# Hiring hackers

## The arrival of 5G creates a boom in demand for friendly hackers.

AS the number of online devices surges and super-fast 5G connections roll out, record numbers of companies are offering handsome rewards to ethical hackers who successfully attack their cybersecurity systems.

The fast-expanding field of Internet-connected devices, known as the Internet of Things (IoT) which includes smart televisions and home appliances, is set to become widespread once 5G becomes more available – posing one of the most serious threats to digital security in the future.

At a conference hosted by Nokia, "friendly hacker" Keren Elazari said that co-opting hackers – many of whom are amateurs – to hunt for vulnerabilities "was looked at as a trendy Silicon Valley thing six to eight years ago".

But "bug bounty programmes" are now offered by organisations ranging from the Pentagon and banks such as Goldman Sachs to airlines, tech giants and thousands of smaller businesses.

The largest bug-bounty platform, HackerOne, has 800,000 hackers on its books and said its organisations paid out a record US$44mil (RM180.3mil) in cash rewards this year, up 87% from the previous 12 months.

"Employing just one full-time security engineer in London might cost a company £80,000 pounds (RM434,400) a year," said Prash Somaiya, security solutions architect at HackerOne.

"We're starting to see an uptick in IoT providers taking hacking power seriously."

She said it's cheaper to hire hackers through a specialist organisation, adding that the company now regularly ships Internet-connected toys, thermostats, scooters and cars out to its hackers for them to try to breach.

"We already know from what has happened in the past five years that the criminals find very clever ways to utilise digital devices," Elazari said.

A sobering example was the 2016 "Mirai" cyberattack, during which attackers took control of 300,000 unsecured devices, including printers, webcams and TV recorders, and directed them to flood and disable websites of media, companies and governments around the world.

"In the future of 5G we're talking about every possible device having high-bandwidth connections, it's not just your computer or your phone," Elazari warned.

In October, Nokia announced it had detected a 100% increase in malware infecting IoT devices than the previous year, noting in its threat report that each new application of 5G offers criminals "more opportunities for inflicting damage and extracting ransom".

### Breaker mindset

The rewards for hackers can be high: 200 of HackerOne's bug-hunters have now claimed more than US$100,000 (RM409,800) in prizes, while nine have breached the million-dollar earnings mark.

Apple, which advertises its own bug bounty programme, increased its maximum reward to more than US$1mil (RM4.1mil) at the end of last year, for a hacker able to demonstrate "zero click" weaknesses that would allow someone to access a device without any action by the user.

"A big driver is, of course, the financial incentive, but there's this element of a breaker mindset, to figure out how something is built so you can break it and tear it apart," Somaiya said.

"Being able to hack multibillion-dollar companies is a real thrill, there's a buzz to it."

The rush of companies shifting to remote working during the pandemic has also led to "a surge in hacktivity", the company said, with a 59% increase in hackers signing up and a one-third increase in rewards paid out.

The French and UK governments are among those that have opened up coronavirus tracing apps to friendly hackers, Somaiya added.

### Incentive to act

While 5G Internet systems will have new security features built into the network infrastructure – something absent before – the new technology is vastly more complex than its predecessors, leaving more potential for human error.

"I see a lot of risk for misconfiguration and improper access control, and these glitches are one of the main risks," said Silke Holtmanns, head of 5G security research for cybersecurity firm AdaptiveMobile.

But companies are being motivated to act as security moves up the agenda, Holtmanns believes.

The European Union, along with governments around the world, has begun demanding tighter cybersecurity from organisations, and fines for data breaches have been increasing.

"Before now it's been hard for companies to justify higher investment in security," Holtmanns, who sits on the EU cybersecurity advisory group Enisa, said.

But she added, "If they can say: 'With that security level we can attract a higher level of customer, or lower insurance premiums', people start thinking in this direction, which is a good thing." – AFP

The increase in Internet-connected devices due to 5G is expected to bring about new security threats. — 123rf.com