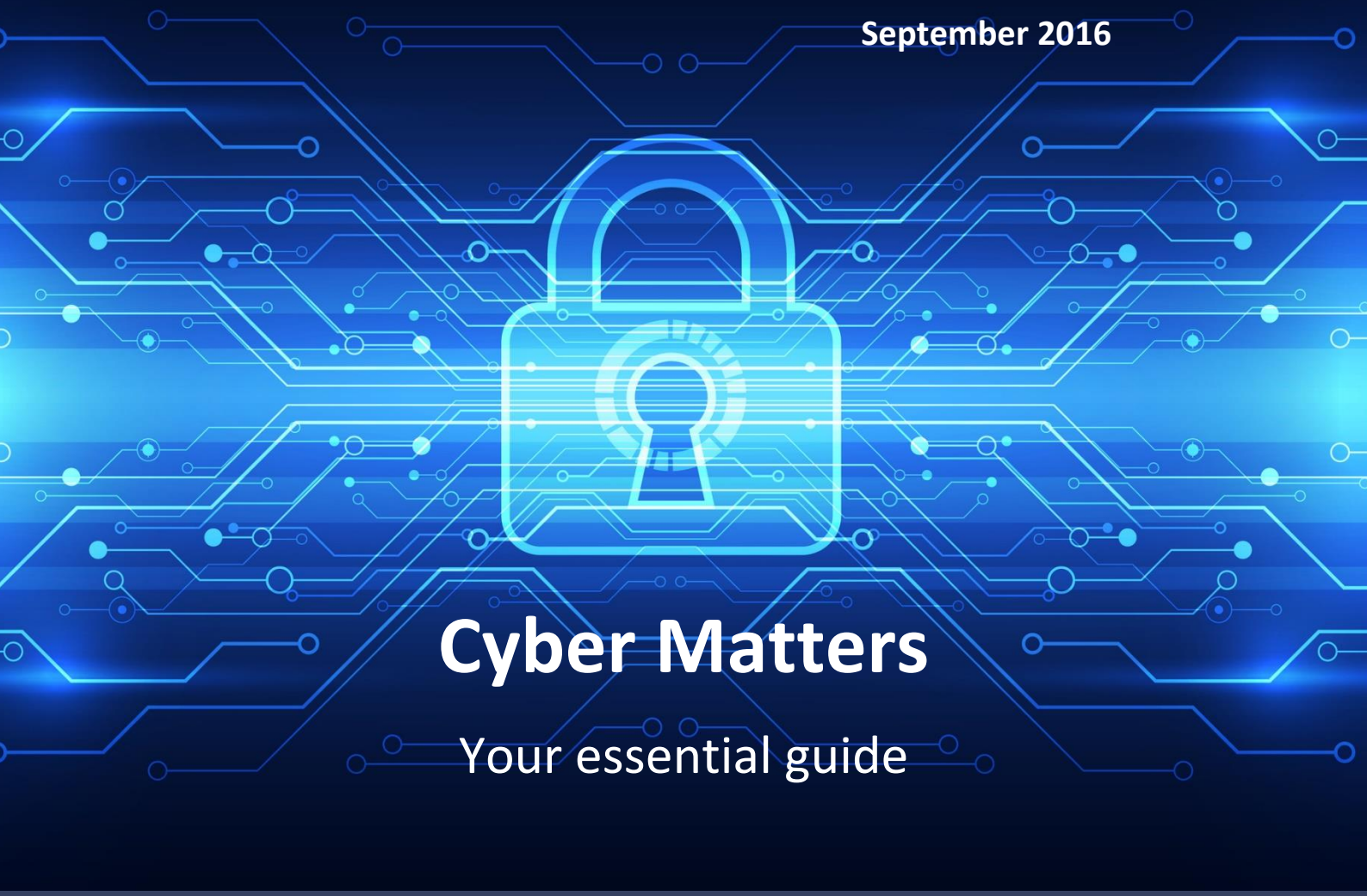
September 2016



Cyber Matters

Your essential guide

In this issue:

- What is Black Hat?
- USB Baiting Still Reaps Rewards
- 'Virtually Any Person' Can Be Made To Click On A Dangerous Link
- Bug Fear in 900 Million Android Devices
- Trojan Found in 155 Google Play Android Apps

01704 542 420
info@p-ccomms.com

WHAT IS BLACKHAT?

The annual Black Hat Conference is billed as the most intensely technical and relevant global information security event in the world and provides attendees with the very latest in security research and development.

Last year, two researchers grabbed the headlines with their Jeep computer hack which resulted in Chrysler having to recall 1.4 million vehicles.

The pair returned this year to demonstrate how to remotely force a Jeep into making sharp turns while travelling at speed. Amongst the other headlines were demonstrations of Internet of Things vulnerabilities, ways to bypass the security on Chip-and-PIN cards to enable unauthorised payments, and also the mysteriously-named 'Danger Drone'. This $500 custom-built drone carries common hacking software and has been designed to help hackers conduct remote attacks when physical access to a target is not possible.

