CYBER RISKS & LIABILITIES_
NEWSLETTER

Provided by **Crendon Insurance Brokers Ltd**

December / January 2015

IN THIS ISSUE

DarkHotel Hackers Target Bosses in Hotels

A November report is warning companies to shield their high-profile executives, directors and officers from a new threat dubbed DarkHotel, which targets specific individuals accessing the Internet via Wi-Fi or an Ethernet cable while staying in upmarket hotels abroad. It works like this: Individuals who connect to the Internet receive a request for a fake update to a popular software package such as Adobe Flash, Google Toolbar or Windows Messenger. The installation files include legitimate software but also secretly harbour the DarkHotel code. Once the target approves the download with a single click, the malicious DarkHotel code goes to work, employing a number of different malware, including the following:

- **Keyloggers** monitor users' activity by recording and transmitting their keyboard and mouse presses.
- **Information stealers** copy data such as passwords stored by Internet browsers and other credentials.
- **A Trojan** scans a system's contents such as data about its anti-virus software. The malware then uploads that information to the hackers' computer server.
- **Droppers** install more viruses on computer systems.
- **Selective infectors** spread malware to other computer equipment via a USB connection or removable storage.
- **Small downloaders** contact the hackers' servers after 180 days, in a presumed attempt to allow hackers to regain control of machines that detected and/or removed their malware.

DarkHotel has targeted hotel guests in Japan, Taiwan, mainland China, Hong Kong, Russia, South Korea, India, Indonesia, Germany, the United States and Ireland—but the majority of attacks have taken place in luxury Asian hotels. Although attacks have happened around the world, the hackers always target company leaders such as CEOs, senior vice presidents, sales and marketing directors, and other top employees. The attacks cut across industries, including electronics manufacturing, pharmaceutical companies, cosmetic makers, car designers—even the military and non-government organisations. Researchers know DarkHotel is personally targeting each victim, but it remains unclear how hackers are able to track victims before they arrive at a hotel.

To prevent DarkHotel attacks, avoid hotel wired and wireless Internet services—instead rely on a company-provided mobile hotspot device. When you must use a hotel's Internet connection, do not perform any system administrative tasks or updates.

Crendon Insurance Brokers

Tech Support Scams Rising

A growing number of people are falling victim to computer tech support scams—up to15 per cent of Britons have been duped so far, according to Microsoft research. The scammers have two main strategies.

The first involves scammers setting up fake websites offering anti-virus downloads that are designed to fail on installation. The failed installation alerts users to call a phone number that connects them to the scammers. Then, using a variety of social engineering tactics, scammers trick users into believing their computers have a virus that can only be removed using the scammers' software. The scammers install their software on the users' computers or provide users with instructions on how to do so. This software can accomplish several illegal tasks, such as gathering credit card information, tracking users' keyboard movements or gaining unfettered access to users' computers.

The second tech support scammer strategy starts with actual phone calls—scammers call victims at home, pretending to be experts recruited to help with a computer emergency. Using fake websites and expert coercion, the scammers make it seem as if they are fixing problems on victims' computers. Scammers usually charge hundreds of pounds for their services—then things can escalate quickly. After gaining the victims' trust, the scammers ask to gain remote control of the victims' computers in order to 'fix' the non-existent problems. From there, scammers can install any number of nefarious programs, such as those that track users' Internet histories and compile their online banking information.

If you suspect you are being scammed: hang up. Reputable companies do not contact computer users unexpectedly. You can safely assume that any unsolicited communication concerning anti-virus software is illegitimate. If you are receiving unsolicited calls, register your complaint with the Telephone Preference Service at: www.tpsonline.org.uk/tps/index.html. If you believe you fell victim to a cyber-scam, contact Action Fraud, the United Kingdom's national fraud and cyber-crime reporting centre, at: www.actionfraud.police.uk.

Devon marketing firm slapped with huge fine for nuisance calls

A Devon marketing firm was fined £70,000 for making hundreds of nuisance calls. The firm used two third-party companies to make calls on its behalf to identify payment protection insurance claims. However, the firm failed to make sure that they were not calling people who had previously asked not to be called or who had registered with the Telephone Preference Service (TPS), the free opt-out service enabling people to record their preference on an official register and not receive unsolicited sales or marketing calls. The firm was responsible for 630 complaints that were made to the Information Commissioner's Office (ICO) and the TPS between March 2013 and February 2014. Factoring in this fine, the ICO has issued more than £500,000 total in fines for non-compliant live nuisance calls.

Director fined for illegally accessing phone company's databases

A 25-year-old company director was fined £500 plus £438.63 in costs and a £50 victim surcharge for illegally accessing Everything Everywhere's (EE) customer databases. The director managed three marketing and telecoms companies, and used details of when EE customers were eligible for a mobile phone upgrade in order to target them with services offered by his own companies. He successfully impersonated a member of Orange's security team to obtain details from their customer database, and gained access to 1,066 customers' records. EE quickly realised the breach and alerted the ICO.

Hotel-booking website fined after data breach exposed customer payment details

A hotel-booking website was fined £7,500 after a vulnerability allowed hackers to access the full payment card details of 3,814 customers. Although customers' payment details had been encrypted, administrators mistakenly stored the encryption key with the data, letting the hackers easily access the customers' full card details—even the three-digit security code that is needed to authorise payments. The website would have received a £75,000 penalty, but the ICO was required to consider the impact such a hefty penalty would have on the company's finances.

CYBERRISKS&LIABILITIES_
NEWSLETTER

Crendon Insurance Brokers Ltd
11 Greenfield Crescent
Birmingham, West Midlands, B15 3AU
0121 45 45 100
www.crendoninsurance.co.uk