Signals

Quarterly security assessment

Q3 2016

CommonwealthBank

Ben Heyes
Chief Information Security and Trust Officer, Commonwealth Bank

Signals aims to empower business executives with unique insights into the cyber threat environment and advice on the strategies and controls necessary to ensure a robust defence.

This advisory was prepared by our security analysts for business leaders that trust Commonwealth Bank as their preferred supplier of financial services.

In this edition, we provide a deep dive on scams that impersonate your senior executives or suppliers in order to transfer funds into the accounts of criminals.

We hope and anticipate the report will filter out the noise from media reporting of cyber security events and provide context and confidence for your security strategy.

Cyber Security:

Trends and Observations

Key trends observed during the quarter

> “Information stolen in these attacks was listed for sale in underground forums for $10,000 - $20,000 per database”

Point of Sale networks targeted

The hospitality industry was the fastest growing target for malware-based attacks in 2015, and events of the last quarter suggest profit-motivated criminals continue to target the industry. In August, Oracle-owned MICROS[i], one of the world's largest providers of Point of Sale systems, suffered a very public data breach, while attacks were also recorded against several competing providers. Some of these attacks allow criminals to capture the credentials required for remote administration rights for entire networks of Point of Sale terminals used in hotels, bars, restaurants and associated retail outlets. Information stolen in these attacks had been placed on sale in underground forums for $10,000 - $20,000 per database. Australian Point of Sale system suppliers are among those targeted[ii].

CHECKLIST

- MICROS customers are asked to reset account passwords to its online portal. The volume of attacks against competing PoS vendors suggests the same action would be prudent for accounts used for remote administration of any brand of Point of Sales system.
- Consider limiting remote access to PoS systems, isolating them from the corporate network (where practical), and requiring two-factor authentication for credential changes.
- If you learn that your Point of Sale system has been compromised, notify both your bank and law enforcement to ensure affected customers can be offered assistance immediately.

Aussies smashed with Smishing (SMS Phishing)

Australian regulatory bodies have warned about the increased use of 'Smishing' (phishing over SMS) to steal account details from smartphone users, both in Australia and across the globe. The Commonwealth Bank Cyber Security Centre has seen reports from a reliable Government body that the number of Smishing campaigns targeting domestic financial institutions, online media, e-commerce sites and cloud service providers has grown 500 percent since the start of 2016.

CHECKLIST

- Instruct staff to be vigilant about SMS messages featuring links to web sites that ask for their user credentials.
- Advice to staff on Smishing will vary depending on your organisation's use of SMS and in-app messaging. The best advice is to be wary of any message that asks them to click on links or provide credentials. If unsure, the safest course of action is to contact your service provider's call centre directly using its publicly-listed number.

Phishing goes professional

Several recent phishing campaigns targeting Australians have featured precise replicas of the imitated organisation's brand design and competent use of English, where the typical phishing email might historically have been easier to identify thanks to spelling errors, poor grammar and inconsistent design. Underground cybercrime forums also feature advertisements asking for copywriters to clean up grammar in phishing campaigns[iii]. Both suggest organised cybercriminal groups now have the necessary skills to accurately mimic the designs of their targets, increasing the difficulty for staff to detect phishing scams.

CHECKLIST

- Ensure staff awareness campaigns reflect the growing sophistication of phishing campaigns. Provide a more exhaustive list of indicators than language or design errors.
- Consider conducting phishing simulation exercises against your staff to raise the level of awareness about how to detect phishing attacks. This edition of Signals features a 'Deep Dive' on CBA's experience with its phishing simulation program on Page 7.
- Commonwealth Bank offers our valued clients an eLearning module on email security should you wish to deploy to your staff. Talk to your relationship or account manager for access.

