White-hat hackers, from their passion to the job to earn money, and little-known things

White hat hackers - heroes who don't cloak!

One day, in a peaceful neighborhood, there were a few spare young people who possessed quite a lot of IT skills and were especially passionate about exploring and exploring sophisticated security systems that had broken. successful protection barrier of a smart lock smart lock system, which is commonly used in modern apartments today and proved to be more efficient and convenient than with traditional door locks.

However, penetrating that 'fragile' security class is not the real purpose of these young people. Rather, it is only a necessary step for them to gain access to the 'smart hub' - the center of the intelligent control system - that regulates the operation of this smart lock system (and also those Other similar smart locks, are being used in millions of homes across the planet. And they only take 2 days to get into this system.

1. 12 'must-have' devices for smart home (Smart Home)

Smart lock - smart home appliance is increasingly used popularly - not as safe as many people think

When Charles Dardaman, an over 20-year-old hacker - and a well-known game addict, lives in Dallas, USA, he and his close friend, Jason Wheeler, a young information security specialist, together entered the control center of a smart lock system. Here, both found the hard-coded administrator password on its memory card. This is much more valuable than just cracking security and breaking into that smart lock system.

Smart hubs that Charles Dardaman and Jason Wheeler have infiltrated are those of Zipato, a company operating in the field of smart home technology, currently controlling and operating many smart door lock system utilities. thermostat and home security system. Obtaining administrator-level access to smart hubs is like holding the key to opening any home using Zipato's smart lock technology.

Here, many people probably think that Charles Dardaman and Jason Wheeler will come together to find homes that are using smart lock Zipato, use the security key that they hacked, open the door and 'steal' something there. Or worse, sell your findings on the black market and earn a profit. But no, these two young men did not only have no illicit intentions, but also decided to report all details related to the "violation" that they had made to Zipato so that the company could have a plan. This is the act of moral 'hackers', also known as white hat hackers.

1. Filipino hackers attack the Vietnamese web, retaliating that many users' Facebook accounts are 'hacked' by Vietnamese people

Charles Dardaman's Twitter account, young white hat hacker is very popular

So what is the specific white hat hacker? First, it must be affirmed that white-hat hackers are righteous, in stark contrast to black hat hackers. White-hat hackers are experienced and professional cyber security professionals like black hat hackers, but instead of trying to attack the system to gain unauthorized profits, they take the time to research, prevent Block, prevent and report to system owners about security vulnerabilities before it is exploited by bad guys.

According to HackerOne statistics - a platform dedicated to rewarding hackers when they report security vulnerabilities - the majority of white-hat hackers operating in the platform live in India (23%) and the US (20%), 6 % in Russia, 4% in Pakistan, and 4% in the UK. They come from many different educational environments, of which mainly self-study (58%), while some study in computer science at university or high school. Most white-hat hackers are young people, 90% of white-hat hackers on HackerOne are under 35, 50% are under 25 and 8% are under 18 years old.

Dardaman and Wheeler are also white hat hackers who break into a system with the desire to make the system even more comprehensive. In addition to free white hat hackers like Dardaman and Wheeler, many other individuals work for government agencies or large corporations and businesses. They are sometimes referred to as security - network security experts.

1. The most dangerous hackers on the planet: Anonymous, Equation Group, Department 121 . What do you know about them?

White hat hackers are righteous people - in stark contrast to black hat hackers

Although the activities of white-hat hackers are not illegal and have a righteous color, that does not mean that all acts of intrusion into their systems are strictly authorized. While many white-hat hackers work on 'orders', asking them to check the vulnerabilities of a particular company, some people like Dardaman and Wheeler spend days, even months. In order to find a way to break into a system, pursue informal projects, this sometimes causes them to encounter unnecessary problems with the target system owner.

