Signals

Quarterly security assessment

Q1 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.

It reflects the calibre of guidance I provide executives and boards in my role as Chief Information Security and Trust Officer of Commonwealth Bank.

In this edition, our focus is on growing concerns around cyber-attacks on physical infrastructure, as well as a deep dive on our observations of DDoS activity in 2015.

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

> “Run hourly or daily **snapshots (backups) of data** to ensure a rapid rollback to a pre-infection state”

Cyber-attacks harm physical industries

Industrial control systems have proven to be vulnerable to cyber-attacks, with recent incidents causing physical damage to critical infrastructure such as power and water networks. US investigators have confirmed[i] that simultaneous service outages at three Ukrainian power utilities in late December 2015 were caused by a coordinated cyber-attack. Attackers engaged in extensive reconnaissance prior to the attacks, abused trusted identity credentials to gain remote access to systems, and used malware that wiped company drives after the incident to prevent system restoration. A specific form of identity-stealing malware (BlackEnergy) was found on systems at all three utilities, which had been delivered via spear-phishing emails sent to staff. Investigators were unable to definitively confirm that BlackEnergy was the malware responsible for harvesting the credentials used in the attack. Cyber intelligence organisations believe the attack was perpetrated by the Russia-based ‘Sandworm’ gang.

Reported attacks on US industrial sector, 2015[iii]

CHECKLIST

The US Government’s cyber emergency response team for Industrial Control Systems recommends[ii]:

- Isolating Industrial Control Systems, where practical, from internet connectivity and otherwise limiting communications to a single port on a restricted network path.
- Use of application whitelisting to protect systems against execution of malware.
- A routine process of verifying the currency of access management credentials distributed to staff.

Hospitals targeted in malware campaigns

Four hospitals in the United States[vi] and two hospitals in Germany fell victim to ransomware attacks in the first quarter of 2016. In February, the Hollywood Presbyterian Medical Center in California paid a US$17,000 ransom to unlock files following a ransomware infection[v]. In Australia, the Royal Melbourne Hospital reverted to manual processes after its systems in its pathology department was infected with the QBot virus. In almost all reported cases, the malware was delivered via phishing attacks and infected back-office administration systems, but clinical systems were nonetheless impacted – some relied on data stored on administrative systems or suffered performance degradation as a result of being on the same network, others had to be deliberately disabled by administrators to quarantine them from infection.

CHECKLIST

- Offer your staff security awareness training to reduce the risk of malware infection. Commonwealth Bank has made available a set of online learning modules that our valued customers can use to educate their staff. Talk to your relationship manager if you would like to trial these modules.
- Schedule routine security audits of both clinical and administrative systems.
- Run hourly or daily snapshots (backups) of data to ensure a rapid rollback to a pre-infection state. Develop a practice of testing your recovery capability to account for changes in the IT environment.
- Consider isolating critical systems from the remainder of the network (network segmentation).

By the Numbers

Over **13,700 students**[xi] have signed up for the first online cyber security course sponsored by Commonwealth Bank and UNSW.

Over **39,000 Australians**[xiv] reported a cybercrime incident to **ACORN** in 2015.

Over **225,000 Ukranians** lost power during a December 2015 cyber-attack on three utilities

Cyber Security:
Trends and Observations

Major cyber-crime actors arrested

The actors behind several of the world's most lucrative malware campaigns have been arrested in a swathe of law enforcement operations spanning the globe during 2015 and early 2016. Individuals accused of operating or distributing the Dyre, Dridex, Citadel and Gozi malware campaigns were arrested in Russia, Cyprus, Norway and Latvia respectively. The United States has sought the extradition of all of these actors to face US courts. Authorities also managed to 'sinkhole' (effectively dismantle) the botnets used in the Ramnit and Bugat (Dridex) campaigns. Disappointingly, security analysts are tracking new malware campaigns that use some of the same code and/or the same delivery mechanism (botnets) in the months since these takedowns took effect.

