HONG KONG BUSINESS

http://hongkongbusiness.hk/information-technology/exclusive/deciphering-modern-day-hackers-who-they-are-what-they-want-and-ho-0

Deciphering modern-day hackers: Who they are, what they want, and how to beat them

29/09/17

Deciphering modern-day hackers: Who they are, what they want, and how to beat them

Find out how your company can prevent the next cyberattack that could cost you billions.

The recent data breaches and cyberheists across the world unmasked one of the scariest enemies of private and public entities alike: cyber criminals. And if the progression of the recent attacks are anything to go by, we can only expect these perpetrators to become even more sophisticated and aggressive over time.

Several companies from different sectors in Asia and around the world have fallen victim to some of the largest, most damaging cyberattacks. For instance, early this year, the WannaCry ransomware made headlines after it infected more than 200,000 computers in over 150 countries around the world, including the UK's National Health Service. Just recently, a data breach at US credit reporting agency Equifax compromised the personal information of almost 150 million Americans. Last year in Asia, the banking industry was shaken after $81m was stolen from Bangladesh Bank's account with the Federal Reserve

Bank of New York. In the same year, Thailand’s Government Savings Bank shut down 7,000 ATMs after hackers loaded malware onto the machines and stole $350,000.

These are just some examples of the many cases of cybercrime around the world, proving that cybersecurity must be one of the top priorities of companies, governments, and enterprises. This was one of the major topics discussed at the 2017 NetEvents Global Press & Analyst Summit in San Jose, California held on September 27 to 29.

In one of the keynote sessions, **MK Palmore**, information security risk management executive at the Federal Bureau of Investigation San Francisco, said the most prolific computer network intrusion activities throughout the world are those motivated by financial concerns. He said the barrier to entry to most financially motivated attacks is extremely low, and the attackers who do it with almost 100% anonymity are “mostly self-taught males aged 14-32 years old who have access to the dark web and to a limitless amount of information.”

What’s more alarming is the fact that these attackers, particularly in the financial sector, all know each other. **Ronald Layton**, deputy assistant director at the US Secret Service, said, “They all are collaborative, they all use Russian as a communications modality.”

He added that the technological sophistication and capability of threat actors have increased. “The toolsets that you see today that are widely available would have been highly classified 20 years ago. Sophistication has gone up exponentially. Sometimes between hackers and law enforcement, they say it’s a cat and mouse game. I reject that. To me, it’s the old game of rock, paper, scissor. It’s an adjustment to the last iteration. Specifically, in 2014, ransomware was the 22nd most popular threat. In 2017, it’s number five,” he said.

What can be done?
So with these threats looming, how can companies prevent the attacks? What are the steps they can take to make it less likely for their firm to be targeted by the cybercriminals?

Michael Levin, former deputy director of the US Department of Homeland Security, said it all boils down to the basics of security. “If we look at the Equifax hack, it was a simple error made by not providing the general basic security practices on the server,” he noted. “We’re hiring new people and putting them in important roles but we’re not telling them what they can and cannot do. Many organisations do not want to take the time to educate their people. It’s so basic to the day-to-day process of every organisation. It’s about time that every institution starts figuring out a way to educate people to protect themselves,” he added.

Layton concurred and said organisations pay a lot of attention to what the ‘bad guys’ will use to further their own illicit gain without checking if proper internal barriers are in place. “Convenience is the new nicotine, and the new caffeine is curiosity. That’s what makes you text on your phone when you drive when you shouldn’t be. You’re clicking on everything. You’re curious, you want to see what is behind that next click. When you look at the analysis and the pathology of how malware gets on a system, you’re going to find that the major percentage comes from clicking on an email attachment. Human factors and the psychology of cyber is something we must pay attention to. One way to counter this is through cyberhygiene,” he noted. But even then, Layton said awareness does not equal behavioural change. “We need to find new and innovative ways for training and to get our message out,” he added.

This message, whilst simplistic, is not being followed by businesses. “When you go through information security training, there are basics you are taught about protecting systems. We always find that there’s some gap in coverage in security that boils down to the fundamental issue of security protection. We’re talking about simple things such as patch management, audit and log management, security and vulnerability assessments, or buy-in from leadership and management,” Palmore said.

He added that two-factor authentication is an obstacle for threat actors because it represents a waste of their time. “They will move to a target that is easier for them to breach. If a business will be diligent in following those fundamentals, we’ll be in a better position,” Palmore advised.

How can companies strengthen their cyberdefence?
Enterprises can do three things to up their game against cybercriminals, according to Palmore. Firstly, he said there has to be a commitment from the leadership to invest in cybersecurity. Second, they have to practice the information security fundamentals, and lastly, they have to engage in information sharing. “As a business, you do not see the entire cyber threat landscape. You have to plug yourself into an intelligence apparatus,” he added.

In the private sector, Levin said the concept of encryption is an important piece of the puzzle. “One of the things we see all the time is people send emails with very sensitive information. They do not understand that sending emails is like sending postcards. You will never send your credit card number through a postcard. But emails are exactly the same thing—they are going through servers that are not secure, and the average citizen does not realise that. This is why we are seeing more organisations encrypting their emails. So as the crooks get more sophisticated, the private sector needs to be more sophisticated. They can use the same tools that the bad guys are hiding themselves from to protect their customers’ or employees’ data,” Levin said.

He added that it is equally important for firms to establish a practice that creates a sense of community for security. “Security can be just as important as being polite to customers. If you can create that sense within the organisation, you’ll see a better result,” he concluded.