The World of the White Hat Hacker

Date : January 30, 2019

The recent London Fashion Week debuting the spring 2019 styles of top designers, involved some unlikely runway models – a group of female hackers who spend far more time reading and writing computer code than they do buried in the pages of *Vogue* magazine.

One model in particular stood out, not just for the Nicholas Kirkwood boots she was sporting, but also for her serious hacker cred. Her name is CyFi, and at 18, she is one of the most high-profile white hat hackers. Basically, rather then using her advanced computer skills to hack into systems and wreak havoc, like, for instance, stealing money or important data from banks and other businesses, she uses her tech knowledge for good.

White hat hackers – also known as ethical hackers – are often hired by companies to locate vulnerabilities or bugs in their systems that might allow the bad hackers to break into their cyber networks and compromise whatever it is that they're trying to keep secure. CyFi, who goes to high school in Silicon Valley in the U.S., actually co-founded a group and conference known as R00tz Asylum to teach younger kids about ethical hacking and motivate them to find vulnerabilities in mobile apps and programs and help strengthen them. CyFi has said, "Our generation has a responsibility to make the internet safer and better."

White hat hackers have been stealing the tech spotlight, praised for protecting everything from valuable Instagram-influencer accounts to detecting cyber weaknesses at multi-million-dollar companies. And, they are being paid well for their efforts. Bugcrowd, a platform that crowd sources bug hunters for other companies, recently released a report on the economics of white hat hackers. According to Bugcrowd, the average yearly payout of the top 50 white hat hackers in 2018 was $145,000.

White hat hackers tend to be young, digital natives who consider screens as essential as food and water. So, we turned to two of the most well known teen white hat hackers to learn more about their work. Jack Cable, 18 and a freshman at Stanford University, recently appeared on the *Time Magazine* list of the 25 most influential teens of 2018. Dubbed a rising star in the world of white hat hackers, Cable has focused his ethical hacking on the cryptocurrency industry (think bitcoin) through his company, Lightning Security. Sam Curry, an 18-year-old from Lincoln, Nebraska, U.S., who has been covered by the likes of MarketWatch, BBC and the *New York Post* for his six-figure success strengthening the cyber security of companies like Yahoo, graduated from high school two years ago and is taking time off to focus on his business, 17security.

> "Seeing the rise of data breaches, white hat hackers are motivated to work alongside companies, helping prevent the next large-scale hack." — Jack Cable

Both Cable and Curry are passionate about their work. "Cybersecurity is one of the most pressing matters facing companies, our government and our society," says Cable, who has used his renowned hacker-security skills to work with the U.S. Department of Defense. "Just the knowledge that finding one vulnerability can singlehandedly prevent a data breach affecting millions of users is incredible. The challenge of finding vulnerabilities, as well, makes ethical hacking a fun and rewarding field."

They help us better understand the world of the white hat hacker.

White Hats and Bug Bounties. "A white hat hacker is an individual who works alongside companies to help identify

flaws in their security," explains Cable. "Bug bounties are a form of crowdsourced white hat hacking, where a company can make use of hundreds of white hat hackers to find vulnerabilities. This is effective because no company can find or prevent all of its vulnerabilities internally, so enlisting an external set of eyes can expose new vulnerabilities." Bug bounty platforms like HackerOne source the cybersecurity researchers (a.k.a. white hat hackers) and connect them with businesses.

The Bugs Revealed. "Generally speaking, when bug bounty hunters attempt to find vulnerabilities, they're attempting to find web application security vulnerabilities. These are issues that can be identified with pretty much only a web browser and tools to interact with the web browser," notes Curry. "At the end of the day, you're trying to exploit the logic of the web application to do something it shouldn't do in terms of confidentiality (disclosing user information), integrity (displaying content that it shouldn't), and availability (taking the asset offline as a rogue attacker). There are hundreds of vulnerability classifications and examples." Here are a few examples of Curry's ethical-hacking work from his blog: https://samcurry.net/hacking-a-massive-steam-scamming-and-phishing-operation-for-fun-and-profit/ and https://samcurry.net/reading-asp-secrets-for-17000/ and https://samcurry.net/exploiting-directory-traversal-on-a-yahoo-acquisition/.

More bugs! Cable's company Lightning Security worked with Solidified, a company providing a bounty platform to connect certain blockchain companies to auditors skillful in finding vulnerabilities. Solidified reached out to Cable to probe for vulnerabilities in its platform. Lightning was given access only to the public-facing URLs, in order to simulate a real cyber attack scenario, and then Cable set out to make sure those URLs were secure. "While testing, I identified vulnerabilities that could have led to theft of funds stored on Solidified and the exposure of user information, which would have harmed Solidified's finances and reputation if exploited," says Cable. "Instead, Solidified was able to fix these vulnerabilities before the business launched." Hungry for all Cable's bug-hunting details? You can find them HERE.

Show Me the Bounty. Payoffs can be big, but they're not definite. "In the last 12 months, I've made about $100,000 working 20 hours a week," says Curry. "Bug bounty, however, is a field where people are paid in bounties, not salaries. I could make $140,000 in the next 12 months or $60,000 depending on what I'm able to find. The thing that is so scary to bug bounty for most people is that there is absolutely no guarantee that you'll find any issues, and this is true for even the most competent researchers. During high school, I was still making about $70,000 yearly working between the end of the school day and about 1:00-2:00 a.m."

Grasping at Flaws. If you're interested in ethical hacking, you should first understand underlying protocols like HTTP and DNS. HTTP (Hypertext Transfer Protocol), for example, is the underlying protocol used by the World Wide Web that defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. You should also have experience with programming language and have strong critical-thinking skills and focus, suggest our experts. "White hat hacking is an exciting blend of curiosity, adversarial thinking and technical knowledge," notes Cable. "It definitely helps to be familiar with the basics of programming and development. Beyond understanding the technical aspects of various vulnerabilities, having programming experience exposes the process needed to build a secure website, which goes hand-in-hand with the attitude of a white hat hacker to look for flaws anywhere and everywhere."

Adds Curry: "If it's something you're interested in, pursue it! Everything is on the internet, and a challenge to yourself would be to make it your responsibility to figure out the groundwork yourself. Spend time trying and failing to understand things. If you aren't able to learn by yourself it is likely that you won't succeed later down the road."

Black Hoodies and Dark-lit Basements. Get this image out of your mind! A large and well-lit community of people – including established professionals and young part-timers who have few barriers to jumping into the hunt — are pursuing computer security and penetration testing. "People who do this work are generally very successful and competent," says

Curry. “Most information-security professionals are very vocal and communicative people who collaborate with other professionals. Try to completely throw away any assumptions you have of “hackers” (even though they definitely may exist somewhere in the real world) and instead see it as a melting pot of every persona.”

Echoes Cable: “The community of bug bounty hunters is extremely diverse and supportive. Many hackers run a blog where they detail interesting findings and their thought process, and lots of resources are freely available to learn about security. For instance, HackerOne runs a website called Hacker101 (hacker101.com), where it provides resources to get started in bug bounties. There is a community of hackers happy to answer questions and help newcomers to learn. Bug Bounty Forum in Slack communities is one example.”

Good vs. Evil. “We’re fortunate to live in a time where the easiest path to get started in hacking is the legal and ethical path,” says Cable. “Seeing the rise of data breaches, white hat hackers are motivated to work alongside companies, helping prevent the next large-scale hack. Further, experience gained and interactions with companies are invaluable. Countless hackers, including myself, have started careers in cybersecurity by participating in bug bounty programs, which can never be achieved via illegal activity.”