CHECKLIST

- Offer your staff security awareness training to reduce the risk of malware infection. Commonwealth Bank has made available a set of online learning modules for our valued customers to educate their users. Talk to your relationship manager if you would like to trial these assets.

Tax returns growing as fraud vector

A spate of data breaches over 2014 and 2015 has made it increasingly difficult for tax offices to verify the identities of taxpayers lodging tax returns. In February 2016, the US Internal Revenue Service (IRS) reported a 400 percent increase in fraudulent claims[viii], much of which was a consequence of tax documents being stolen from companies through the use of social engineering and/or malware. The stolen records helped attackers cheat a poorly-conceived knowledge-based authentication system (use of secret questions) the IRS uses to identify customers on its transactional web site[ix]. Using this technique, hackers have gained unauthorised access to the tax records of over 700,000 US taxpayers and theft of many tens of millions of dollars using fraudulent tax returns. Media reports in Australia suggest that as many as 500 tax file numbers of Australians are stolen each day using data harvested from prior data breaches for use in tax return fraud.[x]

CHECKLIST

- Review use of 'secret questions' for recovery of credentials or access to customer data - consider objective-based testing (red teaming) exercises to determine whether this method of authentication can be gamed using other publicly-available data
- Educate your administration staff to be extremely wary of emails or calls requesting access to bulk payroll data.

CEOs in the firing line

The FBI reports[vii] that fraudsters have stolen up to US$2 billion from global businesses between October 2013 and February 2016 using a combination of compromised email accounts and social engineering. A 'Business Email Compromise' scam, otherwise known as a 'CEO email scam', occurs when a fraudster sends an employee with purchasing authority an email that appears to be from the CEO requesting that a payment be made to a third party – typically to the attacker's account. Several firms have reported attackers using the same technique to convince staff members to email them tax documents and other confidential information.

CHECKLIST

- Evaluate processes to ensure large or unexpected payments cannot be made without additional verification steps (such as a phone call to the CEO/business leader that has requested the payment or some other form of two-step authentication).
- Ensure that business leaders and staff with authority to make large transactions on behalf of the company have completed security awareness training.

> "Ensure large or **unexpected payments cannot be made** without additional verification"

By the Numbers

CEO Email Fraud Scam

In what is otherwise known as "business email compromise", fraudsters impersonate the CEO or other high-ranking executives of an organisation and email the accounts department ordering that a sum of money be paid to an external party (associated with the attacker).

Over

US$2 billion[xii]

has been stolen October 2013 and February 2016

(Source: FBI)

Impacting

12,000+

victims

With an average loss of

US$120,000

per victim

Deep Dive:

Facing a more determined DDoS adversary

Lessons from 2015

Ricardo Goncalves
Threat Manager

Australia's financial services sector defended their systems against a substantially larger volume of DDoS (Distributed Denial of Service) attacks in 2015.

Our analysis – sourced from observations of activity across Australia's financial sector – paints a portrait of a more determined and adaptive DDoS attacker that has access to low-cost online resources to stage an attack.

A DDoS attack prevents legitimate users from accessing an online service by exhausting its resources.

Historically, attacks have been waged in one of three modes – **volume-based attacks**, which aim to overwhelm a target's bandwidth; **protocol abuse attacks**, which abuse weaknesses in standard connection protocols; and **application layer attacks** which aim to take advantage of a particular design weakness in a web-facing application.

