ZNetLive Malware Monitoring

Introduction

The criminal ways of distributing malware or malicious software online have gone through a change in past years. In place of using USB drives, attachments or disks to distribute viruses, hackers now use a technique called ‘drive by download’ to disperse virus. Drive by download is designed in a way to take advantage of a browser, operating system or an app that has a security flaw or has expired. It then introduces malicious codes into unsuspicious websites. These codes infect the PC of any visitor who lands on that website, triggering an unintentional download of a virus or a malware without clicking anywhere.

If your system gets infected by a malware once, it can pose a serious harm by stealing passwords and corrupting data, eavesdropping to steal credit card details etc. It can also turn an infected machine into ‘zombie’ which means forcing it to join a ‘zombie force’ responsible to launch massive denial of service attack, without its knowledge. Search engines such as Google do not approve of malware attacks. If a website is detected as the one responsible for distributing viruses, Google flags it as dangerous and the website ends up being blacklisted. This leaves a bad impact on company’s reputation.

In this white paper, we have explained what malware is and how it affects a website. We have also thrown light on ZNetLive’s Malware monitoring service to let you know how it ensures security of your website visitors and hence guards the position of your company.

Malware Monitoring

What is Malware?

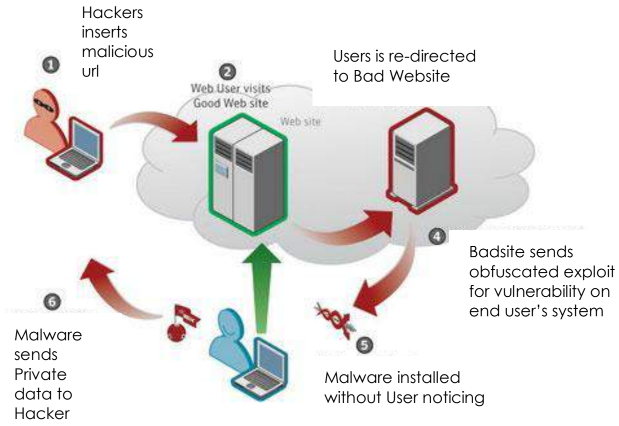
What is the need of malware monitoring service and why is it essential to have it on the website? To understand the basics behind this, first let’s take a look at threats presented by “drive by downloads. It is a technique designed to steal the information from internet users by deceiving them into downloading the malware automatically, without prior consent or their knowledge. Drive by downloads is responsible for unapproved download and installing unwanted malicious files. This includes using several techniques that are defined below.

- Adding an iframe to the hosted web page which is invisible to human eyes
- It directs the visitor’s browser to a server that’s transmitting exploits designed specifically to break the web browser through recognized vulnerabilities.

- It then uses the broken browser for downloading and installing malware/viruses on user's system.

The motive behind designing a malware could be criminal, political or mischievous. Some of the purposes are given below:

- To hoax a user into buying something that he/she doesn't want to
- Sending spam emails
- Launching zombie attacks on other computers/networks
- Distributing malware
- To steal account numbers, corporate secrets, passwords or any other sensitive information.


1
Hackers inserts malicious url
2
Web User visits Good Web site
Web site
Users is re-directed to Bad Website
4
Badsite sends obfuscated exploit for vulnerability on end user's system
5
Malware installed without User noticing
6
Malware sends Private data to Hacker

Viruses, Trojans, rootkits, spam bots, spyware etc. are the kinds of malware. Usually the websites are prone to the injection of malicious code. When these websites fall prey to such attacks, the first negative impact is borne by visitors because the malware installed on their PC intends to steal their personal information such as online banking details, credit card information. Sometimes, malware can give complete control of target's PC to the hacker.

It harms the website's reputation as well. When visitors realize that their data security is at risk due to visiting a particular website, they begin complaining. Search engines such as Google takes notice of this and flags or blacklists the website for hosting malicious content.

By visiting an infected websites, visitors can easily get infected without clicking anywhere or downloading anything. There could be any intention behind designing the malware including monitoring keystrokes, stealing password or personal information or to turn the infected machine into a 'zombie'. Zombie machines are used to launch well-coordinated attacks to overload servers or network. This has emerged as a major problem with many noteworthy attacks such as Aurora (DDOS attack originating from China against many IT companies) and Payback (DDOS attack asrevenge against previous WikiLeaks suppliers) making headlines.

ZNetLive Malware Monitoring

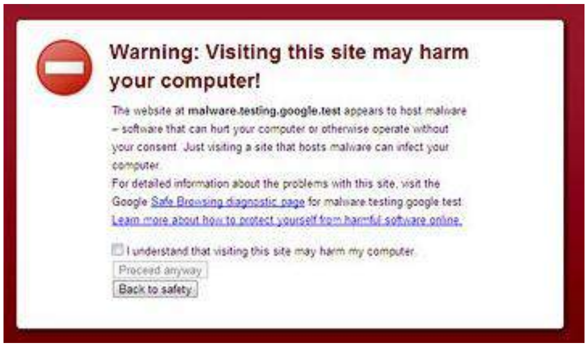
Blacklisting

Acting sternly against the growing issue of malware distribution, presently Google is blacklisting 9500 websites each day that are identified as distributors of malware software.

