webroot.com

The Truth about Hackers, in Black and White (and Grey) | Webroot

Grayson Milbourne

7–8 minutes

Did you know there are three primary types of hacker—white hats, black hats, and grey hats—and that there are subcategories within each one? Despite what you may have heard, not all hackers have intrinsically evil goals in mind. In fact, there are at least 300,000 hackers throughout the world who have registered themselves as white hats.

Also known as ethical hackers, white hats are coders who test internet systems to find bugs and security loopholes in an effort to help organizations lock them down before black hat hackers, i.e. the bad guys, can exploit them. Black hats, on the

other hand, are the ones we're referring to when we use words like "cybercriminal" or "threat actor." These are hackers who violate computer security and break into systems for personal or financial gain, destructive motives, or other malicious intent.

The last of the three overarching types, grey hat hackers, are the ones whose motives are, well, in a bit of a grey area. Similar to white hats, grey hats may break into computer systems to let administrators know their networks have exploitable vulnerabilities that need to be fixed. However, from there, there's nothing really stopping them from using this knowledge to extort a fee from the victim in exchange for helping to patch the bug. Alternatively, they might request a kind of finder's fee. It really depends on the hacker.

So, hackers can be "good guys"?

Yes, they absolutely can.

In fact, there's even an argument that black hats, while their motivations may be criminal in nature, are performing a beneficial service. After all, each

time a massive hack occurs, the related programs, operating systems, businesses, and government structures are essentially shown where and how to make themselves more resilient against future attacks. According to Keren Elezari, a prominent cybersecurity analyst and hacking researcher, hackers and hacktivists ultimately push the internet and technology at large to become stronger and healthier by exposing vulnerabilities to create a better world.

Why do they hack?

The shortest, simplest answer: for the money.

While white and grey hat hackers have altruistic motives in mind and, at least in the former group, are invested in ensuring security for all, the fact of the matter is that there's a lot of money to be made in hacking. The average Certified Ethical Hacker earns around $91,000 USD per year. Additionally, to help make their products and services more secure, many technology companies offer significant bounties to coders who can expose

vulnerabilities in their systems. For example, Apple offered a reward of $1.5 million USD last year to anyone who could hack an iPhone to find a serious security flaw. There are even groups, such as HackerOne, which provide bug bounty platforms that connect businesses with ethical hackers and cybersecurity researchers to perform penetration testing (i.e. finding vulnerabilities). Multiple hackers on the HackerOne bug bounty platform have earned over $1 million USD each.

And for black hats, theft, fraud, extortion, and other crimes can pay out significantly more. In fact, some black hats are sponsored by governments (see the Nation-State category below).

You mentioned subtypes. What are they?

As with many groups, there's a wide range of hacker personas, each with different motivations. Here are a few of the basic ones you're likely to encounter.

Script Kiddies

When you picture the stereotypical “hacker in a hoodie”, you’re thinking of a Script Kiddie. Script Kiddies are programming novices who have at least a little coding knowledge but lack expertise. Usually, they get free and open source software on the dark web and use it to infiltrate networks. Their individual motives can place them in black, white, or grey hat territory.

Hacktivists

Ever hear of a group of hackers called Anonymous? They’re a very well-known example of a hacktivist group who achieved notoriety when they took down the CIA’s website. Hacktivists are grey hat hackers with the primary goal of bringing public attention to a political or social matter through disruption. Two of the most common hacktivist strategies are stealing and exposing sensitive information or launching a denial of service (DDoS) attack.

Red Hats

Red hats are sort of like grey hats, except their goal is to block, confound, or straight-up destroy

the efforts of black hat hackers. Think of them like the vigilantes of the hacker world. Rather than reporting breaches, they work to shut down malicious attacks with their own tools.

Nation-State

Remember earlier in this post when we mentioned that some black hats are sponsored by governments? That would be this group. Nation-state hackers are ones who engage in espionage, social engineering, or computer intrusion, typically with the goal of acquiring classified information or seeking large ransoms. As they are backed by government organizations, they are often extremely sophisticated and well trained.

Malicious Insiders

Perhaps one of the more overlooked threats to a business is the malicious insider. An insider might be a current or former employee who steals or destroys information, or it might be someone hired by a competitor to infiltrate an organization and pilfer trade secrets. The most valuable data for a malicious insider is usernames and passwords,

which can then be sold on the dark web to turn a hefty profit.

What are your next steps?

Now that you better understand the hacker subtypes, you can use this information to help your organization identify potential threats, as well as opportunities to actually leverage hacking to protect your business. And if you haven't already, check out our Lockdown Lessons, which include a variety of guides, podcasts, and webinars designed to help MSPs and businesses stay safe from cybercrime.

Beyond the educational steps you're taking, you also need to ensure your security stack includes a robust endpoint protection solution that uses real-time threat intelligence and machine learning to prevent emerging attacks. Learn more about Webroot® Business Endpoint Protection or take a free trial here.

About the Author

Grayson Milbourne

Sr. Intelligence Director

Grayson Milbourne is the Security Intelligence Director at Webroot, Inc., part of OpenText Security Solutions, where he has worked for the past 17 years. In his current role, Grayson works to support the Product Management team to ensure Webroot products are effective against today's most advanced threats.