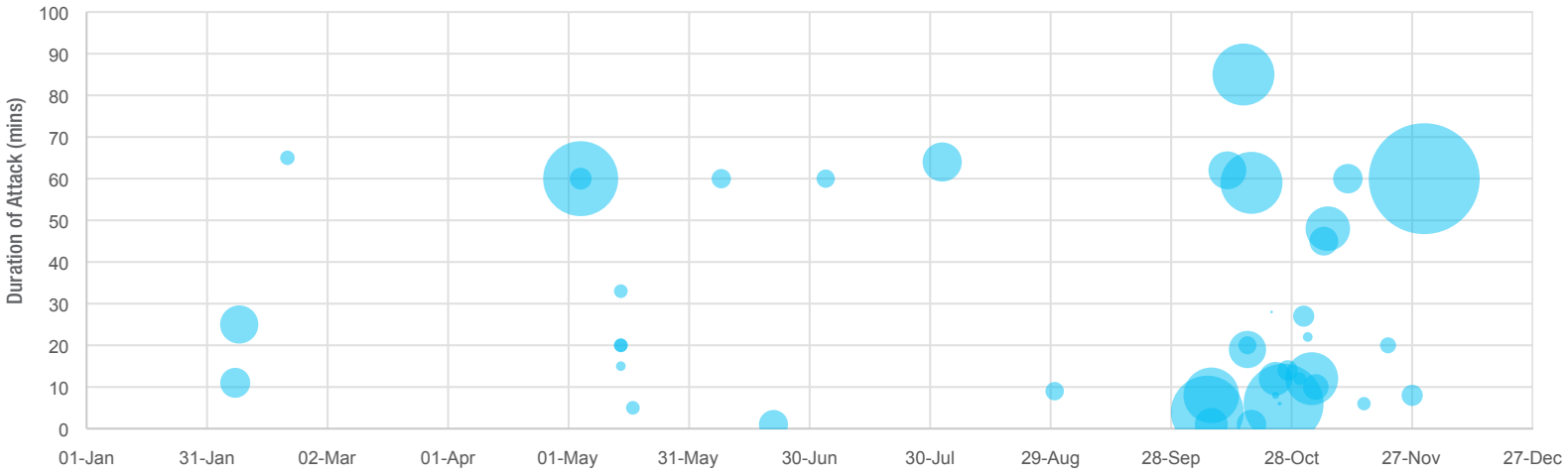
In a greater number of attacks reported over 2015, adversaries exhibited an ability to switch dynamically between these modes while an attack was underway. A disruption might first be noticed as a volumetric attack, for example, compelling defenders to apply controls that reduce the impact of this specific mode of attack. But within minutes, attackers might shift to an application-layer attack against the same target to continue to cause disruption. We call these '**multi-vector**' attacks.

There are also indications that **attackers have devoted far more time and energy to reconnaissance on attack targets and into studying the controls applied by defenders**. At times, attackers aim their fire at multiple online services offered by the same organisation. Attacks might also target one component within the victim's infrastructure and shift to another as soon as defenders adjust controls to the first.

Attackers that use DDoS range from cybercriminal gangs motivated by financial gain to loosely-connected hacktivist groups or even thrill-seeking nihilists. While **attribution for any given attack is problematic**, these patterns of behaviour support recent observations about threat actors made in the threat intelligence community. A 'professional class' of attacker has evolved that is well-financed, well-practiced, and has more time to dedicate to the incremental advancing of tools and techniques. Actors within this community have lowered the barrier to entry for new threat actors by renting their tools (botnets, user interfaces etc.) on an 'as-a-service' basis.

By consequence, there is a category of unsophisticated attacker that can disrupt services by logging into an automated service that attacks a target for as little as US$7 an hour – a stark reminder of the **massive**

Duration & Peak Traffic



Deep Dive:

Facing a more determined DDoS adversary

> “Adversaries exhibited an ability to **switch dynamically** between [attack] modes while a DDoS attack was underway.”

asymmetry between the resources required to attack versus the cost and resources required to successfully defend.

Broadly, our analysis suggests that:

