Hacking Back – Why It's a Bad Idea

Let's face it, cyber crime is never going away and there will always be someone out there looking to exploit people, breach company networks and expose government secrets. However, it has been suggested by some that it's time for a new approach, one where law enforcement and organisations work together to go on the offensive against cyber criminals and instead of just accepting a beach, they should be hacking back.

Everyone has a responsibility when it comes to cybersecurity and companies around the world need to be doing all they can to ensure the safety of their networks, data and their customers. The idea of retaliation is a natural reaction to any wrong doing, but when it comes to hacking back it brings up a number of ethical and legal problems.

In our opinion, it's a bad idea. And we'll tell you why.

Playing Catch Up

Even the largest enterprises, with large security teams and big budgets, are playing catch up with respect to the cutting edge of cybersecurity and software lifecycles. The sheer volume of incoming threats and newly published vulnerabilities is overwhelming, and most companies struggle to keep pace with evolving security best practices.

For example, when Equifax were breached, and 145.5 million records stolen, it took attackers just three days from the release of a security patch to create an exploit, weaponise it, launch an attack and successfully exfiltrate a vast amount of data undetected. The Equifax security team are probably operating efficiently most of the time, but on this occasion they were just too slow to patch.

Eight of the top ten most prolific strains of malware target unpatched systems, so evaluating, prioritising and installing security patches should be a top priority. Yet, thousands of companies are compromised in this manner every day. It should be noted that updating and patching software is only one component within a multi-faceted security policy needed to provide an organisation with a robust and mature posture.

None of this should be surprising because the odds are heavily stacked against defenders. Security teams must find and remediate every single vulnerability in their organisation, at speed, in a landscape of ever evolving threats. An attacker need only find a single mistake, or oversight and exploitation can occur.

The priority therefore must be focused on getting the basics right. If you're not doing that adequately, and most companies have weaknesses despite their best efforts, then diverting resources to go after your attackers is most likely a poor use of time and budget.

It should also be noted, hacking back does not prevent an attack, it takes place after the fact, so could be likened to revenge or vigilantism. There are many grey areas, for example,

what constitutes an attack? Who determines when attacking an attacker is acceptable and what severity of action is appropriate?

Whodunnit?

A further complication is the difficult nature of positive attribution. It is easy for a threat actor to obfuscate their identity, or to include misleading signatures that frame a third party, so if you can't identify your attacker with any degree of certainty, should you really be attacking them?

This could lead to innocent people being targeted and compromised. It's not an approach that would be tolerated in the physical world, so why would it be acceptable in the online world? And suppose your security team did manage to successfully hack an attacker, what action would they take? Shut their computer off? Delete all their files? Infect them with malware? Capture their personal data? All of these actions are problematic, and for the most part, illegal.

Our advice would be to focus all resources available at improving defensive security measures and implementing a rigorous testing schedule to identify and fix any vulnerabilities that have found their way into your business.

Hacking back isn't the only way to deter cyber criminals from attacking your business. To find out more about our methods, contact us today.