16th November 2016

Cyber Matters

Your essential guide

P&C COMMS

In this issue

01704 542 420
info@p-ccomms.com

IoT Botnet Saga Rumbles On

The threat of Internet of Things (IoT) botnets was very publicly reiterated last weekend after what some new sites described as the largest internet blackout in US history. The attacks targeted the Domain Name System (DNS) services of Dyn, an internet performance management company, which prevented their servers from being able to resolve DNS queries for many popular web services including Amazon, Reddit, Twitter, GitHub and Spotify.

Who Was Responsible?

There has been much speculation about who was responsible after both ‘New World Hackers’ and ‘RedCult’ claimed responsibility. Whilst the culprits and the actual size of the attack remains unclear, Dyn have admitted the DDoS was in-part facilitated by the Mirai malware, an IOT botnet that targets Linux-based IoT devices such as DVRs, CCTV systems and IP cameras. It exploits devices that use default or simple passwords and was recently responsible for the record-breaking DDoS attacks against Brian Krebs and web-hosting company OVH.

Perhaps to avoid law enforcement scrutiny in the wake of these high-profile attacks, Mirai's author recently leaked the malware's source code. As expected, this has resulted in numerous botnets appearing and, now the botnet’s capabilities are available to a much wider audience, identifying the original creator has become much harder.

As if the previous record DDoS attacks were not enough of a wake-up call about the threat of IOT botnets, last week’s disruption serves as another key reminder of the importance of changing default passwords on internet-connected devices. To mitigate the threat, end-users should take more proactive action to secure their devices, but vendors can also assist by enforcing password changes upon installation. Although some vendors take responsibility and release patches for insecure devices, the fact remains that the passwords on some equipment cannot be changed and there will still be plenty of unpatched devices available for malicious hackers to use. Sooner or later an IoT botnet is likely to attack a service you or your business rely on, and a simple password change could help prevent your devices becoming part of the next attack.

Diagnosis Cyber

To offer support to SMEs in the face of the many growing cybercrime threats, last week our cyber security partners, PGI, held a unique cyber awareness and training event in their bespoke cyber academy in Bristol. whilst appreciating how cyber security may appear to be complicated and can invoke images of confusing and highly expensive solutions. In light of this, their aim was to reassure SMEs that cyber security does not have to be expensive or indeed complicated. The free event encompassed talks on cyber topics from industry experts, including warnings about emerging threats, new technologies and legal and insurance issues. The 50 attendees were also given the opportunity to attend free 1-2-1 sessions with cyber experts to receive advice on how to tackle cyber threats, as well as an open Q&A Panel with industry leaders. Attendees were also given the opportunity to watch live hacking demonstrations on phishing and social engineering attacks in the hope that businesses can more effectively identify and avoid these types of threat.

Jargon Buster: What is a Botnet?

A botnet is a number of Internet-connected devices that, although their owners are unaware of it, have been infected by malware and can be instructed to forward spam or viruses to other devices ('bots') on the Internet. The controllers (aka 'bot herders') can use botnets to spread malware or spam, or combine an army of bots to conduct DDoS attacks as described in our headline story.

Data Leakage from Mobile Apps

In what may come as a surprise to many mobile users, a study of 45 million transactions over a three-month period has revealed that Android and iOS users are equally vulnerable to a wide range of mobile security threats.

Privacy leakage was identified as the most serious problem, with too many apps sending metadata, location and personal identifiable information to the developer's server or an ad server.

For Android transactions, 0.3% resulted in some level of private data becoming available to a third party, with 58% of those exposing the phone's International Mobile Equipment Identity (IMEI) number, Media Access Control address and the International Mobile Subscriber Identity (IMSI) number. What is perhaps most surprising is that iOS apps for iPhones and iPads revealed more private data than their Android counterparts (0.5% resulted in privacy-related information being shared).

As employees are now increasingly using personal mobile devices to access business networks, this research demonstrates the need for businesses to enforce stricter mobile device management programs to protect users and network assets.

2017 – The Year of the……..?

As the end of 2016 approaches, we enter the period when security vendors publish their predictions for what cyber threats may emerge in 2017.

Whilst 2016 will be remembered as the year of the data breach, several obvious threats are likely to feature in the next 12 months: Mobile – Whilst a predicted rise in attacks against mobile devices has been repeatedly predicted for a number of years, many experts believe that 2017 really will be the year of significant attacks against mobile devices.

As this threat continues to grow and businesses increasingly utilise Bring Your Own Devices in the workplace, corporate breaches that originate on mobile devices will become a more significant corporate security concern.

Internet of Things (IoT) – The threat from IoT devices has been starkly highlighted in the past few weeks with the creation and exploitation of IoT botnets used in record breaking DDoS attacks. As more IoT devices are connected in 2017, the threat surface will increase accordingly.

Cloud - An attack to disrupt or take down a major cloud provider has the potential to affect a number of customers' businesses. As more organizations start to utilise cloud services, these attacks are likely to start finding their way into this new infrastructure, either by encrypted files spreading cloud to cloud or by malicious actors using the cloud as a volume multiplier.

Do you have a story for Cyber Matters?

We're always interested to hear your news and views on Cyber Matters and if you have a contribution, or a tip for a potential subject to cover. we may consider it for a future edition.

Let us know by emailing us from our website using the link on the next page, or give us a call on 01704 542 420.

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.

P&C
COMMS

01704 542 420
info@p-ccomms.com