By the Numbers

500 percent

increase in Smishing attacks against Australian targets in 2016

Macro-based malware grew

39%

last quarter[vii]

1 in 6 cyber jobs

advertised in Australia will never be filled due to lack of skills.[viii]

Cyber Security:
Trends and Observations

> “Even taking into account that many attacks are not reported, **the FBI has received a 300 percent increase** in reports”

World’s largest DDoS attacks recorded

A series of recent attacks on international firms suggests the capability of at least one threat actor that employs Distributed Denial of Service (DDoS) attacks far exceeds the defensive capabilities available on the market. On September 20, French internet service provider OVH claimed to have recorded botnets able to throw over 1 Tbps at victims. Two days later, attackers targeted the web site of cyber security journalist Brian Krebs in attacks that exceeded 620 Gbps. Earlier in the month, a Chinese gaming company claimed to have been hit by a 470 Gbps, 110m packet-per-second attack. The attack on KrebsonSecurity was so severe, his DDoS mitigation service – which provided services pro bono – had little choice but to turn off its protection for the web site, resulting in a three-day outage.

CHECKLIST

- Consider subscribing to DDoS mitigation services if you are a target industry – over 80% of attacks are waged against gaming, media and entertainment firms, while telcos, software companies, educational institutions and financial service providers tend also to be targeted.
- Infrastructure hosted in Australia would be unlikely to experience attacks of 100 Mbps+ due to limited international connectivity to Australia. Targeted industries should nonetheless consider placing sensible limits on the volume of traffic from suspect international sources.

Ransomware rampage continues

Reports from both the US and Australian Government indicate the use of ransomware – a form of malware that encrypts a victim’s hard drive prior to an attacker seeking payment to unencrypt the device – continues to grow exponentially.

Even taking into account that many attacks are not reported to law enforcement, the FBI has received a 300 percent increase in reports from victims (4000 per day in first half of 2016 compared to 1000 per day in 2015). The ACCC’s ScamWatch (which groups Ransomware and Malware attacks as one category) reports that the average amount lost by Australians reporting these attacks leapt from an average of ~$15,000 earlier in the year to $50,000 in August 2016.

CHECKLIST

- Make regular backups of systems, and keep some of those backups offline (as some ransomware attacks will encrypt drives attached to the system).
- Disable executables and macro scripts from files transmitted via email.[iv]
- Implement application whitelisting and/or controls that prevent programs from executing from temporary folders associated with web browsers.
- Consider conducting phishing simulation exercises against your staff to raise the level of awareness about how to detect phishing attacks. This edition of Signals features a ‘Deep Dive’ on CBA’s experience with its phishing simulation program.
- Offer your staff security awareness training to reduce the risk of malware.

Nation-states lose control of cyber weapons

Cyber weapons developed by nation-states continue to find their way into the hands on non-state actors. These weapons usually take the form of software crafted to exploit zero-day (previously unknown or undisclosed) vulnerabilities in common hardware and software to intercept communications or gain unauthorised access to systems[v]. A set of exploits that were assumed to be developed by actors affiliated with the US National Security Agency (NSA) were anonymously dumped online in August, allowing members of the public to download them. The dump included exploits designed to compromise network equipment from Cisco, Fortinet and others, forcing the vendors to rush to develop patches in an effort to protect customers. Cisco has reported that the exploits were used in attacks against its customers before the company could make a patch available.[v]

CHECKLIST

- Expect intelligence services to continue the pursuit of offensive capabilities. A cold war of sorts has developed between nation-states – underpinned by a black market for exploits and vulnerability information. The volume of this activity will invariably lead to further leaks of exploits into the hands of non-state actors.
- Ensure your patching processes can respond as quickly as practicably possible when zero-day vulnerabilities are disclosed in the technologies that underpin your digital services.

By the Numbers

US$6.5 Million
Average cost of data breach to an organisation[ix]

US$170K
Median cost of data breach to an organisation[ix]

620 Gbps
Record for largest DDoS attack in history against a single site (by traffic volume)[x]

The FBI receives 4000
reports per day of ransomware infections

Deep Dive:

Email Payment Fraud

Educate your accounts teams on the latest scams

Brett Winterford
Senior Manager, Cyber Outreach and Research

The speed at which transactions can be processed today require accounts teams to be more vigilant than ever when making payments.