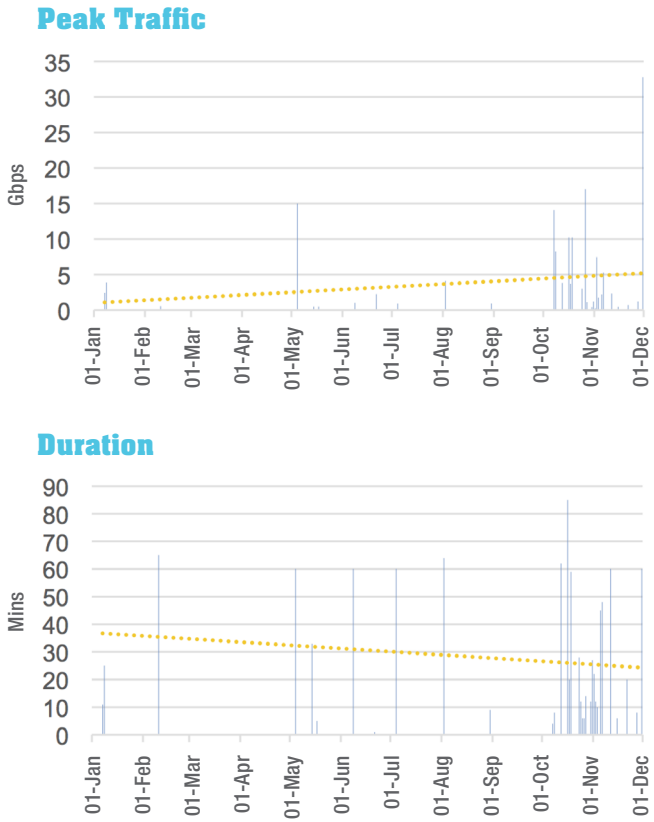
a. Attacks are becoming shorter - the average length of an attack trended down over 2015 from 40 minutes to around 25 minutes. The longest recorded attack was around 80 minutes.

b. While attacks are shorter, a threat actor is more likely to engage in subsequent waves of attacks that are timed specifically to make an impact before new mitigations can be applied;

c. Attacks are larger in volume (the average used to attack Australian financial services organisations was around 4 Gbps and the peak at 32 Gbps). It’s worth noting, however, that these are substantially lower volumes than attacks waged elsewhere in the world, which are now peaking at around 300-400 Gbps.

d. As discussed, attackers are switching between types of DDoS activity (attacks at the protocol layer, vs application layer etc.) mid-way through attacks to adapt quickly to the mitigations implemented by the defending enterprise. This requires defenders to have operations teams on standby or rotation with a variety of controls at their disposal.

Duration and peak traffic of attacks on Financial Services organisations in 2015



Attacks waged to date in 2016 exhibit a continuation of several of these trends.

Who is behind DDoS attacks?

- Cybercrime [financial motivation]: criminal activity intended to steal, or otherwise illegitimately profit from, victims’ money, goods, or services;
- Nation States [military and political motivation]: malicious activity that targets corporate and government entities to collect information for the purpose of strategic advantage;
- Hacktivists [ideological motivation]: threats arising from malicious, ideologically motivated activists.

How do cybercriminals profit from DDoS?

- DDoS extortion: these attacks target the availability of an organisation’s web facing services, often seeking to cause both reputational and financial damage for a period, followed by a demand asking for payment to stop further attacks. These type of attacks were commonplace during 2015.
- Advertising of DDoS-as-a-Service: many attacks are a threat actor’s personal test of skill or a show of force. These attacks are often opportunistic, and credit for the success of the attack is more likely to be claimed on social media or on forums with the objective to gain notoriety for their skills and services.

Regulatory & Legal

New laws and legal precedents relevant to security strategy

Industry welcomed to US, Australia cyber dialogue

In January 2016, Prime Minister Malcolm Turnbull announced a new initiative to strengthen the cyber security partnership between the US and Australia. The annual Australia-US Cyber Security Dialogue will be convened by the Australian Strategic Policy Institute (ASPI) and the US Center for International and Strategic Studies and invites industry to participate in discussions about shared approaches to incident response, sharing of cyber threat information and other initiatives that aim to "ensure the internet remains open, free and secure by promoting peacetime 'norms' for cyberspace."

CHECKLIST

- Commonwealth Bank is a major sponsor of ASPI's International Cyber Policy Centre. Please contact your relationship manager if you feel your executives would like to be included in this dialogue.

