# Why Websites Get Hacked

By Nick Butler, Founder Of Ireland Website Design

I spend a good amount of time engaging with website owners across a broad spectrum of businesses. Interestingly enough, unless I'm talking large enterprise, there is a common question that often comes up:

Why would anyone ever hack my website?

Depending on who you are, the answer to this can vary. Nonetheless, it often revolves around a few very finite explanations.

## Automation is Key

Understand that the attacks affecting a large number of website owners in the prosumer category (a term I'm using to describe website owners in micro, small, and medium-sized businesses leveraging platforms like WordPress, Joomla and others) are predominantly automated.

The benefits of these automated attacks have not changed because they still provide the attacker:

- Mass Exposure
- Reduces overhead
- Tools for everyone regardless of skill
- Dramatically increased odds of success

It is not to say that these attacks are never manual, but for the mass majority, automated attacks are what we see during the initial phases of the attack sequence. When I say **attack sequence**, I am referring to the order of events an attacker takes to compromise an environment.

A very simple illustration of the sequence would look something like:

1. Reconnaissance
2. Identification
3. Exploitation
4. Sustainment

The attack sequence can have varying levels of complexity depending on the group of attackers. When working with everyday websites, the most effective way to affect the largest number of websites at any given time would be with the deployment of scripts and bots during steps one and two. Although not always a manual process, steps three and four often have a tendency to have more manual elements to them, although many can be automated as well. While thinking of how these attacks occur, it is important to note the two forms of attack categories **– attack of opportunity** and **targeted attack**.

### Attack of Opportunity

Almost all prosumers fall within the realm of opportunistic attacks. Meaning that it is not any one individual that is intentionally trying to hack your website, but rather a coincidence. Something about your site was caught by the trailing net as they randomly crawled the web. It could have been something simple, like having a plugin installed, or maybe displaying the version of a platform.

In our analyses, we have found that it takes about 30 – 45 days for a new website, with no content or audience, to be identified and added to a bot crawler. Once added, the attacks commence immediately without any real rhyme or reason. It can be any type of website, the only commonality is that it is connected to the web.

These crawlers then begin looking for identifying markers. Is the website running one of the popular CMS applications (i.e. WordPress, Joomla)? If so, is the website also running any exploitable software (i.e. software vulnerabilities or bugs in code)? If the answer is yes, then the site will be marked for the next phase of the attack, exploitation.

The sequence of events can happen in a matter of minutes, days or months. It is not a singular event. Instead, it occurs continuously, always scanning for changes or updates. It is automated, therefore, once your website is on the list it will just continue trying.

### Targeted Attack

This is often reserved for the larger businesses but not always. Think of the NBC hack in 2013, or the recent Sony hack. There are many examples of these types of hacks lately, and it is apparent why they would be targeted. The level of effort it takes to gain entry into these environments is exponentially more difficult yet rewarding. That being said, a very common form of targeted attack, known as a Denial of Service (DoS) attack, is when the attacker works to bring down the availability of your site. This is popular with competing businesses. They can be deployed against big or small sites, and can be driven by competition or pure boredom and need for challenge. These attacks can range from very simple to very complex.

## Hacking Motivations and Drivers

Now that we have a better appreciation for the **how**, let's turn our attention to the **why**– why websites get hacked?

## Economic Gains

The most obvious of the reasons is economic gain. This manifests in attacks known as **Drive-by-Downloads** or **Blackhat SEO** campaigns. As you might imagine, these are attempts to make money from your audience.

A **Drive-by-download** is the act of deploying a payload (i.e. injecting your website with malware) and hoping to infect as many of your website visitors. Think of your mom or dad visiting your website and the next thing you know, they are calling you because they installed a fake piece of software you recommended on your website, but this time their bank accounts were drained. Scary, but very real and very devastating.

**Blackhat SEO spam campaigns** are not as devastating, however, in many instances more lucrative. This is the game of abusing your audience by directing them to pages that generate affiliate revenue. This form of attack runs rampant in the pharmaceutical space, but has extended into other industries like gambling, fashion and others. What they do is inject links through your website, sometimes you see them. Sometimes you won't. On the contrary, when it comes to search engines like Google or Bing, they see everything and once those links make it onto the Search Engine

Results Pages (SERPs) the attackers begin generating revenue from your audience.

### System Resources

There is one motivator, the use of your resources, that many don’t talk about. These are things like bandwidth and physical server resources. I break this out as its own motivator, but it’s also a group under economic gain. The business of farming system resources is big business and a huge motivator for many cyber groups; they’re able to not only use it as part of their own networks, but build a leasing environment off yours.

You have likely heard of large botnets that I have also referenced above. Botnets are nothing more than interconnected systems across the net. They can be desktops, notebooks and even servers – similar to your webserver employed to perform tasks simultaneously. These can include Denial of Service attacks, brute force attacks, or even some of the automated attacks we’ve gone over.

These attacks target your system resources and are dangerous mainly because of their ability to attack without you – the website owner – even realizing it. You go about your day with no worries, your website appearing to be in good standing and no complaints. Then one day, out of the blue, your host shuts you down, your usage bill is through the roof, or you receive a notice from the authorities about your hacking attempts.

### Hacktivism

This motivator is perhaps the hardest to contend with and understand. Similar to others, the drivers for these attacks are monetary or abusive. However, they are often protesting a religious or political agenda; showing off to peers within the hacking community, using it as bragging rights.

A very common form of this can be identified with Defacements. The point of these attacks often comes down to awareness and can be combined with other attacks, but in our experience they are often benign and create more embarrassment to the site owner than affecting their users.

### Pure Boredom

Something that always catches folks off guard is the idea of people attacking a website out of sheer boredom and amusement. It's unfair to say they are always young, but a good percentage of the time these attackers are computer-savvy teens with nothing else to do.

There really isn't much to say about this, other than, *put your kids into sports!!*

### Good Security Begins with Good Posture

It's easy to feel overwhelmed by some of this information, but it is our belief that the best tool you have at your disposal as a website owner is knowledge. Driving your head into the proverbial sand doesn't make it disappear but rather amplifies the impact. I assure you that attacks happen more often than not, and Google agrees! They blacklist close to 10,000 sites a week for malware and flag over 20,000 sites for phishing every week.

Bruce Schneider likes to say:

> As a species, we are risk averse when it comes to gains, but risk seeking when it comes to loss.

This statement becomes apparent when I speak with website owners and they say, "I've had a website for 10 years and never been hacked. I don't need to worry about it." Those owners always make for the most interesting and painful conversations when the hack does occur.

I like to think of website security in the form of posture. It is through good posture that you position yourself for success.

Remember, security is not about risk elimination, but rather risk reduction. Risk will never be zero. You can, however, employ tools and steps to reduce it where you can so as not to become part of the statistic.