In recent months, many Australian organisations have received email scams that appear to be valid requests to third parties, such as payment instructions or invoices. The two most common of these email payment frauds are:

- a perpetrator sends an email to a company impersonating one of its suppliers, requesting the bank account numbers for the supplier be changed in their backend systems. This results in funds being diverted to the perpetrator's account when the next payment is made.

- a perpetrator impersonates the client's CEO, COO or another senior executive, asking their accounts staff to make an urgent payment to a supplier on a bank account accessible by the perpetrator.

While these scams might sound simple, they have proven exceptionally effective.

In February 2016, the FBI announced that after collecting two years of data, the 'CEO Email' scam has cost global organisations US$2b. Six months later in June of 2016, the bureau reported that losses from the scam were closer to US$3.5 billion. The Australian Federal Police also reported a notable spike in this activity closer to home since the start of this year.

How Does the Scam Work?

The criminal actors behind these scams have become far more studious, patient and willing to invest money and effort in the quest for larger payouts.

Scams analysed by the Commonwealth Bank Cyber Security Centre exhibited such a depth of research that on first appearance, it was assumed they required some level of insider knowledge. Attackers, however, can often find all the information they need for these attacks on the public internet. They engage in extensive reconnaissance using a combination of publicly available data and social engineering to extract the information critical to the scam.

For example, in order to impersonate suppliers, fraudsters may target organisations that have announced new business partnerships in the media, knowing that large transactions are likely to flow between the two organisations in the months ahead. The criminal groups behind these attacks have clearly learned that a little patience pays off handsomely, as business-to-business payments tend to be far larger sums of money than what can be gained by attacking the online banking sessions of an individual that applies daily payment thresholds to their account.

These email-based schemes are also growing more professional – some have clearly enlisted the help of graphic designers or copywriters to help make requests for payment appear more legitimate (advertisements for these services have been reported in underground cybercrime forums). Organised criminal groups have even hired unwitting accomplices in Australia who, responding to offers of 'work from home' opportunities as accounts or call centre staff, are roped into making follow-up calls or moving funds through their personal accounts on behalf of these criminal groups.

The perpetrators of the 'CEO email' version of these scams are also doing a lot more reconnaissance. The hierarchical structure of a targeted organisations can be gleaned by either buying the victim's 'org chart' from sales lead generation services, and by studying the connections of executives listed on professional social networks such as LinkedIn. The attackers select an individual to email based on their ability to authorise transactions, as well as their proximity (or lack thereof) to the highest authorities in the organisation. With a few simple phone calls they might also ascertain when C-Level executives are going to be out of the office on leave or on business.

> "Email-based schemes are **growing more professional** – some have enlisted the help of graphic designers or copywriters"

With this information in hand, the fraudster might email their target, impersonating the CEO that is on leave or away on business, demanding that an urgent and confidential payment be made to close out a top secret

Deep Dive:
Email Payment Fraud

> While there are standardised tools an organisation can deploy to prevent spoofing, it is impossible to provide a 100% guarantee

acquisition, for example. The emails can also feature spoofed (fake) threads of email conversation between senior members of the company to lend a greater sense of legitimacy to the scam.

The Art of Impersonation

In all of these cases, fraudsters have several means of making the sender's address appear legitimate - as either the same or very similar to the actual email address of the senior manager they have set out to impersonate.

In its crudest form, the attacker might simply register a webmail address in the CEO's name for use when the CEO is known to be on leave or on business, making it difficult for the victim to verify its authenticity.

Other attackers use homoglyphs – registering a domain that is strikingly similar to the target's (think Facebrook.com instead of Facebook.com).