Whilst many of these headline hacks are fascinating, the impact or likelihood of exploitation 'in the wild' can often be overstated. As we have seen from many previous stories in the Cyber Matters, the weakest link in the cyber security landscape continues to be the human factor; two social engineering sessions suitably demonstrated that this week:

USB BAITING STILL REAPS REWARDS

Elie Bursztein demonstrated the continued success of 'USB baiting'. This is where infected USB sticks are deliberately left outside offices in the hope curious workers will pick them up and insert them into workstations.

Bursztein's team dropped nearly 300 USB sticks at a University and found that 98% of them were scooped up. Worryingly, in 45% of the cases, people also interacted with files.

Not only is this risky as the device might be pre-loaded with executable malware, but more sophisticated attackers could also exploit such devices that use a HID (Human Interface Device). These can trick a computer into believing it is actually interacting

Continued…

with a keyboard and when the “USB stick” is plugged in, it could inject keystrokes and allow a hacker remote access to the victim’s computer. Bursztein’s work provides a timely reminder that whilst many attack techniques are well known, they still remain a large threat to a workforce with limited security awareness.

‘VIRTUALLY ANY PERSON’ CAN BE MADE TO CLICK ON A DANGEROUS LINK

Also this week, another researcher claimed that anyone can be tricked into clicking on dangerous links. She argued that even with effective awareness training against phishing emails and malware, it would be "highly unrealistic" to expect a person not to become a victim because of two factors: context and curiosity. Adding context to the malicious email was "by far the most frequent reason" for clicking, and natural human traits, such as curiosity, will forever remain exploitable. As employees cannot be ‘patched’ against malicious attacks, it is important that businesses ensure employees are provided with awareness training and that this is regularly and effectively reinforced.

BUG FEAR IN 900 MILLION ANDROID DEVICES

A set of Android security vulnerabilities has been discovered in Qualcomm chipsets that potentially affects more than 900 Million Android users. Researchers from Check Point encountered the four vulnerabilities (dubbed “Quadrooter”) in devices running Android Marshmallow and earlier. Affected devices included:

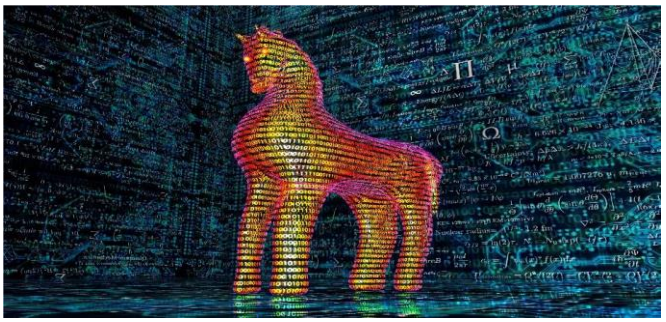
- BlackBerry Priv
- Blackphone 1 and 2
- Google Nexus 5X, Nexus 6 and Nexus 6P
- HTC One, M9 and 10
- LG G4, LG G5, and LG V10
- New Moto X by Motorola
- Sony Xperia Z Ultra

Continued…

Exploiting the bugs could potentially allow an attacker to take control over a device and gain access to its data, camera and microphone. Qualcomm has reportedly distributed security patches to phone makers and operators, but it is not clear how many of those companies have issued updates to customers' phones. Publication of their existence does now present a window of opportunity for malicious actors until the patches are widely adopted.

Despite the **potential** vulnerability, there is **no evidence of the vulnerabilities currently being used for malicious attacks.** Android users can check if their device is vulnerable to Quadrooter by using Checkpoint's free app. This story provides a timely reminder of the importance of regularly downloading security updates and Android owners should only download apps from the official Google Play store to ensure that they are protected against the latest security threats.

TROJAN FOUND IN 155 GOOGLE PLAY ANDROID APPS



In a bad week for Android, it was also reported that there are currently 155 Android apps on the official Google Play Store infected with the Android.Spy Trojan. The .305 version is a newer variant of the Android.Spy family which was previously seen in April 2016. Google have yet to remove all of the infringing apps and users have been warned against apps offered by developers including MaxMitek Inc, Fatty Studio, Gig Mobile, TrueApp Lab, Sigourney Studio, Doril Radio.FM, Finch Peach Mobile Apps, and Mothrr Mobile Apps.

As with the original trojan, once a user has downloaded the affected app, Android.Spy.305 will begin collecting data on the device including the user's email address, OS language, OS version, device name and model, and IMEI. Whilst the trojan is currently only focused on delivering adverts and not stealing any sensitive data, the information it is gathering can be very useful for future technical attacks and for social engineering purposes.

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