When Ethical Hacking Can't Compete

Companies are paying “white hat” hackers to probe their cybersecurity systems for weaknesses—but some say that so far, they aren’t paying enough.

Donna Lu • Dec 8, 2015

The cybersecurity expert Chris Rock is an unconventional killer. At this year's Defcon hacking conference—one of the largest conferences of its kind, attracting more than 6,000 hackers and security experts from around the globe—the Australian information-security researcher demonstrated how to manipulate online death-certification systems in order to declare a living person legally dead. Potential motivations for hackers, he explained, range from plain revenge to financial gain in the form of life-insurance payouts.

Rock began researching these hacks last year, after a Melbourne hospital mistakenly issued 200 death certificates instead of discharge notices for living patients. He also uncovered similar vulnerabilities in online birth-registration systems. The ability to create both birth and death certificates, Rock told a packed session at Defcon, meant that hackers could fabricate new legal identities, which could in turn engender new types of money laundering and insurance-fraud schemes.

In the hacking world, Rock is known as a “white hat”: an ethical hacker who exposes vulnerabilities in computer systems to improve cybersecurity, rather than compromise it. In recent years, white-hat hacking has become increasingly lucrative, as companies have turned to professionals like Rock to protect them from the growing threat of cybercrime. But to combat the sophistication of more malevolent hackers, the ethical-hacking industry still has a long way to go.

In a threat report published by the U.S. director of National Intelligence earlier this year, cyberattacks were listed first among global threats, above both terrorism and weapons of mass destruction. “We foresee an ongoing series of low-to-moderate level cyber attacks from a variety of sources over time, which will impose cumulative costs on U.S. economic competitiveness and national security,” the report reads. “During 2014, we saw an increase in the scale and scope of reporting on malevolent cyber activity that can be measured by the amount of corporate data stolen or deleted, personally identifiable information (PII) compromised, or remediation costs incurred by U.S. victims.” According to the security firm Gemalto, an estimated 1 billion records worldwide were compromised in 2014.

David Burg, the head of global and U.S. cybersecurity at PricewaterhouseCoopers, says that public data breaches—like the high-profile hacks of Ashley Madison, the Office of Personnel Management, and Sony Pictures over the past year—comprise just a small portion of the hacking activities that take place. Attacks that relate to payment cards, PII, or protected health information are publicized because of mandatory breach-disclosure laws, but “most of the cybercrime that occurs, which is of the economic-espionage variety, is never made public,” he says. “Attack activity is very big business. You’re talking trillions of dollars in wealth being transferred globally.”

> *These hackers present a quandary for the tech industry: Ensuring a company’s cybersecurity requires the same skills as destroying it.*

In response, some large companies have increased allocated more money to protect themselves against hacks. According to a PwC report, American companies’ cybersecurity budgets have grown twice as much as their information-technology budgets over the past two years. Some companies hire external information-security professionals like Rock to undertake what's known as penetration testing—attacking their software systems, as malicious hackers would do, in order to expose weaknesses. Others use "bug-bounty" programs, which pay freelance hackers for each previously unknown software vulnerability they uncover.

These programs may be run in-house—Google, for example, has had its own bug-bounty system since 2010 and pays up to $20,000 for a single bug—or outsourced to separate companies like HackerOne and BugCrowd, which connect hackers with clients and take a cut for each bug found.

Alex Rice, the chief technology officer of HackerOne and the founder of Facebook's product-security team, says that HackerOne's global network includes just under 2,000 paid hackers, many of whom hold full-time jobs and pursue their hacking projects on the side. And Jay Kaplan, the CEO of Synack—which offers clients a subscription-based system of protection—says his hacker base, which spans 35 countries, is mixed: Some are moonlighting, but others support themselves entirely from white-hatting, especially in less developed places like China, India, and eastern Europe. Payments for hackers, Kaplan explains, can vary widely depending on the project: "The market rate is dictated by how widespread an issue is and what the relative impact is to an organization."

In many cases, though, it can be a difficult way to earn a living. Clifford Trigo, a 22-year-old living in Bohol, in the Philippines, is a full-time white hat who joined HackerOne at the beginning of 2014. He makes his money entirely from bug bounties and freelance penetration-testing gigs, but says that lucrative bounties can be difficult to come by; every few months, he'll find a bug worth several thousand dollars. "I typically get those kinds of big rewards when there are new bug-bounty programs," he says, when the possibility of discovering large vulnerabilities is greater. More often, though, "you could do research for hours, then get paid 50 or 100 bucks or so." He knows a few white-hat hackers, he says, who have supplemented their bug-bounty income with shadier activities, like using their skills to access people's credit-card information.

These so-called black-and-white hats create an ethical quandary for the tech industry: Ensuring a company's cybersecurity requires the same skills as destroying it. Rock believes that the issue of white-hatters who also conduct malevolent hacks is likely widespread. "Many companies say they don't employ black hats, but most probably do," he says.

Kaplan, who is a former counterterrorism analyst at the National Security Agency, disagrees. "I think the vast majority of people who are doing this type of work are highly ethical and they want to be doing it legally," he says. Notwithstanding, Synack puts all of its own candidate researchers through a thorough interview process and background check.

Burg believes that the benefits of using outside white-hatters outweigh the risks: "Organizations that are willing to take criticism and analysis from independent parties are more likely to be able to combat cyber-threat actors," he says. Burg also believes that the Cybersecurity Information Sharing Act, which passed the Senate in October this year, will bolster the growth of the white-hat hacking industry. The bill calls for the federal government to declassify certain pieces of intelligence on cybersecurity threats and make the information available to private-sector companies.

Rice shares Burg's view. "We all have vulnerabilities, and we're not going to overcome them unless we can eliminate entire categories of attacks in collaboration," he says. "There's a huge community of companies and hackers out there at the ready."