ELSEVIER

computer FRAUD & SECURITY

ISSN 1361-3723 May 2020

www.computerfraudandsecurity.com

Featured in this issue:

Is there a silver bullet to stop cybercrime?

While the benefits of the latest mobile devices, smart capabilities or automated processes can't be disputed, the need to be constantly vigilant goes hand-in-hand with them.

This is especially true for businesses and banks, pressured by tech-savvy vendors and customers to adopt the latest payment methods. Fraud continues to be a top concern, and dealing with it is a constant battle. However, with the right mix of fraud controls and resources, there is a way to gain the advantage, says James Richardson of Bottomline Technologies.

Full story on page 6…

Stress-testing the skills gap

Cyber security expertise is still not sufficiently distributed, pushing up salaries and causing over-demand and stress among cyber security professionals. Yet cyber security is critical to every organisation.

Skills gaps aren't going away on their own. They must be attacked head-on with the appropriate training to bridge the skills gap from within. There's no time to wait and see how things play out before resolving the risks. People are behind the problem and they are also the biggest part of the solution, reckons Melanie Jones at Global Knowledge.

Full story on page 9…

A multi-cloud world requires a multi-cloud security approach

More than a third of global organisations store data in shared or public cloud environments. And around the same proportion store data in a private cloud.

As organisations move to multi-cloud architectures, malicious actors are looking to capitalise on any new attack vectors that this opens up, such as data and application sprawl and possible misconfiguration of cloud infrastructure. A holistic cyber security strategy will help to mitigate the risks inherent in a multi-cloud environment, while enabling the organisation to reap the business and technology rewards associated with it, explains Rory Duncan of NTT UK.

Full story on page 11…

Cybercrime in a time of coronavirus

An alert issued jointly by the US Department of Homeland Security's Cyber security and Infrastructure Security Agency (CISA) and the UK's National Cyber Security Centre (NCSC) warns that so-called advanced persistent threat (APT) groups are exploiting the Covid-19 pandemic to ramp up operations targeted against organisations involved in responses to the emergency at both national and international levels.

"These organisations include healthcare bodies, pharmaceutical companies,

Continued on page 3...

Contents

...Continued from front page
academia, medical research organisations and local governments," the alert says.

APT groups are typically state-run or state-sponsored actors and so CISA and NCSC see a political angle to these operations.

"APT actors frequently target organisations in order to collect bulk personal information, intellectual property and intelligence that aligns with national priorities," they say. "The pandemic has likely raised additional interest for APT actors to gather information related to Covid-19. For example, actors may seek to obtain intelligence on national and international healthcare policy, or acquire sensitive data on Covid-19-related research."

The agencies are investigating a number of attacks using 'password spraying' – ie, brute force login attempts. They have also seen a number of websites being actively scanned for potential software vulnerabilities.

It's believed that the majority of the attacks are emanating from Russia and Iran, although some have been tentatively traced to China. In the UK, attacks have been particularly focused on research institutions and universities, although there's no evidence so far that any have been successful.

The alert is here: www.us-cert.gov/ncas/alerts/AA20126A.

The Federal Bureau of Investigation (FBI) also issued an alert concerning phishing campaigns being mounted against US healthcare providers. "These attempts leveraged email subject lines and content related to Covid-19 to distribute malicious attachments, which exploited Microsoft Word document files, 7-zip compressed files, Microsoft Visual Basic script, Java and Microsoft executables," it said. The alert is here: https://bit.ly/2Z0hzGj.

Google has also been tracking state-backed attacks related to the pandemic.

"Hackers frequently look at crises as an opportunity, and Covid-19 is no different," it said. "Across Google products, we're seeing bad actors use Covid-related themes to create urgency so that people respond to phishing attacks and scams. Our security systems have detected examples ranging from fake solicitations for charities and NGOs, to messages that try to mimic employer communications to employees working from home, to websites posing as official government pages and public health agencies. Recently, our systems have detected 18 million malware and phishing Gmail messages per day related to Covid-19, in addition to more than 240 million Covid-related daily spam messages."

The firm's Threat Analysis Group (TAG) has identified more than a dozen state-backed groups using Covid-19 themes as lures for phishing and malware attacks. One targeted the personal accounts of US government employees, using offers of free meal vouchers or by impersonating health organisations. International health organisations have become a focus for many campaigns. The Google report is here: https://bit.ly/2SY6S3r.

One thing that CISA, NCSC and Google all agree on is that phishing and malware attacks overall have not risen in volume. The pandemic-related attacks represent a change in focus rather than additional malicious activity.

A monitoring unit within the European Union (EU) claimed that it has seen a large-scale disinformation campaign launched from Russia. "Pro-Kremlin media outlets have been prominent in spreading disinformation about the coronavirus, with the aim to aggravate the public health crisis in western countries, specifically by undermining public trust in national healthcare systems," says a report quoted by The Guardian.

Cardiff University's centre for crime and security research participated in the monitoring and said that, rather than generating false information itself, the Russia-backed campaign was providing a wider distribution of propaganda, conspiracy theories and fake news originating from China, Iran and far-right groups in the US.

Since 23 March, UK tax authority HMRC has issued requests to ISPs to take down 292 websites being used for phishing scams related to Covid-19, most of which were impersonating HMRC or other official bodies. In addition, scammers have been targeting the HMRC's Job Retention Scheme, which pays 80% of the wages of furloughed employees at firms affected by the pandemic. The phishing emails attempt to steal bank account details.

Meanwhile, the World Health Organisation (WHO) reported that it had seen a five-fold increase in cyber attacks against its platforms and employees. Around 450 active WHO email addresses and passwords were leaked online, alongside credentials belonging to thousands of other people working on the pandemic response.

Study reveals real cost of cybercrime

A study carried out by researchers at the University of Portsmouth claims to be the first to really examine the harm to individuals caused by cybercrime.

Commissioned by the Home Office and Her Majesty's Inspectorate of Constabulary, Fire and Rescue Services, its aim was to assess the nature and impact of cybercrime and the kind of support that victims could expect.

"There has been a perception that cybercrimes don't have as bad an impact as some physical crimes, but this report shows that computer misuse crime has similar, and in some cases a worse impact, than comparable traditional crimes such as burglary," said Professor Mark Button, director of the Centre for Counter Fraud Studies at the Institute of Criminal Justice Studies, University of Portsmouth and leader of the research team. "We found victims who compared the cyber attacks to physical assaults."

Some victims even contemplated suicide as a result, he said.

Part of the issue is that many victims are not taken seriously when they try to report crimes, and the understanding of cybercrime among authorities is patchy and often faulty.

The researchers found poor classification of computer misuse crime by authorities and they recommend new systems for reporting. They suggest regular monitoring and evaluation of the classifying procedures at Action Fraud and the National Fraud Intelligence Bureau to make sure they are accurate.

The report finds that the 'Action Fraud' brand has been a barrier to some reporting.