BIZCOMMUNITY

Fantastic (ethical) hackers and where to find them

By Simon McCullough

26 Apr 2019

Data breaches and cyberattacks are unignorably on the rise and hackers are becoming increasingly sophisticated. Across the world, businesses are finding it difficult to grapple with rapidly shifting cybercriminal motivations, tactics and appetites for destruction.

Image source: Gallo/Getty

The problem is exacerbated by emerging technologies such as IoT constantly expanding exploitable attack surfaces. At the same time, massive volumes of work data and applications are moving to the cloud in various deployment configurations, potentially leaving additional swathes of data unprotected.

To both understand and keep pace with cybercriminal mindsets, many businesses are seeking to fight fire with fire. It is particularly important to consider every single possible attack vector when protecting applications. This is where the ethical or “white hat” hacker can often make a difference.

While security architects have a wealth of knowledge on industry best practise, they often lack first-hand experience of how attackers perform reconnaissance, chain together multiple attacks or gain access to corporate networks.

Equipped with – one hopes – all the skills and cunning of their adversaries, the ethical hacker is legally permitted to exploit security networks and improve systems by fixing vulnerabilities found during the testing. They are also required to disclose all discovered vulnerabilities.

White hat hacker community

According to the 2019 Hacker Report, the white hat hacker community has doubled year over year. Last year, $19m was doled out in bounties, nearly matching the total paid to hackers in the previous six years combined. Eye-catchingly, the report also estimates that top earning ethical hackers can make up to forty times the median annual wage of a software engineer in their home country.

So where do you find these mythical creatures?

The most common method is a “bug bounty” scheme operating under strict terms and conditions. This way, any member of the public can search for and submit discovered vulnerabilities for a chance to earn a bounty. It can work well for publicly available services, such as websites or mobile apps. Rewards depend on the level of perceived risk once the affected organisation confirms the validity of its discovery.

Using crowdsourcing and paying incentives has obvious benefits. Hackers get reputational kudos and/or hard currency to showcase and test their skills in a very public forum. In exchange, the hiring organisation gains new dimensions of security smarts and perspectives.

Some businesses choose to hire hackers direct. Hands-on experience is key here. While it may sound counter-intuitive to make use of external hackers – some of which have a track record of criminal activity – the one thing they have in abundance is hands-on experience. At the end of the day, a hacker is a hacker. The only difference is what they do once a bug or vulnerability is found.

Ultimately, employing an ex-cybercriminal is a risky decision that should be made on a case-by-case basis. It is also worth noting that criminal background checks only help identify previous offenders – they lack context on how a person has changed. For example, it is unlikely that someone charged for a denial of service attack at a young age has mutated into an international career criminal. Indeed, some young offenders often go on to become well respected security consultants and industry thought-leaders.

Hunting for hackers

Another fertile hunting ground for hackers could be closer to home. The best practitioners are curious, with a strong passion to deconstruct and reassemble. Businesses need to get better at harnessing the skills of those building their applications, code and network infrastructure. They may already know about vulnerabilities but have yet to report them as it isn’t part of their job description. This is a waste. Decision-makers need all the insight and help they can get, and there’s more of it out there than you think. Over the years, I’ve met many people at security workshops or capture the flag hacker events that have built products but claim to enjoy the process of ameliorative, intelligence-gathering hacking even more.

Finally, ethical hacking is also becoming increasingly formalised. Notable qualifications include Certified Ethical Hacker (CEH), Offensive Security Certified Professional (OSCP) or Global Information Assurance Certifications (GIAC). Naturally, many seasoned hackers will balk at such educative evolutions but watch this space. Ethical hacking is set to become more mainstream as perceptions and security-first business imperatives change.

ABOUT SIMON MCCULLOUGH

Major Channel Account Manager at F5 Networks
- Try to tackle cybersecurity during #RWC2019 - 20 Sep 2019
- Stay safe from cybercrime with what's left of 2019 - 30 Aug 2019
- Multi-cloud's new multiculturism - 21 Aug 2019

- A new phase of cyber warfare has begun - 7 Aug 2019
- The ABC of DevOps - 27 Jun 2019

View my profile and articles...