The most sophisticated attackers actually spoof the company's domain (i.e. the email address in the 'from' field appears as the CEO's legitimate email address). While there are standardised tools an organisation can deploy to prevent spoofing [see 'Email Spoofing' explanation on page 6], there is no 100% guarantee that an email address can't be forged. We recommend that accounts teams be told to assume that it is trivial for an attacker to send an email from any address within your domain – they should not rely exclusively on an address for determining the authenticity of a sender.

On very, rare occasions, mail can be sent from the manager's email address because the attacker has gained authorised access to that account, but in most cases a fraudster doesn't need to go to this effort. They simply need one person that can authorise payments to be fooled.

The best defence against these attacks is awareness. Accounts staff need to be made aware that they should never deviate from agreed payment authorisation processes, even when subject to pressure from a perceived authority.

How to spot email payment frauds:

- **The request claims to be urgent and/or confidential;**
- **You are requested to ignore standard payment authorisation processes;**
- **The request includes grammatical and spelling errors;**
- **The type of request and the language and formatting are unusual for the supposed sender;**
- **The 'reply to' email address is different to the sender's address.**

Deep Dive:
Email Payment Fraud

> To protect your organisation from spoofing-based attacks, **it is a very useful exercise to check the DNS settings** on your domains

Email Spoofing

How can an attacker spoof (forge or impersonate) an email from your CEO's email address?

The protocol that email is based on – SMTP (Simple Mail Transfer Protocol) – was developed with any-to-any messaging as its goal. By default, it has no inbuilt checks that an email has been sent by a person authorised to use that address.

Since the early 2000s, Internet standards bodies concerned about the proliferation of spam have developed email integrity and authentication standards to help validate that mail purporting to come from a given domain actually comes from IP addresses associated with that domain.

SPF (Sender Policy Framework) and DMARC (Domain Message, Authentication, Reporting and Compliance) are anti-spoofing standards that are free to implement, but for various technical and business reasons (such as the outsourcing of email marketing to third parties), many organisations have been slow to support them.

To protect your organisation from spoofing-based attacks, it is a very useful exercise to check the DNS settings on your domains to ensure they include both SPF and DMARC records:

- Generally the owner of a domain populates **SPF (Sender Policy Framework)** records with a whitelist of IP addresses associated with the organisation's authorised mail servers. If an attacker attempts to spoof your domain in an email sent to an organisation that also uses SPF records as part of their filtering of incoming email, the suspect email can be blocked or quarantined based on checks against DNS (domain name system) records.

- Assuming the owner of a domain uses SPF or DKIM (a similar standard that uses digital certificates to achieve the same result), an additional control called **DMARC (Domain Message, Authentication, Reporting and Conformance)** can be called upon to provide additional features. The domain owner publishes a DMARC record which describes how to handle spoofed emails (reject, quarantine, do nothing) upon SPF or DKIM failure. Better still, it provides domain owners with reports of the source IP addresses used in emails purported to be from its domain that have been received by other DMARC-enabled gateways.

These two controls in combination provide both a level of protection against spoofing and also some insight into when fraudsters are attempting to impersonate your domain.

Implementation of these standards requires that a System Administrator has gained a very solid understanding of where legitimate mail is sent from using your domain – and that sometimes might include authorised third parties. Misconfigurations can lead to legitimate email being blocked – a scenario that tends to land the IT security function in very stormy situations. It's thus advisable to implement the controls gradually, possibly one business unit or functional group at a time, testing each for any impact on mail delivery or service interruption that might need to be addressed before moving on to the next.