Back to the hack smart zipato hub of 2 young men. At first they had no idea to do such a mission, that thought only appeared when they read the story of an experienced information security specialist named Lesley Carhart. Number is Lesley Carhart living in a rental apartment, a beautiful day, the owner decided to switch to using smart door lock to ensure safety, Lesley certainly did not object but she met no less troublesome while learning how to use this 'modern power damage' system. Immediately, plus the desire to learn and talent for information technology, this security expert decided to hack the newly installed smart lock system. It is this humorous but equally cool story that inspired Dardaman and Wheeler.

1. With this fake Lightning cable, hackers can remotely take over your computer in minutes

Dardaman and Wheeler have 'hacked' into Zipato's smart hub system to prove that Lesley Carhart's concerns about security holes in smart lock systems and capital devices are designed to enhance safety. Now, it becomes less safe, is completely grounded.

The incident was later shared by techCrunch TechCrunch and the news immediately spread. Another fact that is exposed, companies are now focusing on promoting the excellence of smart home technology that ignores security enhancements, because they probably don't think the weaknesses on their products I was exposed so quickly.

Such 'ethical hacking' missions mean really important to everyone's safety, as well as related businesses.

In 2015, a group of hackers successfully infiltrated the management and remote control system of a jeep when it was on the road - extremely dangerous behavior, causing Chrysler to make a decision. recalled 1.4 million cars to fix errors.

In 2018, a white-hat hacker group from Anonymous security organization Calgary Hivemind has silently hacked into Nest's security camera system software to warn people about potential vulnerabilities - causing Nest's

customers to worry. sediment, forcing this company to patch the system as well as encourage users to apply 2-factor verification.

Or as it was earlier this year, an anonymous white-hat hacker group revealed a series of security flaws in Medtronic's heart-implanted medical devices that could allow an attacker. Remote device control, endangering patients. Soon, Medtronic was forced to explain the incident to the US Food and Drug Administration (FDA) and release a vulnerability patch.

1. Most mobile calls in the world today can be eavesdropped by hackers

The relationship between white-hat hackers and the companies that own the products they have discovered is sometimes not very smooth.

The above are just small examples of white-hat hacker contributions to people's safety, as well as contribute to improving the quality of products and services. If those security holes are not found and reported before being used by bad guys, the consequences will be unpredictable.

However, the relationship between these moral hackers and the companies that own the products they invaded are sometimes not very smooth. While some organizations and enterprises always appreciate the activities of white-hat hackers and consider these valuable contributions to help them improve their products, there are many other companies that consider hackers to be enemies in general. , and hardly distinguish between white hat hackers and cyber criminals. 'For many companies, they would rather pay fines or even sacrifice the interests of customers instead of investing in fixing security holes,' said a white-hat hacker who declined to be named. In the context that sanctions and regulations on this issue have not yet been fully promulgated, the attention of the media and pressure from public opinion will still play a role as the most optimal measure to force enterprises must implement security policies in a reasonable way, respect customers' rights.

In contrast to Dardaman, breaking the law for personal gain, such as finding a loophole to extort money from businesses, has never been a viable option. 'I want to have a normal life, do what I think makes sense, and help people,' said the young hacker.

1. Detecting vulnerabilities in Snapdragon chips allows hackers to penetrate nearly every Android smartphone via wifi

The chance to lead Dardaman to become a white-hat hacker is quite accidental. During the summer break after graduating from high school and preparing to enter college, the young man was free all day and tried to write cheating software for Minecraft games. Dardaman appointed to write and play to see how well his ability was but 'how bad the sky makes' succeed. From there he shot his head more interested in finding out how to get into a system himself.

As time went on, cultivating Dardaman's passion for the life of a hacker, and until he got a degree in information technology major, he really realized that he would definitely must become a white hat hacker, a career of choosing people, it can't be helped.

Charles Dardaman is currently working at Critical Start, an intermediary brokerage firm, which helps white-hat hackers sign security monitoring contracts for large commercial and banking corporations. Companies like Critical Start are part of the 'information security industry' - an emerging and fast-paced sector, in line with the growing number of cyber attacks. both in quantity, complexity and damage they have caused in recent years.