Law enforcement and tech industry clash over security mechanisms

Governments and technology companies continue to clash in several jurisdictions over the extent or means by which providers of digital services allow access to customer data for law enforcement purposes. In February, the FBI has asked a US court to compel Apple to deliver a software update to a locked iPhone that would allow law enforcement to bypass security mechanisms that protect the device from unauthorised access. Apple refused to comply[xix], arguing it will set a worrying precedent for future violations of user privacy. The FBI has since dropped the case and claims to have gained access via other means. In Brazil, a Facebook executive has been detained[ii] over law enforcement requests to access data stored in 'Whatsapp', a Facebook-owned messaging service that offers end-to-end encryption.

CHECKLIST

- Continue to protect your data with the strongest available security mechanisms. Assume that law enforcement has alternative means to access data in extreme circumstances.

US regulators sue over lack of product security

Taiwanese company ASUSTek will be subject to 20 years of annual security audits to settle a dispute with the US Federal Trade Commission over the security shortcomings of the routers and data storage accessories it markets to consumers. The FTC found that ASUSTek misrepresented the security of its products and services and didn't take 'reasonable steps' to secure the software in the routers it shipped. Among other complaints[xxii], users were not notified to change the default credentials ('admin' and 'admin') on the router during installation, while an associated cloud service offered by the company also did not encrypt files in transit. Further, FTC argued that ASUSTek failed to notify consumers or provide a timely security update after hackers gained unauthorised access to 12,900 ASUSTek devices in early 2014. The regulator recently took action over Oracle's[xxiii] failure to provide uninstall tools for older, less secure versions of Java and against Wyndham Hotels over data breaches it suffered in 2008 and 2009.

Rejected cyber insurance claims head to court

The nascent cyber insurance market is experiencing growing pains as insurers and policy holders come to terms with a rapidly evolving threat landscape. A spate of data breaches in 2014 and 2015 sent premiums skyrocketing, while several policy holders that have experienced cyber-attacks have turned to the courts to test whether they received adequate payouts. Two recent claims in the US (Ameriforge Group vs Federal Insurance[xxiv] and Bitpay vs MBIC[xxv]) were rejected on the basis that Business Email Compromise (BEC) [See Trends and Observations – Page 3] was not considered a forgery of a financial instrument and therefore not covered in the policy. In an earlier dispute, a claim by a US healthcare supplier was rejected due to the insurer's view that its policy holder failed to follow minimum security standards (Cottage Health vs CNA[xxvi]).

CHECKLIST

- Carefully consider the full range of scenarios that could result from a cyber incident prior to considering insuring against these risks. Be mindful that cyber security is a rapidly evolving space for which future risks can be difficult to predict.
- Most policies cover the costs of recovery – including forensics, legal costs and remedy for affected customers – but will not cover a range of other reputational or remediation costs.
- Be mindful that your insurer will assess your level of security capability before agreeing to fund a claim. It is prudent to align your security practices to an established and respected standard (such as the Australian Signal Directorate's **Information Security Manual**[xxvii] **or 'Top 4 Strategies to mitigate cyber intrusions**[xxviii]' or the NIST Cybersecurity Framework) to support any future claim.
- Ultimately, strong awareness programs and the security practices encouraged by the aforementioned standards are the best form of insurance (or assurance) money can buy.

Better Practice

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

A checklist for Australian business

The Australian Securities and Investment Commission – in assessing the security posture of the ASX and Chi-X securities exchanges in March – has incidentally **documented (see Section C)** what it asserts are 11 examples of information 'good practice' that would apply to all Australian businesses. These are based loosely on the **NIST Cybersecurity Framework**.

Secure your email services

The US National Institute of Standards and Technology has released a **draft guide**[xxix] for IT administrators to secure configuration of email systems and the setting of user policies to protect against threats delivered via email.

A checklist for critical infrastructure owners

The US ICS-CERT **advisory**[xxx] into the attack on the Ukraine power grid makes several key recommendations on securing industrial control systems against similar attacks.

One simple way to defend against Android malware

Tech news site ZDNet has published a devastatingly simple **column** that nominates a single setting every Android user needs to switch on as a first line of defence against malicious software.

Know your enemy: the exploit kit

CERT UK have released an **educational paper on understanding Exploit Kits**[xxxi], with some handy tips for administrators to defend against them.

