

Forum:[Hack Forums](#)

Thread: [\[Information\] Antivirus Blacklists \[Information\]](#)

Cloud9™ - January 3, 2013, 10:56 pm

What are Antivirus Blacklists?

Ever since the rise of exploit packs such as Black Hole and Crimepack, many antivirus companies have a blacklist of websites or even IP addresses that are viewed with suspicion or disapproval. Usually these blacklists are built up by malware researchers such as Steven Burn from Malware Bytes and they're then used by antivirus companies. Most of these lists are actually available to the public and many antivirus companies surprisingly share collections amongst each other. You can find a blacklist checker here:

[URLVoid v2.1](#)

What happens when a domain is blacklisted?

If the domain you're using is on a blacklist, the visitor's antivirus will block them from visiting your website and you won't be able to potentially infect that visitor. You can bypass this blacklist with a domain change. If you're sharing a domain with other individuals who are using the same domain to spread, your chances of getting to infect someone drop even more. By purchasing your own hosting and your own domain, you'll have a less chance of being caught and your chances of infecting someone rise once more.

What happens when an IP address is blacklisted?

When you purchase hosting you have an IP address that will be linked to your hosting account. When you add a domain to your account, that IP address is referenced for that domain. In this example, we'll use 208.91.197.160 as our IP address. If I add a domain to my hosting account, let's say <http://www.myawesomewebsite.com>, that domain is now linked to our IP address 208.91.197.160. Now if we ping <http://www.myawesomewebsite.com>, it will return 208.91.197.160 as the IP address for that domain.

Well let's say 208.91.197.160 gets blacklisted, that means <http://www.myawesomewebsite.com> is blacklisted now. When a visitor visits our <http://www.myawesomewebsite.com> website, their antivirus will block that website since it has the IP address 208.91.197.160. Only way to bypass this blacklist is to get a new IP address and a new domain from your hosting company.

How can I remove a blacklisted domain or IP address?

Getting a domain or IP address removed from a blacklist is nearly impossible. In order for your domain or IP address to be removed from a blacklist, you're required to send an e-mail explaining why your website does not belong on the blacklist. You can usually find the e-mail address on the said blacklist website.

T?ny - January 3, 2013, 11:10 pm

great guide. Might help a few, sadly not me.