This field has been around for a long time but has only been developed in the early 2000s as a way to deal with data breaches of the pre-Internet globalization era, and the birth of the Social media as well as online retail. At that time, the black hat hacker 'washing his hands and guarding the sword, changing the rules' to being a white-hat hacker after being arrested or sentenced to punishment was extremely unlikely, sometimes even considered abnormal. . For now, such cases are not uncommon, such as the case of 'WannaCry' Marcus 'MalwareTech' Hutchins. Marcus Hutchins was a cybercrime who was arrested by the FBI for alleged acts of creating and distributing various types of malicious code to steal money in banks in 2014, but later It has been 'major reassertion' and became a well-known security researcher, playing an important role in the WannaCry malware attack campaign in 2017.

1. The hero WannaCry Marcus 'MalwareTech' Hutchins will not be imprisoned - a common victory for white-hat global hackers

WannaCry 'Marcus hero' MalwareTech 'Hutchins, who has successfully changed the hat color and is loved by the community

For young people who want to be white hat hackers like Dardaman, it's easy to sign up for school-based, or online, and online ethical hacking courses, and get online security certification.

Dardaman contracted to test system vulnerabilities with businesses almost continuously, and each such contract is usually completed in about 1 to 2 weeks. Typically, companies that have contracted Dardaman will not disclose to their internal security team about the contract as well as the appearance of Dardaman. They allowed him to freely "wander" in his network quietly, watching how things worked and finding a way to penetrate deeper into the system. will only last for a few days.

Immediately after the well-intentioned screening, it will be the "steel punches" that Dardaman will inflict on the security system of that enterprise to check its defensive capabilities as well as overcome damage on the system. More specifically, his final destination is usually to gain absolute access to the company's servers to 'test the security team'. Leaving Dardaman in the system means that the company's security wall has a problem, and if after a few days still can't 'catch' Dardaman, the company's IT team will be forced to reassess the Their security tool.

In his free time, without a contract, Dardaman often hacks smart home technology - devices that can be activated by voice, remote controlled by sensors or an internet connection - because he believes that virtually Everyone does not know the danger from security risks on these devices.

Back in 2018, a hack aimed at Guardzilla's security camera system allowed Dardaman to gain access to the information store stored on users' devices. However, Dardaman does not "touch" the amount of data in that repository, because doing so is illegal, no longer an act of a white hat hacker.

'There is no better way to protect your system than testing it in real-life situations. This situation is the case of an attacker or a cyber criminal trying his best to infiltrate the system, without any mercy, 'said Phillip Wylie, a system penetration test specialist. at the US Central Bank, and information security professor at Richland College, said.

1. The 5 most notable cyber security conferences in the world take place throughout the year

Phillip Wylie is a system penetration test expert - "genuine" white hat hacker

Like Charles Dardaman, Phillip Wylie is drawn to sweating situations when he attempts to infiltrate a system, the excitement of successfully drilling a closed security wall, and above all the joy was mixed with pride when

announcing that vulnerability to the system owner because he knew that he had done something meaningful.

Before joining the US Central Bank security team, Wylie had long worked as a security consultant, specializing in the implementation of penetration tests or meetings. Authorized network attack on web applications. Once, Wylie found a serious vulnerability that allowed him to access the core database of a client system. The password of this system is set in a way that can't be overstated, just 'password1', and Wylie didn't take much effort to break it. Later, he used a tool called John the Ripper to infiltrate the system (this process only took a total of 30 seconds). 'I can add users to that system; I can close the server, turn off the database, delete the profile. I have full control of the system, 'Wylie said. And then of course Phillip Wylie reported all the information about the vulnerability and how to infiltrate the company. He was awarded a bonus, but the most significant thing for Wylie was admiration and thanks.

But not all hackers put a lot of effort into penetrating the system just to reveal security risks. Jane Manchun Wong, a 23-year-old computer science engineer living in Hong Kong, often spends his free time "training" his reverse-engineering applications to understand the the power of the future. 'The things I find are public information,' Wong said, 'they are hidden in people's phones, computers, and extracting these data will be extremely difficult.'