CHECKLIST

- Ensure your accounts/payments staff are aware of these attacks. Commonwealth Bank has developed A3 posters that clients can place around these teams to heighten their awareness – ask your relationship or account manager to forward them to you.
- Review payments processes and enforce strict compliance, ensuring there is clear separation of duties. Ensure that large or unexpected payments cannot be made without additional verification steps.
- Senior executives should promote a culture where staff are encouraged to question a process change that doesn't make sense, particularly with respect to payments.
- Check your SPF/DKIM and DMARC settings provide protection against and reporting on attempts to spoof emails from your domain.
- Ensure staff with the authority to make large transactions have completed security awareness training. Commonwealth Bank offers our valued clients access to eLearning modules on email security should you wish to deploy to your staff. Talk to your relationship or account manager for access.
- Consider deployment of phishing simulation against your staff to help them identify phishing attacks. See what Phishing Simulation has achieved for CBA on Page 7.

Deep Dive:

Phish Your Own Staff. It Works!

Phishing simulation at CBA has led to more resilient, wary staff

Sam Stapleton
Information Security Analyst (Learning and Awareness)

For all the sophistication of today's cyber weapons, the most common means by which cybercriminals steal data or gain unauthorised access to systems continues to be one of the oldest tricks in the book – phishing.

In phishing attacks, criminals send emails to an organisation's staff that either trick them into revealing sensitive information (such as system credentials or banking details), trick them into opening a malicious attachment that infects the user's computer, or directs them to a compromised web site that achieves the same result.

One of the many measures CBA takes to reduce the number of malware infections is use of a Phishing Simulation Service. This service aims to educate staff about the tell-tale signs that an email might be a phishing campaign, in the hope that over time they will become less susceptible to clicking on suspect links or attachments.

So What is a Phishing Simulation Service?

CBA's Digital Protection Group (DPG) regularly sends simulated phishing emails to staff – many of which ask them to click on links or to enter sensitive data. When a staff member takes the bait, they are redirected to a training page that features tips for identifying phishing emails. Additional training and assistance is made available to repeat offenders.

The practice of phishing your own staff is relatively new, so there isn't a lot of data available on how effective it is at reducing staff susceptibility to compromise.

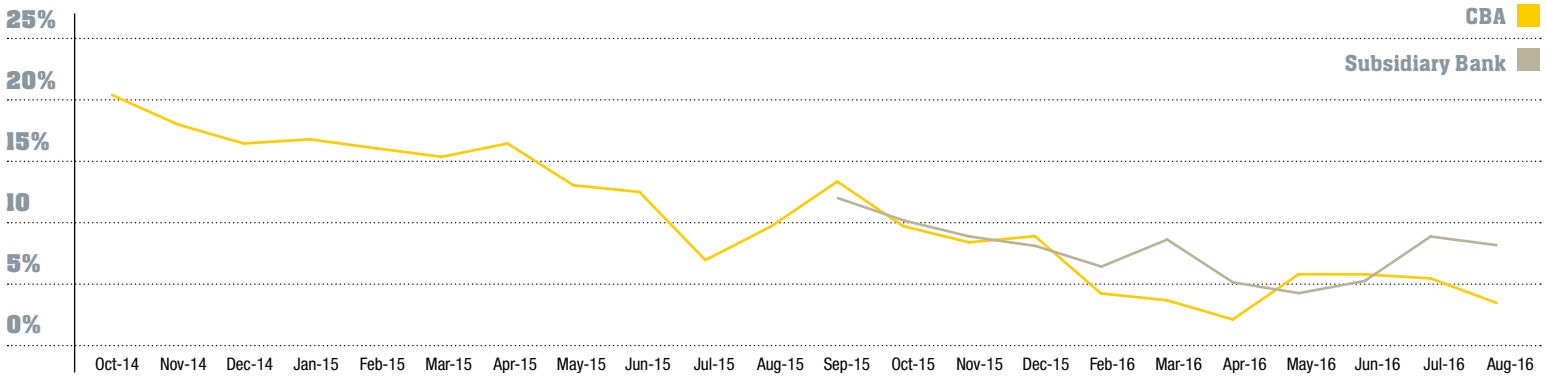
CBA's Digital Protection Group now has several years of data upon which to measure the impact of the Phishing Simulation Service.

