Meet the hacker: GangsterSquad

BY INTI DE CEUKELAIRE · JANUARY 7, 2022 · LAST UPDATED ON MARCH 6, 2025

Have you ever wondered what it would be like to be a cybercriminal? Well, if you're an ethical hacker, you must go beyond imagining and put yourself into the shoes of one.

Not all hackers are inherently bad. However, they get a bad reputation from mainstream media. Despite having the same skill sets, education, and creative way of thinking, malicious hackers have taken claim over the title "hacker". Luckily, perceptions are changing.

Today, ethical hackers, also known as white hat hackers, are seen by many to be the backbone of IT security testing. By being on the ground 24/7, businesses can protect their digital assets continuously and at scale. Ethical hackers are essentially the Sherlock Holmes' of the cybersecurity world, except they solve the case before it even happens.

But who are these so-called Sherlock Holmes'? And what drives them to use their expertise for good? To find out, DutchCowboys talked to GangsterSquad (@StanFaas), an ethical hacker who uses bug bounty platforms to hunt for security vulnerabilities on behalf of businesses.

Hi GangsterSquad! Tell us, what drew you to hacking?

I've always been interested in hacking. Back in 2011, I started playing some Capture-the-Flag (CTF) events. After that, I focused on my development career and got into PicoCTF, a free computer security education program, and Hack the Box through a colleague. In 2020, I discovered that bug bounties were a thing – where a monetary reward is offered to a person who identifies and alerts a company to an error or vulnerability in their computer program or system. I wasted no more time on CTFs and jumped straight into the bug bounty scene.

Hacker Portrait of GangsterSquad

What has been the most noteworthy vulnerability you've found?

I've found some really cool vulnerabilities, but the most remarkable one is where I took over the entire security camera system that belonged to the headquarters of one of my targets in 2020.

I was able to see eight cameras that were covering the entire inside of their office. Then I quickly took a screenshot of what I was seeing, edited the picture by writing "SMILE" on it, and went on to report the issue on Intigriti's platform. I reported it around 2 AM and by the next morning, my report was already accepted and paid for. It was an amazing overall experience!

Do you think there are still misconceptions around the role of ethical hackers today? If so, how do you think that could be changed?

Yes, there are. Many people don't understand ethical hacking or don't want to understand it. Being a hacker is often seen as something bad due to its portrayal in mainstream media. I think as an IT security community, we need to spread awareness, concern and break the hacker taboo.

What would be your top tips for businesses to protect themselves against cyber threats?

I could give endless amounts advice for this! If I had to pick my top tips, it would be to:

1. Make sure that you have dedicated people working on cybersecurity. Even if you're a small company, make sure that one person dedicates a bit of time to defend the company's assets.
2. Raise awareness amongst your employees that phishing is one of the most common ways to get hacked. Teach them to not open email attachments from unknown sources, and to always triple-check before clicking on a link and putting in their login credentials.
3. Keep your software up to date. As well as new features and functionality, software updates will often contain security patches and new security features.
4. Finally, minimise the usage of different platforms. The more platforms you need to govern, the more work you'll have with regards to security governance so it's best to centralise where possible.

Have you seen any changes in the way that businesses are embracing bug bounty programs today since, let's say, 5 years ago?

The number of businesses jumping on the bug bounty bandwagon is growing rapidly, which is a good thing. In my opinion, it's a great way to secure your company's online assets. Unlike penetration testing, companies have access to thousands of ethical hackers with a bug bounty program in place. It's the job of these security experts to actively seek out the cracks in your application and infrastructure, and they're

incentivised by bounty rewards based on impact and quality. There's also no time limits on it, so you can keep your bug bounty program running all year.

What's the first thing you would share with somebody who is new to infosec?

The biggest tip I can give is to be patient. In infosec, nobody gets to the top one spot in just one day. It's a process that can take a while. It all depends on how motivated and dedicated you are. Try to read and learn as much as you can. Try some new things out and don't be scared when you fail –you'll get there eventually!

Great advice! Thanks for speaking to us, GangsterSquad

With the rapidly increasing expansion of the online world, the importance of ethical hackers is increasing accordingly. To bust through scalability constraints, overcome skills shortages, and stay within allocated budgets, effective security is no longer something that businesses can do alone.

Read the original article posted on DutchCowboys.