1. This 23-year-old female hacker is the one who finds secrets that Facebook and other tech giants don't want to reveal

Jane Manchun Wong has revealed shocking information about Instagram

In April, this hacker revealed a shocking information that Instagram was, is, and will try to hide data about visits, such as the number of views on photos, to certain user objects. 'For the first time when I posted about this discovery, Instagram tried to say, "We didn't do that." However, that code actually exists - that's the bottom line,' Wong. At the end of April, Instagram announced that it would begin testing hidden likes for some users in seven specific countries, just as the Chinese female hacker discovered.

However, Jane Manchun Wong's ultimate goal with his findings is similar to other white hat hackers, which is reported to the owner. After finding leaked user data in the code, she reported to the company so they could overcome potential violations, which is the job of a "real" white hat hacker.

In a BBC interview, Wong explained: 'Ever since I started getting the attention, companies started tracking my tweets, many companies have improved their security. Their use is thanks to my findings, and I'm happy about that. In addition to passion, this is also one of the important motivations to help me overcome difficulties and pursue the career of a moral hacker. When companies successfully improved their security capabilities, they sent me thanks and even remuneration. I feel like life is more meaningful '.

1. Mysterious hackers offer Windows zero-day vulnerabilities to the world's most dangerous cyber criminals

Sometimes Manchun Wong makes big companies 'salty' after revealing gaps in their products

Wong's hacking missions really caught the attention of the media. When she revealed the news about Instagram, online, almost all major tech sites reported, thousands of debates broke out across technology forums around the world, the reputation of this female hacker also so that is enhanced. Sometimes Manchun Wong makes big companies 'salty' after revealing holes in their products, and of course no one wants to be humiliated. Many companies do not like Wong, but because of the pressure from public opinion, they are forced to quickly release bug fixes, and users will be the most beneficiaries, that's what she really does. center.

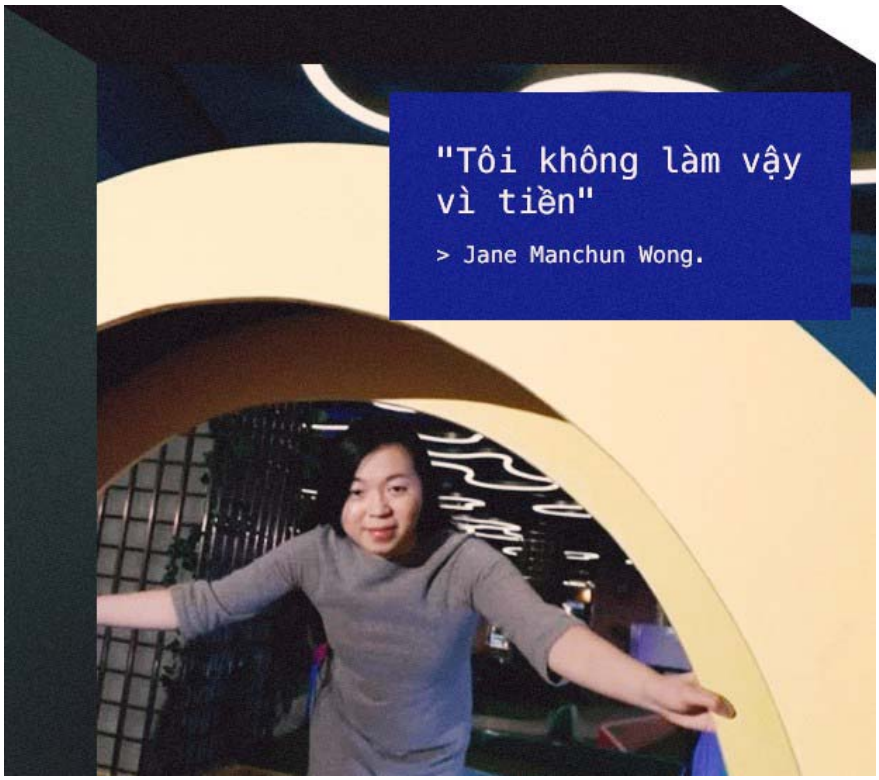
Most white-hat hackers have pledged that they have no intention of "stalking" to lower the reputation of companies or try to spark a media crisis to knock down a certain brand. Indeed, normally, the vulnerability will be reported privately to the owner by white hat hackers, and left them for about 90 days - the standard time offered by Google ED Project Zero - to patch any any security hole After that time, if the vulnerability has not been patched, they will understand that the company deliberately does not care, and will publicize its findings, which is the usual workflow of white hat hackers.

