January 2017

Cyber Matters

Your essential guide

In this issue:

- Were the 2016 Cyber Threat Predictions Right?
- Is Cybergeddon Coming in 2017?
- What Lies Ahead This Year?

01704 542 420
info@p-ccomms.com

Were the 2016 Cyber Threat Predictions Right?

In our first Cyber Matters of 2017, we thought we would reflect on last year's cyber predictions and capture the threats we think are likely to feature in the next 12 months.

A key characteristic of annual threat predictions is that they rarely change from previous forecasts. For years now we have seen recurring warnings of the rise of cybercrime and mobile malware, that terrorists will use cyber to attack critical national infrastructure (CNI), and that the Internet of Things (IoT) will wreak online havoc. Expect more of the same this Christmas.

Whilst a rise in cybercrime has been a predictable feature for many years, Ransomware was specifically anticipated to grow significantly in 2016. Unfortunately, this indeed came to fruition and Trend Micro claimed this week that new ransomware families soared by 400% between January and September. It has also been claimed 20% of organisations worldwide suffered ransomware-related incidents this year and 1-in-5 small businesses never got their files back, even after paying up.

Whilst ransomware is not new, this year we saw significant changes in the range and sophistication of techniques. Previously the norm was for individuals to receive pop-up messages from fake anti-virus companies threatening that their device was crippled with malware, or even from law enforcement threatening users with arrest for online violations, unless they paid a ransom. However, 2016 saw a proliferation of crypto-ransomware where cybercriminals take aim at the most valuable part of a system - the data.

The rapid growth of the '*Ransomware as a service*' model, whereby ransomware operators lease their infrastructure to other customers, has also enabled non-technical users to join the fray.

As expected, the number of IoT devices grew significantly in 2016. Although many of these innovative and (mostly) useful devices are increasingly integral to our everyday lives, few are designed with cyber security and data privacy in mind. The development of cyber capability, along with security weaknesses in IoT devices, now enables skilled and motivated individuals to conduct low equity, high impact attacks on a worldwide scale. This was demonstrated recently after two of the largest ever Distributed Denial of Service (DDoS) attacks were facilitated by an army of compromised smart devices (known as

Continued…

the “Mirai” botnet). This botnet was assembled thanks to weak default passwords found in internet-connected cameras.

Another predicted threat that materialised in 2016 was Business Email Compromise (BEC). This technique, sometimes referred to as *whaling*, involves sending socially-engineered emails to employees which imitate legitimate email contacts such as that of the CEO or CFO. The unsuspecting employee is then pressured and coerced to authorise a payment as requested. In June, the FBI warned that they had discovered a 1300% increase in BEC attempts since January 2015, and since October 2013, hackers have attempted to send £2.2 billion in 22,000 separate cases.

Is Cybergeddon Coming in 2017?

Cyber threats are undoubtedly mounting in scale and sophistication, but what are the chances of the ‘Big One’ (i.e. a cyber-attack that cripples a nation’s CNI or causes widespread blackouts) happening next year?

It can be argued that it is actually happening already, as seen with the widespread IoT DDoS attacks, the CNI attacks against a Ukrainian power station and the $81 million Bangladesh bank heist.

Whilst many observers might be awaiting a single catastrophic cyber event in 2017, these irregular, but significant attacks, are actually building knowledge, experience and cyber resilience as they occur, so the ‘big one’ becomes less likely, albeit not impossible.

What lies ahead this year?

2017 SME THREATS

RANSOMWARE

As we have seen, 2016 was the Year of Ransomware and it is unlikely to change significantly next year. Enterprise-targeted ransomware attacks have become mainstream and will continue to be a major threat, while new methods of attack may include exploiting vulnerable web servers as an entry point to gain access into an organisation's network. Ransomware-as-a-service, custom ransomware for sale in dark markets, and creative derivatives from open-source ransomware code will also pose a significant threat. We also expect Mobile ransomware to continue to grow.

CLOUD SERVICES

During the past few years, the rapidly growing use of cloud services and an increase of new devices are challenging traditional methods of protecting everything digital. Increasing amounts of sensitive data and business-critical processes are shifting to public and hybrid clouds. Attackers are adapting to this shift and will seeks to attack cloud infrastructure.

INTERNET OF THINGS

The IoT encompasses thousands of types of devices in every industry. IoT should be thought of as networks of devices enabling and offering services, many of which are cloud-based. The threat is multifaceted; ranging from ransomware to cloud. IoT devices will also be useful attack vectors into control, surveillance, and information systems, as seen with the recent Mirai malware.

BEC AND BPC

Simple-but-effective Business Email Compromise (BEC) attacks will continue to grow, while we will begin to see more hard-hitting Business Process Compromise (BPC) attacks like the US$81-million Bangladesh Bank heist.

THIRD PARTIES

Third parties such as vendors and contractors pose a risk to companies. Most have no secure system or dedicated team in place to manage these third-party employees. High-profile breaches of US chains Wendy's and Target illustrate how cyber criminals have become increasingly sophisticated.

GENERAL DATA PROTECTION LEGISLATION

European adoption of the General Data Protection Regulation (GDPR) in 2018 will mean a change of processes to comply. They comprise:

- A Data Protection Officer – resulting in a large bill for hiring, training, and keeping a new senior-level employee
- Users must be informed of their newly outlined user rights and companies must ensure users can exercise them
- Only the minimum data required to use a service must be collected. Enterprises must revise their data-collection practices to adjust

These changes will force enterprises to conduct a top-to-bottom review of data processing to ensure or establish compliance and segregate EU data from the rest of the world's.

Wishing all our readers a Happy New Year from the P&C Communications team.

Thank you for downloading this guide.

Please feel free to contact us on the details below if you have any questions or comments, or would like advice on any of your own cyber security issues.

01704 542 420
info@p-ccomms.com