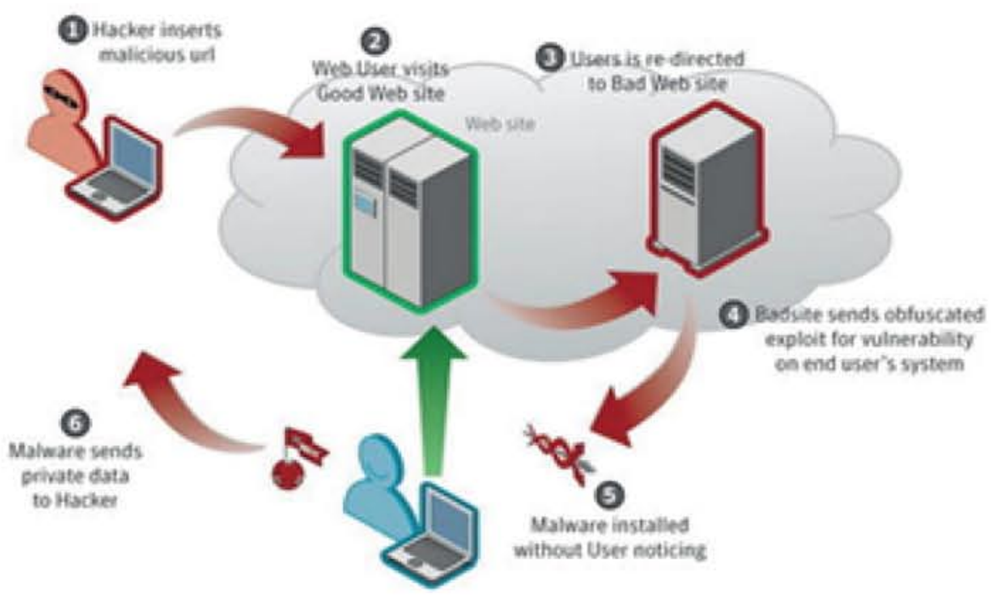
Malware Monitoring Solution Powered by StopTheHacker

Understanding the threat of malware distribution

Threat of Malware

To understand the growing need for a malware monitoring solution it's important to understand the growing threat of "drive-by downloads". Drive-by downloading is a hacker technique resulting in the unauthorised download and installation of unwanted malicious software (malware) onto the client PC of anyone visiting the website. It is designed to steal information from Internet users by forcing them to automatically download malicious software (malware) without their knowledge or consent.



For the Website Visitor

A malware attack can lead to stolen information such as online banking credentials and credit card details. Theft of personal information in this manner also leads to increased incidences of email hijacking, fraudulent access to social networking sites and identity theft.

For the Website Owner

Search engines such as Google flag and blacklist websites that are identified as hosting malware. Search traffic is driven away due to warnings search engines post prior to entering the website. The site may even be completely removed from search results altogether; damaging the business reputation, decreasing website traffic and ultimately having a detrimental effect on business revenue.

Recent Malware Case

In August 2010, malware experts identified an infection in the Network Solutions infrastructure – a widget housed on Network Solution pages. The widget took advantage of an Internet Explorer vulnerability and resulted in the Koobface malware (a virus that "phones home" for further instructions) being widely distributed. The press identified the widget as being distributed via millions of landing pages reserved for parked domains.

Malware Monitoring Solution

ZNetLive's malware monitoring solution is powered by StopTheHacker, Which helps website owners avoid a doomsday situation by providing monitoring for malicious code injection and drive by downloads. By giving duemalicious code to facilitate timely removal, the service protects both thecustomer and corporate reputation

Provided as a cloud-based service, StopTheHacker's non-intrusive solution crawls a website and actively analyses the content on each page for signs of compromise. StopTheHacker uses numerous advanced and unique techniques to ensure known and unknown, malicious codes are identified quickly and even the most advanced malware distribution techniques are efficiently identified.

StopTheHacker Features

- Fully automated non-intrusive scans
- Weekly, daily or hourly scans, depending in SSL Certificate type purchased
- Automated email alerts should your site become blacklisted or affected by malware
- Details of injected code snippet to facilitate timely removal of malware and code-level remediation
- SaaS based portal to fully view reports and manage website domain
- Trust Seal to increase visitor confidence

Contact us today to learn more and to discuss your individual needs.

Contact ZNetLive's SSL Specialists

+91-8875002200 ssl@znetlive.com www.znetlive.com/sslcertificates