Finding Hacked Websites!

Posted on August 29, 2019

If you are a website administrator, web-business owner or even a compulsive blogger, waking up one fine day to realize that your website has been hacked can become your worst nightmare. The internet is becoming more and more complex by the minute; in this ever-changing environment the task of ensuring that your website is free from malware and viruses, as well as protecting your domain from any unauthorized intrusion, is taking on an increasingly complicated nature that requires constant vigilance and professional care.

But what are the simplest signs that your website has been hacked? Let's find out.

Explicit Website Hacks

Sometimes, realizing that your website has been hacked can be as simple as not being able to access it. This usually happens when your domain name and Whois server accounts have been compromised by a malicious entity. Such hacks can also take the form of website defacement; in such a scenario your website content is usually defaced or replaced by objectionable material or entirely unrelated content. Sometimes, you may find that your domain name is now linked to a web property that has nothing to do with you.

A hacked website can cause severe damage to the credibility and authenticity of your website. Interestingly, hacks which actually allow you to recognize that your website has been compromised may be tackled relatively easily as they allow the opportunity of instant detection and rectification. Sophisticated website hacks, however, are harder to detect and correct.

The Hidden Hack

Most website hacks won't allow you to understand that your website has been hacked at all. Advanced hacking techniques are designed in a manner which makes it very difficult to detect them. As a result, hackers can continue with their activities unhindered. Such website hacks, which may target Domain Name Server (DNS) or Whois servers, are serious breaches. Using these routes hackers can compromise the integrity of your website in any of the following ways:

- Collect information regarding your website.
- Steal the credentials and monitor the usage patterns of your website visitors.
- Install and spread malware to other computers and websites connecting to your web property.
- Divert your website visitors to other malicious sites.

These are only some of the ways by which such hidden website hacks can harm your site. If not addressed in a timely manner, such attacks can easily destroy the credibility of your website or online business.

How To Detect A Hacked Website?

While explicit hacks make themselves pretty obvious, detecting advanced hacks such as attacks on Whois servers are best handled by professionals who are experienced in such matters. Security experts take into account varied factors and employ techniques to determine if a website has been hacked. Some of these are listed below:

- **Whois Record Anomalies-** Sudden changes in your Whois records, as well as domain expiry, can lead to your website being compromised. In case you notice any change in the information of your Whois records, or have neglected to renew your domain registration for extended time periods, then your web property can become a prime target for hackers. To prevent such compromises, make sure your Whois data is properly updated and you monitor your valuable domains.
- **DNS Monitoring**- The DNS service is another common target for hackers. DNS runs behind the scenes and hence is easily ignored. Furthermore, DNS configurations are often difficult to fortify against attacks. This leads to cyber-criminals using exploits such as Cache Poisoning and DNS Resolver Modifications to redirect traffic to illegitimate destinations. Keeping your DNS software up-to-date and restricting zone transfers can be effective ways to guard against such hacks.

- **Finding Malware Signatures-** Experts can detect whether your website has been exposed to malware by scanning your site's Whois server and associated resources for anomalies and malware signatures. Updated malware detection techniques allow prevention as well as timely containment in case of an infection.

- **Checking Source Files-** Often, website hacks can manifest themselves in the form of anomalous code in the source files of a website. Therefore, a thorough examination of the source code can reveal any problems that may be lurking beneath the surface. Hackers often insert malicious links inside source code. A professional analysis can help detect any such problems.

- **Monitoring Site Traffic-** The nature of a website's traffic can often be a good indicator of whether the site has been compromised or not. Certain website hacks often result in unusual fluctuations in website traffic. If such spikes and drops in website traffic become intense, it may be a sign that the website has been hacked.

Protecting Against Future Attacks

Once the website hack has been detected, the infected files must be separated from the clean ones and then scrubbed for removing the malicious code. Then they can be re-integrated into the website. Doing this requires professional expertise, and backups of all resources should be maintained to guard against possible mishaps during the recovery process.

The job of protecting the website does not end there, however. Websites and servers must be protected at all times using sound security practices. The traffic and usage patterns must be regularly monitored, passwords changed periodically, and Whois records must be protected to ensure privacy. Whois API, Inc provides Enterprise Tool Packages which can help you monitor & keep your domain name secure from malicious entities.

Final Thoughts

A hacked website can result in heavy losses for the website owner. However, by maintaining security best practices and using updated monitoring and protection tools, websites can be

guarded against cyber attacks.