How do Websites get Hacked and Blacklisted

Overview

Websites today are used for various purposes: to project an image for a corporate persona, to provide a view into the personal side of people, to allow shoppers to buy goods off websites easily and comfortably, to provide entertainment, and many more uses. With increased functionality such as allowing users visiting a site to comment on websites, the content becoming dynamic, changing according to the taste of a user and such ; the computer code that powers these interactive and informative websites becomes extremely complicated.

As a result of these complex interactions, web designers prefer to save development time when constructing websites and prefer to use pre-packaged tools for designing and implementing websites really quickly. These third party tools, like WordPress, Joomla, Django, Drupal and more provide the flexibility that web designers need, while reducing the headache associated with managing the complex interactions of a website.

Since websites are becoming more complex, and a lot of the website administrators do not usually understand what is going on under the hood when third party tools are used, this leads to security vulnerabilities getting introduced and allows hackers and bots to break in and infect websites.

Every day 6,000 websites get blacklisted by Google and other search engines. Once blacklisted, all modern browsers like Internet Explorer, Firefox, Safari will block access to the site. This leads to drop in visitors, sales and destroys the reputation of the site.

What kind of interactivity on a website causes vulnerabilities?

Features such as allowing comments on blog posts, forms to accept emails of users for newsletters, login pages with a username and password field, and basically any input that the user has control over, can be used to infect a site. Sometimes computer code associated with drop down menus, and other javascript based interactions (such as dynamic image resizing) can also be a cause for infection.

How do malicious hackers exploit these vulnerabilities?

Malicious hackers exploit vulnerabilities like SQL injection and Cross Site Scripting, primarily, to infect websites by pushing in input that is not expected and hoping that the computer code responsible for handling the input will be weak enough to let the malicious input go through and provide a way to infect the website. Think of a hacker as using a Trojan horse. Your website expects a nice toy, while the toy (the horse), contains malicious computer code inside it.

Can all vulnerabilities be fixed?

Yes, theoretically. Realistically though, all vulnerabilities can never be fixed. This is because every week a new vulnerability is discovered in software powering websites. Unless your website is managed by a dedicated team of security experts, it is very likely that your website will always be vulnerable.

How can you protect your website?

You can protect your website, your visitors and your reputation by employing website scanning and monitoring tools like StopTheHacker. StopTheHacker's SaaS based Health Monitoring service, requires no software installation and you can protect your site in less than 5 minutes. In case your website gets infected, you will get detailed alerts about how to remove web-malware from your website and prevent the reputation of your website from getting tarnished.

For more information, please visit StopTheHacker.com and have a look at our blog (www.stopthehacker.com/blog) articles and our educational videos around malware and website security (www.youtube.com/stopthehackervideo)