CASE STUDY

KEEPING FULL CONTROL OF YOUR CPU USAGE AS A HOSTING PROVIDER

Web host providers understand the importance of managing CPU usage on a server, but what they might not realize is that malware and CPU usage spikes are interconnected, making cybersecurity a critical part of server administration. In a shared hosting environment, malware could infect thousands of sites.

Without the right monitoring and mitigation techniques in place, the accumulation of hacked sites could cause performance degradation leaving the entire server unusable for customers and causes loss in revenue.

ABOUT GUZEL HOSTING

Guzel Hosting is one of the biggest web hosting companies in Turkey. They host over 100,000 websites with shared hosting services. They work hard to ensure that customer sites run efficiently, and servers run at optimized performance.

After Guzel Hosting implemented Imunify360, all shared server loads went down dramatically, which means that Guzel Hosting makes a profit from CPU power. Customer websites are no longer hacked often anymore. Because of the better performance and fewer hacking incidents, customers are happier with service. Guzel Hosting believes that Imunify360 is as important as control panels when it comes to service, mitigation of attacks, and preservation of CPU resources.

Because of Imunify360, Guzel Hosting can make a profit on customer work and backup restoration tasks.

güzelhosting
Web Hosting ve İnternet Hizmetleri

OPTIMIZATION AND PERFORMANCE WITH IMUNIFY360

Malware authors continually evolve their code to overcome the latest cybersecurity defenses. In a shared hosting environment, numerous sites could be hacked without the site owner's knowledge. By allowing sites to continue hosting malware, server CPU could spike to usage that affects all other sites on the server.

To add to the shared hosting frustrations, many site owners work with common content management systems such as WordPress. Research shows that 40,000 of the top WordPress sites are vulnerable to hacker attacks.

40 000

of the top WordPress sites are vulnerable to hacker attacks

WordPress developers consistently upgrade the software to remediate these vulnerabilities, but site owners must install the update. This requires always authenticating into the dashboard to ensure the software has the latest updates installed.

Generally, the WordPress core software is secure, but plugins can be written by any third-party developer and uploaded to the marketplace or distributed on sites where developers can sell their code.

Plugin creation is lucrative for many developers, but it's not common for small developers to have their code professionally pen-tested for any vulnerabilities.

This means that sites with the plugin installed would be open to attacks.

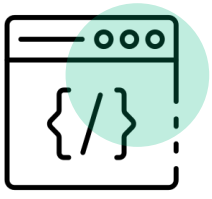
For Guzel Hosting, hacked sites were a major issue for server CPU usage. The high CPU usage affected all aspects of the server including its performance and other customer sites. After installing Imunify360, shared server loads dramatically dropped and allowed the hosting company to monetize their server resources.

WHY DOES MALWARE DRAIN CPU RESOURCES AND HOW IMUNIFY360 HELPS?

To understand why malware affects CPU usage, it's important to know the types of attacks launched against servers and hosted websites. Several attacks will show a spike in resource usage and affect server performance.

The first one is a denial-of-service (DoS). Most DoS attacks are distributed, meaning an attacker sends a signal to several hundreds or thousands of hacked devices to flood the targeted server with traffic. The requests are standard web traffic, but the server does not have the resources to handle the gigabytes of traffic sent its way..

Another common attack is brute-force password guessing attempts. Brute-force attacks can be launched against any page that requires authentication. Bots will use a downloaded list of credentials to determine if a user's password is valid. Bot traffic is also common in attack takeover (ATO) requests where credit cards must be validated before selling them on darknet markets or used in financial fraud. With any bot traffic, the attacker sends numerous requests per minute, which can overload server CPU usage.



In many attacks, malware authors inject malicious scripts into pages or the site structure. The code can do anything, but for CPU spikes it usually creates backend activity triggered by the attacker. For example, the attacker could use the server for its email messaging resources to send spam email to thousands of users. It could also be used to send malicious SQL (SQL injection) to identify vulnerabilities with site databases.

WHY DOES MALWARE DRAIN CPU RESOURCES AND HOW IMUNIFY360 HELPS?

The aforementioned attack types must be mitigated to avoid critical resource spikes, and Imunify360 has the ability to stop each one.

IMUNIFY360 WILL STOP:

Vulnerability exploitations

Malware uploads

Sensitive data access

Website scraping and scanning

Web SPAM

Many other web threats

Imunify360's advanced firewall with cloud-based heuristics protects against all types of brute-force attacks targeting FTP, SSH, SMTP, hosting panel logins, and more. It reduces server load caused by DoS and brute-force attacks and malware running on infected sites. It eliminates the resources used by malware and returns it to the users that need it — your customers.

Much of the defense provided by Imunify360 is its advanced Web Application Firewall (WAF) based on ModSecurity with proprietary rules, a real-time blacklist (RBL), and cloud heuristics updated daily with the latest threats and offers a negligible false-positive rate. The WAF protects from malicious requests sent to web applications and APIs.

CONCLUSION

Imunify360 takes care of several sophisticated attacks that create excessive CPU usage. It will stop brute-force attacks, denial-of-service, and the botted traffic that could cause performance degradation on your server. The results will let host providers keep full control of their server's CPU usage and reduce support ticks, increase profitability, and maintain customer satisfaction.

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

Keep your servers secure now!