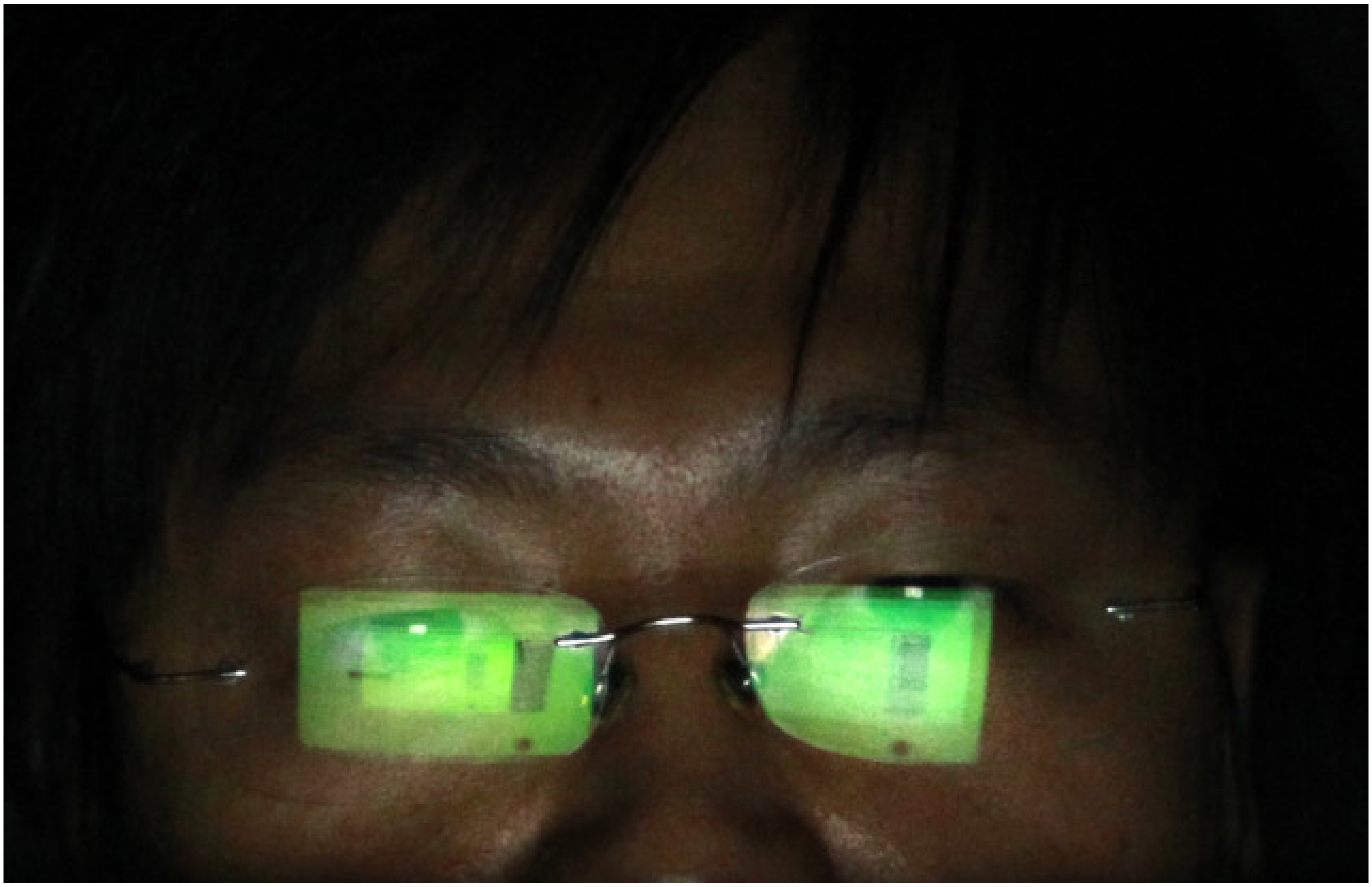
Hacker Business Booming as Security Experts Struggle to Keep Pace

Aida Akl

Posted August 28th, 2015

Tweet

Leave a comment



A hacker works on his laptop in his office in Taipei, in Taiwan, July 10, 2013. (Reuters)

Sophisticated hackers are taking advantage of a regulation vacuum and a shortage of cybersecurity experts to turn stolen data into a lucrative business, with little fear of being caught.

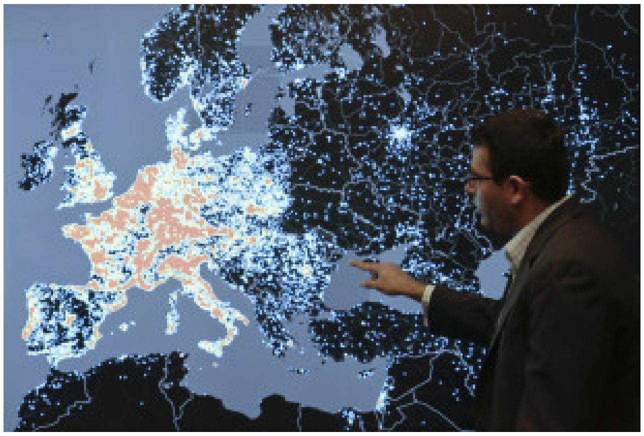
“For $200, you can set up a business,” said Al Berman, President of New York’s Disaster Recovery Institute International (DRI).