When Google flags a website as blacklisted, it causes negative impact as it drives traffic away from it because Google posts warnings in its search results against visiting it, or even worse, removes it from its search results. This can bring down the number of website visitors from thousands of visitors per day to zero.

Whether the website owner is purposely distributing malware or not, Google search results and web browsers like Chrome or Firefox will display a message warning visitors of the possible threats of visiting the website.

Remedial time, which is the time taken by Google to remove a website from blacklist is not defined yet. According to the reposts in the forum, it could be weeks or even months.



Warning: Visiting this site may harm your computer!

The website at **malware.testing.google.test** appears to host malware – software that can hurt your computer or otherwise operate without your consent. Just visiting a site that hosts malware can infect your computer.

For detailed information about the problems with this site, visit the Google Safe Browsing diagnostic page for malware.testing.google.test

Learn more about how to protect yourself from harmful software online.

□ I understand that visiting this site may harm my computer.

Even renowned websites such as cnn.com could not escape being blacklisted and was compromised as a website distributing malware.

Once a website is blacklisted, it is very likely that its domain name will find a place in stopbadwar.org. It is a central database of domains that are infected and referenced by service providers and applications. Getting blacklisted could mean a huge loss of business and reputation to a website owner. It can lead to a downfall in traffic and eventually revenue loss. The corrective measures needed to remove the domain name are slow and costly and does not come with a guarantee of regaining the previous ranking.

Malware in your Environment

If you have a website, it is vulnerable to malware code injection. No matter if you have a dedicated server or use shared

ZNetLive Malware Monitoring

hosting, your website is constantly at the risk of exploitation.

Websites that use hosted space need to be vigilant of the threat of compromise to their infrastructure. Typically, hackers seek the greatest economy of scale to attack infrastructure of a hosting company which results in highest return on effort. In August 2010, an infection was detected by malware experts in the Network Solutions infrastructure- a widget on NetSol pages. The widget took advantage of vulnerability in the Internet Explorer which led to wide distribution of Koobface malware (a virus that phones home). It was identified that the widget was distributed via millions of landing pages that were kept for parked domains.

As explained by NetSol, the malware was distributed via a blog of NetSol.

"Our security Team was alerted this past weekend to a malicious code that was added to a widget housed on our small business tips on Network Solutions' under construction pages. We have removed widget from those pages and continue to check and monitor to ensure security. The number of impacted pages that have reportedly publicly over the weekend are not accurate. We're still investigating the number of web pages affected.

If you have downloaded the GrowSmartBusiness widget to your website, we recommend you delete that widget and scan your site for malware."

ZNetLive's Malware Monitoring Solution

ZNetLive's malware monitoring solution is powered by StopTheHacker. It provides monitoring service against malicious code injection and drive by downloads. When an infection is detected it gives out a warning as well as adequate details to timely remove the injected code. This way it protects the customers from unintentionally downloading any malware as well as the reputation of a website.

This non-intrusive software crawls the website and carries out an active analysis of content on every page of the website for any signs of compromise. Several advanced and unique techniques are deployed by StopTheHacker to ensure quick identification of known and unknown malicious codes and most advanced malware distribution techniques. Visitors are immediately notified via an email if an infection or a malicious code is detected in the website to infect end users PC using drive by downloads.

ZNetLive's malware monitoring service provides protection to business and customers against malware code injection. The service is included as standard with all ZNetLive SSL Certificates along with:

ZNetLive Malware Monitoring

- Hourly/daily/weekly scans on the website: depends on the type of SSL Certificate purchased
- Detailed information of the injected code to timely remove the malware and code level remediation
- Trust seal to enhance visitor's confidence
- Completely automated non-intrusive scans
- SaaS based portal to view full reports and managing website domains
- Automatic email alerts in case your site is affected by a malware or gets blacklisted

About GlobalSign

GlobalSign has been in the business of providing SSL Certificates since 1996. It is one of the world's first CA (Certificate Authority). It offers services in multiple languages and its technical support is present in places like London, Brussels, Boston, Tokyo and Shanghai.

GlobalSign is a leader in public trust services the market of SSL Certificates. Its Certificates include SSL, Code Signing, Adobe CDS Digital IDs, Email and Authentication, internal PKI and Microsoft Certificate Service etc. GlobalSign's root CA Certificates are trusted and recognized by all the major web browsers, operation systems, internet applications, email clients and all the mobile devices as well.

About ZNetLive

ZNetLive is India's leading web hosting provider which has been providing its services since 2001. At ZNetLive, our goal is simple- our customers' online success. And we touch this goal every day, providing Domains Registration, Web Hosting, Business Email, Websites, Business Apps and more, to our diverse global customer base, who make us what we are.

Our state of the art infrastructure and datacenters in Washington, Seattle, Dallas, Mumbai and Bangalore are second to none, we are successful because we promise, and deliver 99.9% network uptime to every single customer of ours. We've been in the industry since 11 years and our experience shows in the finesse of our unparalleled products.