This report contains general advice for educational purposes only. Please consult your cyber security team and legal counsel for advice specific to your organisation.

Horizon Scan

Upcoming events of interest

2016 Apr 12-14

Canberra

Australian Cyber Security Centre annual conference

The Australian Government's annual information security event.

2016 May 5

Canberra

CommBank Cyber Alliance session: Cyber Security and national prosperity

Anticipating the Australian Government's Cyber Security Review. Contact your relationship manager if you would like to attend this closed-door session.

2016 May 23-27

Gold Coast

AusCERT2016 Conference

Australia's largest and oldest information security conference.

Parenting in the Digital Age

Many of your most prized employees are likely to be parents who face the difficult challenge of encouraging their children to use digital technologies in a safe and secure way.

Commonwealth Bank is a proud sponsor of the ThinkUKnow program - a partnership between CBA, the Australian Federal Police (AFP), Microsoft Australia and Datacom, which aims to provide awareness training to parents, carers and teachers to help them fine-tune cyber safety messages for young people. These training sessions are typically delivered to parents at high schools.

As part of our commitment to cyber safety, trained CBA volunteers are now available to run the same informative presentation at your workplace to help your employees navigate this challenge. Presentations last for an hour and are delivered in collaboration with a local police officer.

For more information, or to enquire about booking a presentation, please contact **thinkuknow@cba.com.au**.

Footnotes

i: https://ics.sans.org/blog/2016/01/09/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-grid

ii: https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01

iii: https://ics-cert.us-cert.gov/monitors

iv: http://thehill.com/policy/cybersecurity/266081-dhs-critical-manufacturing-cyberattacks-have-nearly-doubled

v: http://arstechnica.com/security/2016/02/hospital-pays-17k-for-ransomware-crypto-key/

vi: http://www.networkworld.com/article/3047180/security/three-more-hospitals-hit-with-ransomware-attacks.html#tk.rss_all

vii: https://www.fbi.gov/news/stories/2015/august/business-e-mail-compromise/business-e-mail-compromise

viii: https://www.irs.gov/uac/Newsroom/Consumers-Warned-of-New-Surge-in-IRS-Email-Schemes-during-2016-Tax-Season-Tax-Industry-Also-Targeted

ix: https://www.irs.gov/uac/Newsroom/IRS-Statement-On-Get-Transcript

x: http://www.smh.com.au/it-pro/security-it/five-hundred-tax-file-numbers-hacked-every-day-20151028-gklcx7.html

xi: http://www.openlearning.com/SECEDU

xiv: https://www.ministerjustice.gov.au/Mediareleases/Pages/2016/FirstQuarter/18-January-2016-Australian-Cybercrime-Online-Reporting-Network-receives-more-than-39000-reports.aspx

xix: http://www.apple.com/customer-letter/

xx: http://money.cnn.com/2016/03/01/technology/facebook-brazil/index.html

xxi: https://www.ftc.gov/news-events/press-releases/2016/02/asus-settles-ftc-charges-insecure-home-routers-cloud-services-put

xxii: https://www.ftc.gov/system/files/documents/cases/160222asuscmpt.pdf

xxiii: https://www.ftc.gov/news-events/press-releases/2015/12/oracle-agrees-settle-ftc-charges-it-deceived-consumers-about-java

xxiv: http://krebsonsecurity.com/2016/01/firm-sues-cyber-insurer-over-480k-loss/

xxv: http://www.bizjournals.com/atlanta/blog/atlantech/2015/09/atlantas-bitpay-got-hacked-for-1-8-million-in.html

xxvi: https://www.privacyandsecuritymatters.com/2015/05/cna-denies-cyber-insurance-claim/

xxvii: http://www.asd.gov.au/infosec/ism/index.htm

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

xxix: http://csrc.nist.gov/publications/drafts/800-177/sp800-177_draft.pdf

xxx: https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01

xxxi: https://www.cert.gov.uk/resources/best-practices/demystifying-the-exploit-kit/