As the chart below shows, the percentage of CBA staff that are compromised by simulated phishing emails has fallen from 20% to 4% over 18 months since the phishing simulation campaign commenced. And a more recent trial of the same service in one of our subsidiaries is already producing similar outstanding results.

This data demonstrates that phishing simulation is an extremely cost effective measure. It not only drives down the number of compromises of your network, but in doing so reduces the number of infections that highly skilled incident responders have to spend their time attempting to triage.

Brett Winterford, Mark Leung and David Szabo contributed to this analysis.

Staff Compromised by phishing simulations



Key Observations:

- More staff now correctly report phishing simulations as hoaxes. But more needs to be done to encourage this reporting.
- External suppliers were the most susceptible group to phishing simulations.
- Staff were most susceptible to phishing scams that mimic the organisation's internal processes.
- Staff were least susceptible to campaigns that offered free gifts.

Regulatory & Legal

New laws and legal precedents relevant to security strategy

> “Privacy regulators found Avid Life Media’s **security framework gravely inadequate** and lacking basic governance and oversight”

Australia brings cyber security to cabinet

In July, re-elected Prime Minister Malcolm Turnbull appointed Dan Tehan, MP as Minister Assisting the Prime Minister for Cyber Security. Tehan is charged with strengthening the relationship between Government and business and supporting implementation of the Government’s cyber security strategy. It follows the announcement in April of a Special Adviser to the Prime Minister on Cyber Security, Alastair MacGibbon.

CHECKLIST

- These two appointments represent a focal point for the business community to engage with Government on cyber issues.
- Commonwealth Bank will continue to play an active role in implementation of the Government’s cyber strategy and will seek to provide opportunities for the broader participation of our business partners on areas of shared interest.

Obama orders clearer cyber response plans

United States President Obama has released a major policy directive (Presidential Policy Directive 41[xxiv]) on cyber security incident response. The directive delineates US government agency roles during cyber incidents. It also highlights the importance of close communication and coordination with the private sector. The instruction provides a useful template for Australia to emulate when clarifying domestic roles and responsibilities follwing a cyber-incident.

CHECKLIST

- A clear articulation of roles and responsibilities is critical during a cyber incident. Ensure your organisation’s crisis management plans include how to respond to data breaches and other cyber incidents.
- The Australian Government plans to soon conduct a nation-wide cyber security incident response exercise. Please contact CERT Australia for more details.

Privacy Commissioners scold Ashley Madison over data breach

The Privacy Commissioners of Canada and Australia have released a report from a joint investigation into last year’s breach of dating web site Ashley Madison. Over 25GB of data from parent company Avid Life Media (including names, addresses and credit card details of clients) was published online. The privacy regulators found Avid Life Media’s security framework gravely inadequate and lacking basic governance and oversight. Further, Avid Life lacked documented information security and privacy policies or practices; an explicit risk management process, or adequate training to ensure all staff were aware of their privacy and security obligations. Avid Life Media, rebranded as Ruby, has agreed to an enforceable undertaking to address the issues.

CHECKLIST

- Understand your privacy and security obligations under Australian law by reading the Australian Privacy Principles[xi], particularly Privacy Principle 11.
- Beyond legislative requirements, be mindful of regulator expectations regarding security – see the Australian Privacy Commissioner’s Guide to Securing Personal Information[xii].
- Assess what security framework is most suitable for your organisation according to your scale and risk appetite. Larger enterprise might consider certification against ISO 27001[xiii] or adoption of the US NIST cybersecurity framework[xiv], smaller organisations might choose to map protections against the Australian Signals Directorate’s ‘Strategies to mitigate targeted cyber intrusions’.[xv]

Deep Dive:

A Private-Sector Test for Cyber Norms

We need to talk about 'hacking back'

Brett Winterford
Senior Manager, Cyber Outreach and Research

Cyber norms are usually the domain of nation-states and cyber policy wonks. But events in recent weeks suggest it's a discussion all of us may soon need to engage in.

