for data can make an attacker a substantial amount of money on darknet markets. The median price for someone's identity is about $21, which means a large data breach can generate millions of dollars in revenue for a hacker.

To breach a site, attackers often use malware, which comes in many forms and strategies. Malware can be in the form of uploaded shell scripts or malicious requests such as SQL injection. Attacks are typically botted, so a bad actor can compromise numerous sites in a matter of only a few minutes. Data breaches often happen with long-term hidden malware that goes undetected. With malware injected onto a site, the attacker can then continually exfiltrate data from the website and send it to a remote server.

New cryptojacking attacks are also on the rise. As cryptocurrency increases in popularity, the attack strategy focuses on running crypto-mining software that generates digital currency. Just a few years ago, several well-known and popular sites were targets of cryptojacking.

Cryptojackers look for vulnerable sites that give them access to high-powered servers. High-end server resources pooled together give these attackers access to better computing power that generates thousands of dollars in cryptocurrency. By hoarding server resources, hosted websites will see extensive performance degradation slowing their sites to unusable speeds.

Cryptojacking can have the most severe consequences, but it's not the only malware that spikes computer resources. PHP shell scripts used to run commands on the hosted site or the server itself use computer resources, and databases vulnerable to SQL injection could be used to store additional malicious content. An attacker will use scripts to remotely call injected content stored on the site, and these automated requests use computer resources. No matter what type of malware running on a server, computer usage will be needed to trigger, activate, and run it. In a shared environment, there could be hundreds of hacked sites using resources on the server.

ABOUT STABLEPOINT

60 000

supporting over 60,000 websites

38

locations worlfwide

5.0

☆☆☆ Trustpilot eating

STABLEPOINT

Stablepoint is a global web hosting company supporting over 60,000 websites located in 38 locations for customers worldwide. They've maintained a 5.0 Trustpilot rating for their fast severs and well-respected customer service. Although their servers were optimized for speed and security, Stablepoint still had a few issues with hacked and compromised websites, usually due to site owners leaving outdated scripts or insecure plugins installed on their sites.

Even with Stablepoint's server security, responsibility of managing installed software site falls on the site owner. The initial indication that something was wrong manifested in the form of performance degradation. The performance degradation caused problems for other users hosting sites on Stablepoint's servers, so they turned to Imunify360 to solve their problem.

HOW STABLEPOINT TOOK WEB SERVER SECURITY TO THE NEXT LEVEL

To respond to the growing threat of hacked sites on their servers, Stablepoint turned to Imunify360 to help mitigate malware and botted requests to scan web application firewalls. They found that Imunify360 stopped a lot of attacks on the web application firewalls, and it stopped many of the common attacks experienced by website owners such as PHP shell uploads, SQL injection attacks, and others. It also stopped the automated vulnerability scans attackers use to find exploitable websites.

A common attack on small WordPress websites is brute-force automation on the administrator account.

Imunify360 handled these attacks and stopped the botted requests from sending thousands of requests attempting to find the administrator's credentials. It stopped attacks and banned the attacker's IP before requests used too much resources and affected performance. False positives were rare, but CAPTCHAs slowed attacks without blocking the IP entirely.

By using CAPTCHAs, the IP identified in the attack could be throttled while eliminating accidental blocking of a legitimate user IP.

HOW STABLEPOINT TOOK WEB SERVER SECURITY TO THE NEXT LEVEL

After Stablepoint implemented Imunify360, fewer websites were compromised and servers became more reliable. While some Stablepoint customers still experience site compromises, Stablepoint technicians receive straight-forward reports that help them more quickly and effectively remediate the issue. Imunify360 also empowers site owners to scan for malware and perform removal actions directly from cPanel so that they can remove malware as well.

> We really like the Imunify360 package as a whole and consider it a MUST install when running any web-hosting server.
>
> **Darren Lingham**
> Co-founder of Stablepoint

The Proactive Defense tool blocks many attacks per minute, meaning Stablepoint received fewer abuse reports for hacked content. Imunify360 stopped malware from running entirely. Stablepoint experienced hundreds of blocked malware scripts using Imunify360.

BAD ACTORS USE NUMEROUS ATTACKS AGAINST WEB SERVERS

Website owners face numerous types of attacks, and many of them do not understand the intricacies of these attacks or -- more importantly -- how to stop them. Imunify360 stops many of the common web-based attacks in the wild.

Web-based attacks are often based on malicious HTTP/HTTPS requests. For example, scanners use web requests to find vulnerabilities, and SQL injection is sent using an HTTP/HTTPS POST request. This request can be blocked with Imunify360's web application firewall (WAF) along with WebShield and a network firewall. Imunify360 WAF will protect shared hosting customer websites from malicious requests sent to web applications and their APIs

IMUNIFY360 WILL STOP:

Vulnerability exploitations

Malware uploads

Sensitive data access

Website scraping and scanning

Web SPAM

Many other web threats

BAD ACTORS USE NUMEROUS ATTACKS AGAINST WEB SERVERS

Brute-force attacks against passwords are very common on web applications running on popular software such as WordPress. Scripts used to brute force passwords will run at several requests per second, and it can overload server resources as every request must be processed. Imunify360 WebShield component will take care of CDN and Proxy Traffic by determining the real IP address of an attacker versus legitimate users. It grey lists suspicious IPs and serves CAPTCHA challenges and Splash Screens to interrupt bots blocking these malicious requests.

Imunify360 mitigates brute-force attacks with also a pluggable authentication module (PAM) and an intrusion prevention system (IPS) with IP management. In addition, Imunify360 has a port firewall that will prevent all attacks against system services such as FTP, SSH, and IMAP/SMTP.

Some sites are vulnerable to malicious uploads either from authorization misconfigurations or code that does not validate file uploads. Imunify360 protection provides a unique Proactive Defense technology that detects malicious execution flow and stops it in run-time. It analyzes PHP actions and prevents any malicious activity from affecting the server.
This Imunify360 feature is critical to the health of your server, because malicious code is often obfuscated and hidden in legitimate files, database tables, or dynamically retrieved from the network staying hidden from regular signatures-based search . Proactive Defense from Imunify360 stops dangerous execution before it infects any part of the site or the server.

Injecting code into legitimate files or uploading infected files to local storage leave websites vulnerable to data breaches, ransomware, or takeover of the administrator account.
Imunify360 real-time scanner detects and removes malicious code from infected files or ones that can be used for malicious purposes (e.g., PHP web shell scripts). The web scanner validates every uploaded file shortly after it's stored. If the scanner determines that the content is malicious, it automatically cleans it from the system keeping the original file operable.

Finally, Imunify360 has an antivirus program built into its core functionality that runs in the background. It detects malicious files and immediately cleans them from the system. Administrators can also run an antivirus check to verify that files on the server are legitimate. In addition to scanning files, the scanner is capable of searching WordPress databases for malicious injection of JavaScript, iframes and other malicious code that could be used for account takeovers, cross-site scripting (XSS), or redirects.

CONCLUSION

It’s critical for shared hosting providers to monitor all activity on their servers, or it can quickly turn into a situation where hundreds of clients are affected by just a few hacked sites. Malware takes a huge toll on server resources, and it can result in crippling performance degradation on other customer websites when just a few are hacked.

Imunify360 preserves server resources by blocking many of the common attacks in the wild, especially those targeting WordPress. With your servers protected from malware, CPU usage drops, customers file fewer support tickets, and happier clients means better profitability for your services.

Try Imunify360 Security suite for free for 14-days and forget about malware on the server.

Ensure your server’s security now!