THREATS FROM HIGH AND LOW

Andrew Frost, of Lawson Conner, looks at the cyber intrusion challenges facing the industry in the near future

Andrew Frost
is Lawson Conner's director of investment management solutions and is responsible for the ongoing growth of the fund incubation, wealth management and FinTech businesses of the group. He works very closely with the alternative investment community on prospective fund launches (hedge, private equity and venture capital) and with a diverse range of entrepreneurs looking to establish their businesses under the FCA regulatory framework.

We have started to see a rather twisted evolution in ransomware. The latest variants have given users the option to avoid paying the bitcoin ransom (which often runs around £1,000) by voluntarily infecting two other devices. This massively increases the risk of attack to corporate systems as home users that have become infected will be tempted to infect work systems in order to get their files back. Combined with the surge in bitcoin prices towards the end of 2016 and predicted growth in 2017, ransomware infection rates are not showing any sign of slowing down.

A LARGE-SCALE MASS CONSUMER IOT DEVICE BREACH

In the rush to fill the consumer space with cheap IoT devices, security has often been left off the list of priorities. We saw the effects of this in 2016 with the Mirai botnet – a large network of hacked internet-connected CCTV cameras being utilised as DDoS weapons against various websites. In 2017 this problem is only going to get worse as people feel more comfortable welcoming these connected devices into their homes. In 2015 security researchers found that a range of internet-connected baby monitors from nine different vendors were all vulnerable to attack. A large-scale breach of IoT devices like these with cameras or microphones in users' homes (like the Nest Cam or Amazon Echo) would cause widespread chaos and fear, and could be classified as an act of cyber terrorism. Although this scenario may sound far-fetched, in 2016 an internal ISIS communications channel was infiltrated and operatives were found to be sharing links to live feeds of hundreds of CCTV systems around the world that they had hacked into.

INCREASE IN LOW LEVEL "OFF THE SHELF" HACKING BY UNSKILLED CRIMINALS

It's becoming increasingly easy for unskilled criminals to get their hands on plug-and-play malware and phishing campaign kits. Requiring little to no skill at all, criminals

> "IT'S BECOMING INCREASINGLY EASY FOR UNSKILLED CRIMINALS TO GET THEIR HANDS ON PLUG-AND-PLAY MALWARE AND PHISHING CAMPAIGN KITS"

are able to buy off the shelf exploit kits and craft a targeted campaign against an organisation or individual to increasingly devastating effect. As the cyberattack/defence paradigm becomes increasingly asymmetric and the speeding up of the evolution of malware variants puts more pressure on CISOs, businesses are going to need to start taking a 360° approach to security in order to make sure that they are protected from more than dodgy email attachments – unified threat management will start to become the norm in 2017 as the advanced persistent threat (APT) continues to move out of the realm of nation states and into the SME arena.

INCREASE IN TARGETED ATTACKS AGAINST INTERNET INFRASTRUCTURE

Looking back at 2016, we saw some large-scale DDoS attacks against critical internet infrastructure – the root DNS servers. Only a month before these attacks, it was noted that there had been a suspicious increase in internet scans of specific pieces of DNS infrastructure – a theory put forward by Bruce Schneier is that this could have been the work of a state actor, looking to launch a large cyberattack against internet infrastructure. Towards the end of 2016 there was a marked increase in large-scale DDoS attacks that are likely to increase as we enter 2017.

NEXT-GENERATION SPEAR PHISHING ATTACKS

Towards the end of 2016 it was widely predicted that this year would see a marked increase in so-called 'spear phishing' incidents, and in the first few weeks alone there was a huge spike in highly targeted attacks, whereby criminals were spoofing their email addresses to appear to be a senior member of staff, and instructing employees to make a large financial transaction. Criminals are investing much more time researching target organisations and their staff so that they can craft more realistic emails in order to trick the employees into complying with their orders. As employees are spending more and more time outside of work hours responding to emails on their personal devices, users are more likely to fall for well-crafted email scams.

BYOD PIVOT ATTACKS

So called 'bring-your-own-device' policies have become a staple of the modern office. For all of the ease and convenience this brings to employees, it also brings myriad security issues for CISOs. In 2017, we will see an increase in pivoting attacks from insecure personal IoT devices to corporate networks. Combined with well-crafted next-gen phishing attacks, BYOD security will be a hot topic as we move into the year ahead. ■