Hackers used to flex their muscles in cyberspace just for fun. “If you look in 1997, IBM did a survey and about 85 percent of the hackers were cyber joyriders – people who just did it for the challenge of it,” he said. “When you look at it today … almost 80 percent of them are in the business for profit.”

By Berman’s estimates, that market is worth at least tens-of-billions of dollars,” given the sheer volume of stolen data. But Carnegie Mellon University’s Nicolas Christin, Assistant Research Professor of

Electrical and Computer Engineering, said more reliable figures place the annual global costs of online crime at around $3-4 billion. “It may be a bit conservative,” he said in an email, “but I believe in the right order of magnitude.”

Not all hackers make good money, said Christin. Those who do are skilled enough to identify large numbers of targets at once. Connections, skill, experience and luck all play a role in shaping the hacker’s fortune.



Vishant Patel, senior manager of investigations at the Microsoft Digital Crimes Unit, shows a heat map and talks about how malicious Citadel Botnets attack computers in Western Europe, Redmond, Washington, Nov. 11, 2013. (Reuters)

“Operating a botnet very successfully may allow the operators to make a couple of millions at most,” he said. “But between direct [remedial, clean up] and indirect [reputation, etc.] costs, that botnet may cost orders of magnitude more to society.”

Nevertheless, once hackers learn how easy it is to sell stolen data, they are “attracted quickly to a lucrative six-figure career stealing identity, credit cards, and reselling them on the ‘dark web’ anonymously from the comfort of their own PC at home,” said cybersecurity expert Scott Schober, President and CEO of Berkeley Varitronics Systems.

Hackers can find all kinds of free resources and hacking tools on the dark web – a gritty underbelly of the Internet inaccessible to regular users, but commonly frequented by people on both sides of the law keen on hiding their identity.

“The deep web is not indexed by the normal search engines we are accustomed to using,” said Schober in an email interview. “It requires the free Tor browser [easily downloadable] software so specific URLs can be entered.”

Tor provides hackers with anonymity when they buy and sell illicit items in this underground world, home to more than 10,000 known illicit web sites whose URLs change frequently so they cannot be taken down.

While small businesses are often prime targets, Schober, author of *Hacked Again*, said hackers typically look for easy targets, which are “less complicated and pose less of a chance of getting caught. So it’s usually not about the biggest score but rather, the fastest and easiest one.”

The price of stolen data depends on how recent the hack is, whether it has been discovered, the amount of available information, and supply and demand.

“If there is a sudden influx of millions of available credit cards on the black market [a large supply], then the demand [and value] is somewhat diminished," said Schober. "Another important factor is how 'fresh' the credit card is. A freshly acquired stolen credit card can fetch from $26-$45. In comparison, stale, older compromised credit cards may only fetch $8-$28 each."

The anonymous nature of hacker transactions and the lack of regulations make tracking the thieves challenging, if not impossible.

There are no international laws to help authorities go after these hackers, said Berman; and "lawmakers are way behind what's going on in the industry."

Most hackers, according to Schober, are "groomed out of Russia, Romania, China, where it may be somewhat challenging for an individual to land a well-paid job." And the laws are such, said Berman, that "there's no right of extradition. And then, in a lot of places, it's not even a crime."

"It's risk-versus-reward if the real risk of getting caught is very small … and the reward is so great it's – and I hate the analogy – but it's like being a drug dealer," he added.

Meanwhile, hackers are getting smarter, not even touching their loot, but storing it on hacked servers in different regions so that it is even more difficult to trace. That environment has created what Berman calls the "Wild, Wild West in cyberspace."

Not surprisingly, this has contributed to a booming cybersecurity job market, with much sought-after ethical hackers earning as much as $200,000 a year in some parts of the United States. But there aren't enough of them.

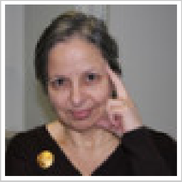
According to Berman, some studies show that only 75 percent of the needed ethical hackers will be in the workforce by 2019.

To fill the gap, tech companies like Cisco are training cybersecurity personnel while colleges churn out the next batch. And more recently, Internet security firm Symantec teamed up with the National Association of Software and Services Companies to train cybersecurity personnel in India, some of whom will receive internships and placements.

"It's one of those careers that [are] developing," said Berman. "But it's like being on the defensive all the time. … It doesn't work that way because you're always a step behind."

But Christin disagreed, saying the hacker-defender tug-of-war is an economic game where the "goal is to raise the bar the opponent has to clear to successfully attack you."

"You can probably filter out easily the vast majority of attacks coming from incompetent, low-level attackers," he said. "And if you place the bar high enough, even the few competent ones may be more interested in seeking other targets to attack if they are looking for monetization."



Aida Akl

Aida Akl is a journalist working on VOA's English Webdesk. She has written on a wide range of topics, although her more recent contributions have focused on technology. She has covered both domestic and international events since the mid-1980s as a VOA reporter and international broadcaster.