'If they responded to our report and immediately embarked on a patch, it was wonderful, reflecting a sense of responsibility and respect for contributions from people like us. But if they do not patch, or simply ignore our report, all information about the vulnerability will be made public. 90 days is a time limit, this excess, all explanations are fallacies. If businesses know how to put their customers' interests first, they will have to patch the gap around that time, 'said Dardaman, who always follows this strict code of ethics.

Jane Manchun Wong is also willing to work with product owners that she finds a problem. Last year, Wong discovered that Facebook is quietly deploying a javascript library to make web applications faster. When she started "hinting" about this secret project on Twitter, a Facebook employee contacted and asked Wong not to disclose the details of the information she had, because Facebook had planned to publish. it was next year - and Wong accepted the offer. Facebook also kept a promise with Wong when releasing this project as an open source

last May, which made Wong feel pleased that he was respected.

1. The Forum focuses on notorious social network hackers who have been hacked and sold for sale on other forums



Hackers on white hats don't 'hide their hair' to lower companies' reputation, extort money, or seek bonuses

However, many other white-hat hackers are not as "easy-going" as Wong, they sided with the interests of users more than businesses. They feel responsible for telling users about security flaws, despite the fact that businesses can suffer heavy losses in prestige. This sometimes causes them to suffer rage and retaliation from many companies. But then, public opinion will raise the question whether this business is really interested in the rights and interests of customers seriously, or just focus on ensuring personal prestige, At this time, the prestige of the business will be even worse.

But sometimes white hat hackers get into trouble with the good work they do. Many businesses even denounce white-hat hackers for violating their systems. 'If you find a flaw and report it, but the product owner says that they will denounce your infringement behavior to law enforcement agencies, it is a problem not easily solved " "Wylie said. Although this doesn't happen often, and sometimes it's just a threat." But don't be too worried, then you'll be given a free legal knowledge test. " .

In the case of young hacker Charles Dardaman with the smart hub system of the smart home appliance maker Zipato mentioned above. The business gave feedback immediately after receiving a report of the vulnerability, and pledged to fix the vulnerabilities as soon as possible. Such businesses are not only unreliable when they are found to have faulty products, but even their reputation is enhanced, as a company responsible for their customers. 'They are certainly not happy to hear me announce the gap,' said Dardaman, laughing, 'however, they quickly corrected the error and I'm happy about it.'

1. The alarming increase in the number of attacks targeted at IoT devices

White hat hackers - heroes who don't cloak!

Hy v?ng sau bài vi?t này, chúng ta ?ã có cái nhìn sâu s?c h?n v? công vi?c và nh?ng khó kh?n mà m?t hacker m? tr?ng ph?i ??i m?t. H? chính là nh?ng ng??i ?ang ngày ?êm chi?n ??u b?o v? s? bình yên trên không gian m?ng, ?? ??m b?o quy?n l?i c?a ng??i dùng công ngh? trên toàn th? gi?i - ?ó là ?óng góp th?m l?ng c?a nh?ng v? anh hùng không áo choàng!

1. Ngoài hacker m? tr?ng và hacker m? ?en, gi?i hacker còn nh?ng màu m? nào n?a? Có công vi?c chân chính nào dành cho h? không?