The severity of a 620 Gbps Distributed Denial of Service (DDoS) attack [See Page 3] on the web site of cybercrime journalist Brian Krebs was such that his DDoS mitigation service provider could only afford to assist him on a pro bono basis for a 24-hour period before the costs of mitigating the attack became untenable.

Attacks like these – while never before at this amplitude - can be dialled up 'as-a-service' for $10 or $20 an hour. The cost of mitigation is several hundred thousand dollars a year. This speaks to the most pressing problem of cyber security: there is a colossal asymmetry between the cost of attack and cost of defence.

If the size of DDoS attacks maintain their current trajectory, the cost of mitigation will likely become too high for most organisations to bear. This dynamic puts huge pressure on organisations that rely on a digital presence to consider previously unthinkable options: such as attacking back in some capacity.

The legal and moral case for 'hacking back' or 'active defence' is far from settled, and a loosely related event to the DDoS on Krebs' web site is already testing the waters.

Prior to the attack on his web site, Krebs enlisted Dyn Research to investigate the actions of BackConnect[xvi], a DDoS mitigation firm that had on at least one occasion taken matters into its own hands to take down an aggressive adversary.

BackConnect was the target of a six hour DDoS attack of over 200 Mbps in early September and alleges that the attack was followed up with personal threats against its staff. In response, the company took the extraordinary measure of hijacking the IP space of the attackers (using what is termed a BGP hijack), to cripple the attack and to collect intelligence on the machines and actors directing it.

BGP hijacking is not a trivial matter. It compromises the trust network operators hold in each other when routing traffic between each of their networks – a trust that is relied on for the healthy functioning of the Internet. Any unilateral interference in Internet routing paths is deemed by ISPs and telcos to be unacceptable behaviour, irrespective of motive. (It's also inherently transparent to external observation[xvii].)

Several parties – spearheaded by the Dutch Government - are currently pushing for the creation of an international norm that prohibits interference in the 'public core' of the internet, such as routing paths.

Internet routing paths are otherwise self-governed by the service providers that route traffic. And that self-governance has kicked into gear:

"Once we let providers cross the line from legal to illegal actions, we're no better than the crooks, and the Internet descend into lawless chaos," wrote one poster on the North American Network Operators Group (NANOG) forum.

"BackConnect's illicit action undoubtedly injured innocent parties", the network administrator noted. "It's not self-defence any more than shooting wildly into a crowd to stop an attacker."

Other representatives of network operators on the list called for some form of communal sanction – be it refusing to peer with BackConnect, or seeking that it's ASN (Autonomous System Number) be revoked.

Bryant Townsend, founder of BackConnect, took to the same forum to humbly apologise for his act of desperation. Townsend claimed that he filed a police report prior to going on the offensive.

"The decision to hijack the attackers' IP space was not something I took lightly," he wrote to the forum, but didn't promise he wouldn't use the same means if put in the same position. After all, he noted, the attacks ceased and he expects the attribution data he collected to lead to successful takedowns and convictions of the offenders.

For better or worse, BackConnect's actions will undoubtedly inflame the debate on norms of behaviour in cyberspace. At what threshold is an attack so debilitating that the community would deem it acceptable for defenders to break some of the internet's most sacred rules?

CHECKLIST

- The Australian Strategic Policy Institute has recently surveyed a number of large Australian firms to seek a private sector view of norms of behavior on the Internet. Contact cyber-outreach@cba.com.au if you would like an advance copy of the resulting report.

Better Practice

The latest advice your technology team should consider when setting security policies:

Prevent Ransomware Infections

The FBI has updated its advice on preventative measures to protect an organisation from Ransomware infections. The advice has been made available as both a 9-page guide for CISOs[xviii] and as a neat summary.[xix]

New advice on mitigation against malicious email

The Australian Signals Directorate has offered some timely advice[xx] on mitigation against threats arriving in your organisation via email.

