

Is Your Site Hacker Proof?



It is not enough to just avoid websites that typically distribute malware or vicious programs on your computer. Your own web site might become a victim of being hacked and could be distributing malware to your best customers without you knowing it.

How Can This Be?

Hackers for the past year have been focusing on small websites to distribute malware because they are easy to hack into and they know that they can infect unsuspecting patrons on your web site that trust you.

While many thousands of small websites have been compromised I am glad to report that I have only witnessed this on only a couple of occasions with my clients.

The common element that I find is that they did not host with me. Every web host server is setup differently and generally by the personal tastes of the server administrator.

I am just lucky that I was able to find a host server for my clients that is operated by a large company with the resources necessary to thwart hacking attempts.

There are many places to host your website. Just beware that small hosting companies may not be able to react quickly enough or have the knowledge to protect your web site.

I know this first hand. I have used many different web hosting services and yes have been maliciously hacked. Go figure?

We have, at Site Mechanix, spent a considerable amount of time migrating hundreds of clients from server to server in order to find the best home for their web sites.

Vocabulary

malware = badware = spyware = deceptive adware

How Does a Website Get Hacked?

In order for your website to get compromised the hacker has to figure out your FTP (File Transfer Protocol) login information to get access to your web site files.

The target is usually the home page and is typically a file named "index.htm" or "default.htm". Because of this commonality it doesn't take long for a hacker to find your home page even if he doesn't know the exact file name. There are only a handful of possibilities.

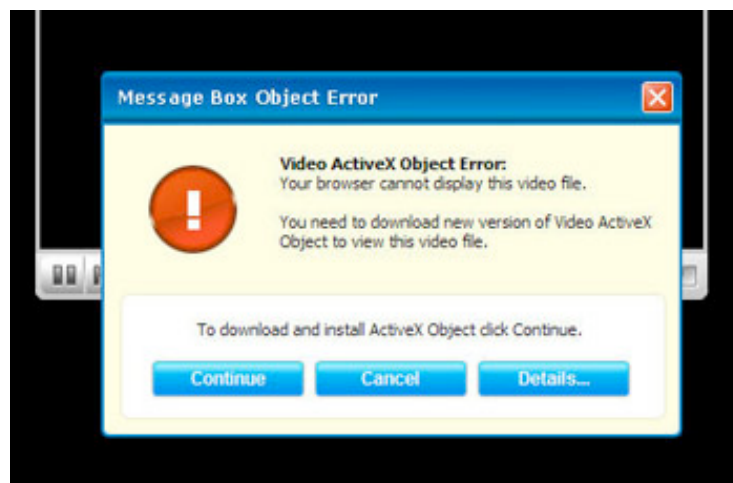
This isn't the only way to get into a website. Depending on the way the web host server was set up there may be many back doors to choose from.

Once he/she finds the file, they inject malicious code that can redirect or execute programs from another location.

Web page code is complicated and a hacker may even disguise the code so that it is not easy to locate.

This happened to one of my clients just recently. They sent me an urgent email saying that when someone clicks on their link on Google that the user is directed to an adult web site.

This was of course embarrassing to the web owner because they were a Christian entity. And of course they did not take my web hosting advice. They hosted the site on their own servers.



What the hacker was doing was redirecting users to a page that look like it was trying to show you a porno video but of course immediately shows an error saying that in order to see the video you have to upgrade your video player software.

It was tempting because you can hear the supposed video soundtrack of someone having sex you just couldn't see anything. It was all fake in an attempt to get you to download malware.

By clicking on the error message you would have been executing a program to install all kinds of malicious software on your computer including possibly a keystroke recorder.

I of course was not so tempted.

So What Can I Do to Protect my Website?

There is not much the web owner can do but rely on their web hosting company for support on this because of the complexity involved with managing a server.

There are a few things that you can do that can help.

Backup Your Website

It is wise to keep a copy of your final web site in different locations. The easiest way to clean up the injected malware code is to replace the web page with the original copy.

Unguessable Passwords

Hackers are very sophisticated and use software that trys every dictionary word until it gets in. Change your hosting account logins to something with upper and lower case characters that include numbers.

Clean Up Install Files

Many of the scripted CMS (Content Management System) websites like WordPress and Xoops leave install files in common location. These are files that the hackers are well aware of and will exploit them. They just need to be removed. The same goes for eCommerce scripts.

Form Verification

Many web sites use form-to-email scripts that allow users to send you an email through your site. Web site forms are also used to create new records on databases. This leaves a doorway to malicious scripts or simply bad html links to naughty sites. Your forms should have scripts that test for abuse and denies the malicious hacker or robot.

FrontPage Extensions

Sorry guys! Microsoft is really good at leaving us all out to dry and FrontPage extensions are no exception. It is suggested that FrontPage extensions are not used because they not only open your website to vulnerabilities but also to the 200 other websites sharing the same server. My advise is to be prepared for the day that FrontPage extensions are banned. This also depends on where your website is hosted.

Third Party Content

If your website contains ads as part of an advertising distribution network make sure it is with a reputable company. If they get hacked you and everyone on the network will be showing potentially damaging and embarrassing content.

Do Not Download Warez

Everyone likes free stuff but beware of free software. It is the best way for hackers to distribute nasty spyware and viruses.

Conclusion

For the most part you do not have to worry about your website. The purpose of this article is to inform and make you aware of potential danger.

We are all participating on the web more and more with online social networking and internet gadgetry. There are going to be more opportunities for people with too much time on their hands to trick you or find holes in your computer. We just have to stay informed.

Posted on December 1st, 2007 by Karl Knelson