19th October 2016

Cyber Matters

Your essential guide

P&C COMMS

In this issue

01704 542 420
info@p-ccomms.com

Yahoo Breach Fallout Continues

It is a fortnight since news first broke of the biggest data breach in history, and the pressure continues to mount on Yahoo to disclose how much it already knew about the breach in 2014; did they intentionally delay disclosing the issue to a potential acquirer (Verizon)?

When they first publicly disclosed details of the attack (which resulted in the loss of data for 500 million users), Yahoo were at pains to say that they were the victims of a state-sponsored attack, although little supporting evidence was presented to suggest that this was indeed the case. This raises an interesting question regarding the reporting of such high profile breaches: do companies perceive that the public will have greater empathy and perhaps be less critical of a company if they have been the victim of a state-sponsored attack as opposed to a run-of-the mill criminal? In fact, an increasing number of security experts are now suggesting that the massive breach was indeed carried out by criminals and not a nation state.

Recent reports have also suggested that the final number of records lost could be closer to 1 billion. Regardless of the final number, one of the main criticisms of this case is not necessarily how Yahoo lost the data two years ago (since, other than size, this was no better or worse than any number of publicised large data thefts), but more about why it took them so long to acknowledge it and the time it took to notify customers to take remedial action.

Large-scale data breaches will continue to be mainstream and it is important that companies continue to protect client data proportionately. However, as this recent case demonstrates, the integrity and reputation of a company will more likely be judged by the professionalism, honesty and openness in which a company responds. It is yet another lesson for company board members, in preparation for the breaches that could one day happen to them.

iOS 10 Zero-Days Worth $1.5 million

Anyone looking for a shortcut to becoming a millionaire might like to consider life as an iOS vulnerability hunter. In a clear demonstration of the value of zero-day vulnerabilities, Zerodium, a company that buys exploits, has significantly raised the price it will pay for an iOS zero-day. Having previously paid $1 million each for three iOS 9 zero-days, they have recently offered to pay $1.5 million for a remote exploit that allows a third party full control over an iOS 10 device.

Continued…

Budding bug hunters should note that Zerodium will only pay for exploits that work against the latest patched iOS version, so they are no longer interested in iOS 9 exploits. Conversely, hackers can offer any zerodays directly to Apple via its private, invite-only bug bounty program, for the significantly lower reward of $200,000.

Jargon Buster: What is a Zero-Day?

A zero-day (aka 0-day) vulnerability is an undisclosed software vulnerability that can be exploited to adversely affect computer programs, data or a network. It is referred to as a zero-day because it is not publicly reported or announced before becoming active, leaving the software's author with zero days in which to create patches or advise workarounds to mitigate against its actions.

Insider Threats On The Rise

With an increasing number of companies embracing mobile working and enabling staff to connect personal devices to corporate networks, the risk of insider compromise (either by accident or through malicious action) is increasing.

This has been highlighted by a recent study on insider leaks by cloud security company Bitglass, which revealed that one in three of the organisations they surveyed had experienced an insider attack. Over half of the respondents (56%) said such attacks have gone up in the past year. The survey also revealed that carelessness is a greater problem than malicious action, with 71% experiencing "inadvertent leaks", while only 61% attributed attacks to malicious insiders.

On a positive note, 64% of the organizations reported that they can now detect breaches within a week (compared to 42% last year), and 57% believe insider threats can be reduced by employee training. Whilst protecting against malicious insiders is notoriously difficult, ensuring employees are suitably trained and encouraging them to adopt good cyber hygiene in the workplace will significantly help mitigate the risk of inadvertent leaks.

The Biggest Just Got Bigger as DDoS Records Tumble

Being forced to take his security blog offline due to a significant two-week long DDoS attack, Google's Project Shield has come to Brian Krebs' rescue by agreeing to provide him with free DDoS mitigation services.

Krebs' world renowned site previously received free protection from Prolexic (which was acquired by Akamai), but having recently exposed vDos, the Internet's most popular DDoS-for-Hire service, his site was subject to an escalating DDoS attack which eventually peaked at a record level of 620 Gbps.

With the offer of free support subsequently being withdrawn, and no other company able to offer free DDoS mitigation, Google's Project Shield stepped in to offer their services to Krebs and get his site back online.

Project Shield was unveiled earlier this year to provide technical support for smaller news organisations, human rights, and/or elections monitoring services. Whilst some sceptics are calling this a publicity stunt, it is an important intervention by Google and demonstrates the high regard given to Brian Krebs' investigative journalism.

Although the DDoS attack against Krebs' site set a new record for the largest DDoS in history, this record was eclipsed just a few days later with an attack against web-hosting company OVH that topped the 1 Terabit per second barrier.

It is not known whether this attack was mounted by the same botnet, but similar to the DDoS against Krebs, OVH have claimed that it was attacked by a botnet of compromised smart devices. During the attack, they provided Twitter updates on the number of devices in the botnet, which at one point included more than 145,000 devices.

This significant escalation in DDoS capability using vulnerable smart devices demonstrates how cyber-criminals are increasingly looking to exploit IoT (internet of things) devices due to their high availability and lack of sophisticated security.

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