Practice, practice, practice

The US Federal Trade Commission has published advice[xxi] to help organisations prepare for the possibility of a data breach as part of their crisis management planning.

Review your patching processes

As previous analysis in Signals demonstrated, the window between the discovery of a vulnerability and its use in mass market exploit kits has narrowed to an average of ~8 days. The Australian Signals Directorate has called on organisations to review patching processes[xxii] to keep ahead of the threat.

Harden iOS

The Australian Signals Directorate has also refreshed advice[xxiii] for system administrators looking to harden iOS deployments against compromise.

Horizon Scan

Upcoming events of interest

2016 Oct 6

Sydney

Cybercrime guest lecture – Oxford University and UNSW

The University of New South Wales will host a guest lecture by University of Oxford criminologist Jonathan Lusthaus on October 6, 2016. Lusthaus will discuss his research into trust networks formed between participants in cybercrime networks. The guest lecture is presented by Commonwealth Bank as part of our sponsorship of both the sec.edu program at UNSW and of the Human Cybercriminal Project at the University of Oxford. Please contact cyber-outreach@cba.com.au if you would like to attend as our guest.

2016 Oct 14

Melbourne

Meet Sir Iain

The Australian Strategic Policy Institute is hosting a closed door panel session with Sir Iain Lobban, former director of GCHQ and an adviser to the Australian Government's cyber security strategy. Sir Iain Lobban will provide insights on his time at GCHQ, with lessons for both public and private sector organisations. Please contact cyber-outreach@cba.com.au if you would like to attend as our guest. Seats are limited.

2016 Oct 18-20

Sydney

Australian Information Security Association National Conference

Annual Conference for local industry group (NB: registration fees apply)

Footnotes

i: http://krebsonsecurity.com/2016/08/data-breach-at-oracles-micros-point-of-sale-division/

ii: http://www.theregister.co.uk/2016/09/20/exclusive_hackers_claim_pos_tech_firm_breach/

iii: http://blog.trendmicro.com/trendlabs-security-intelligence/the-french-dark-net-is-looking-for-grammar-police/

iv: https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view

v: https://motherboard.vice.com/read/what-we-know-about-the-exploits-dumped-in-nsa-linked-shadow-brokers-hack

vi: http://news.softpedia.com/news/shadow-brokers-beningcertain-tool-deployed-in-live-attacks-508455.shtml

vii: http://www.mcafee.com/us/resources/reports/rp-quarterly-threats-sep-2016.pdf

viii: https://www.csis.org/programs/strategic-technologies-program/cybersecurity/cybersecurity-workforce

ix: http://cybersecurity.oxfordjournals.org/content/early/2016/08/08/cybsec.tyw001

x: https://web.archive.org/web/20160922021000/http://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/

xi: https://www.oaic.gov.au/individuals/privacy-fact-sheets/general/privacy-fact-sheet-17-australian-privacy-principles

xii: https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-securing-personal-information

xiii: https://en.wikipedia.org/wiki/ISO/IEC_27001:2013

xiv: https://www.nist.gov/cyberframework

xv: http://www.asd.gov.au/infosec/mitigationstrategies.htm

xvi: http://research.dyn.com/2016/09/backconnects-suspicious-bgp-hijacks/

xvii: http://research.dyn.com/2016/09/backconnects-suspicious-bgp-hijacks/

xviii: https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view

xix: https://www.ic3.gov/media/2016/160915.aspx

xx: http://www.asd.gov.au/publications/protect/malicious_email_mitigation.htm

xxi: https://www.consumer.ftc.gov/blog/data-breaches-and-you-new-video

xxii: http://www.asd.gov.au/publications/protect/assessing_security_vulnerabilities_and_patches.htm

xxiii: http://www.asd.gov.au/publications/protect/ios-hardening-guide.htm

xxiv: https://www.whitehouse.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident

CommonwealthBank