Signals

Quarterly security assessment

Q3 2015

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.

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.

CommonwealthBank

Cyber Security:

Trends and Observations

Key trends observed during the quarter

> If attacked or threatened, **do not engage with any extortion actor** and immediately refer the matter to State law enforcement

Malvertising threat:

Third party ad networks delivering malware

Malware monitoring services have noted an increase in use of malvertising in recent months to infect casual browsers of popular web sites. Telstra[i], Yahoo[ii], The Huffington Post[iii] and Microsoft's MSN web portal[iv] have each inadvertently posted advertisements that delivered malware to users of these sites. These 'malvertising' incidents usually result from the compromise of a third party advertising network upstream from the media site.

CHECKLIST

- Empower your security team to establish a program of third party supplier governance for services delivering content to web pages published by your organisation.
- Consider use of a web proxy to block third party advertisements on the company network to protect your staff from infection.

Australian organisations targeted by DDoS extortion

The online channels of several Australian banks are amongst a large number globally subject to volumetric Distributed Denial-of-Service (DDoS) attacks in 2015, several of which were accompanied by efforts to extort payments (in the form of Bitcoin) for the attacks to cease[v]. The threat actors behind these extortion attempts have been observed attacking financial service providers in Asia and Europe, and more recently smaller organisations in other industries with less sophisticated defences.

CHECKLIST

- Ensure DDoS extortion campaigns are considered in your organisation's crisis response framework.
- If attacked or threatened, do not engage with any extortion actor and immediately refer the matter to State law enforcement.
- Assess the impact of a temporary outage in online services on your business, weighed against the cost of DDoS remediation services available from ISPs and specialist providers of DDoS mitigation services on a subscription or pay-per-use basis.

State-sponsored attacks on the rise

There has been an increase in the scope and efficacy of state-sponsored and 'hacktivist' attacks against large organisations in the United States, Asia and domestically. Intrusions at the Office of Personnel Management – the US government agency in charge of maintaining personnel records for millions of cleared government employees – and Japan's universal pension fund were attributed to state-sponsored actors linked to the Chinese government.

CHECKLIST

- Adjust risk calculations to account for heightened nation-state activity.
- Consider whether your organisation holds any data on employees of government agencies, military contractors, technology companies or other industries of interest to nation-state aligned actors.

By the Numbers

Australians are **75%** more likely to shop online **(vs 56%)** and **85%** more likely to bank online **(vs 61%)** than in any other OECD country.

The Australian Cyber Security Centre responded to **1131** incidents in 2014, **(up 20%)**.

Cyber Security:
Trends and Observations

Phishing remains primary means of gaining unauthorised access

Targeted phishing (sometimes referred to as 'spear phishing') was the primary means by which threat actors gained access to the networks of OPM and Japan Pension Fund. A lack of network isolation, security monitoring and governance of third party suppliers were contributing factors to the success of the attacks against OPM.

CHECKLIST

- Consider a rolling program of phishing simulation to test the susceptibility and raise awareness of staff to spear phishing attacks
- Consider network segmentation as specified by the NIST Cyber Security framework.

Data breaches impact major brands

David Jones [vi] and Kmart [vii] separately suffered data breaches within weeks of each other, most likely attributed to the same threat actor. The online properties of both retailers were found to be vulnerable to the same unaddressed flaw in a popular web server system which should have been patched many months earlier. In August, the user database of extra-marital affair website Ashley Madison was published online. Large-scale breaches of this variety can have serious implications for staff and brand reputation of unrelated entities. The public exposure of staff corporate cards or company email addresses via such a data breach will often result in fraud or blackmail attempts against staff. As was the case with Target in 2013, the severity of the data breach resulted in the resignation of Ashley Madison's chief executive officer.

CHECKLIST

- It is critical for business leaders to invest in people and process to ensure the timely patching of vulnerabilities found in the systems your organisation relies on.
- Consider developing an internal threat intelligence function to assess your organisation's exposure following data breaches at large-scale online service providers. Subscribe to threat intelligence sharing networks.
- Any analysis of a breached data set needs to be treated with sensitivity and in the context of protecting your staff from fraud and blackmail. Be mindful that the presence of an email address or corporate card alone does not necessarily indicate a staff member used a given service, as many services do not verify accounts on sign-up.

> "Large-scale breaches of this variety can have **serious implications for staff and brand** reputation"

By the Numbers

The Australian Competition and Consumer Commission calculates Australians have lost

$45 million

to scams over the last 12 months.

Akamai recorded a

132%

increase in DDoS attacks in 2015

There were over

32 million

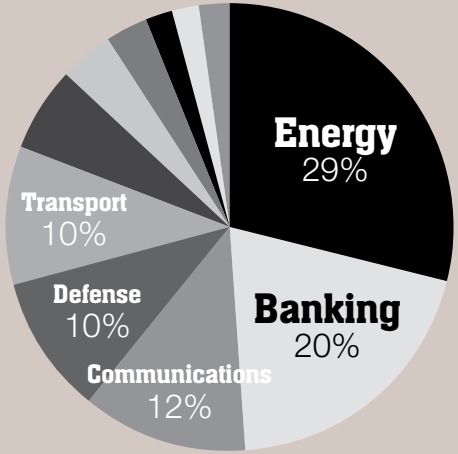
US government employees whose records were breached in the OPM hack.

The FBI has recorded

US$100 million

in securities fraud over five years via attacks on distributors of press releases.

Incidents responded to by CERT Australia affecting systems of national interest and critical infrastructure (2014)



Energy	29%	Information Technology	4%
Banking and financial services	20%	Education and Research	3%
Communications	12%	Health	2%
Defense Industry	10%	Mining and Resources	2%
Transport	10%	Food and Agriculture	2%
Water	6%		

Source: Australian Centre for Cyber Security

Target paid

US$67 million

to Visa in August to cover the cost of reissuing credit cards in response to a breach of 40 million customer details in 2013.

Deep Dive:

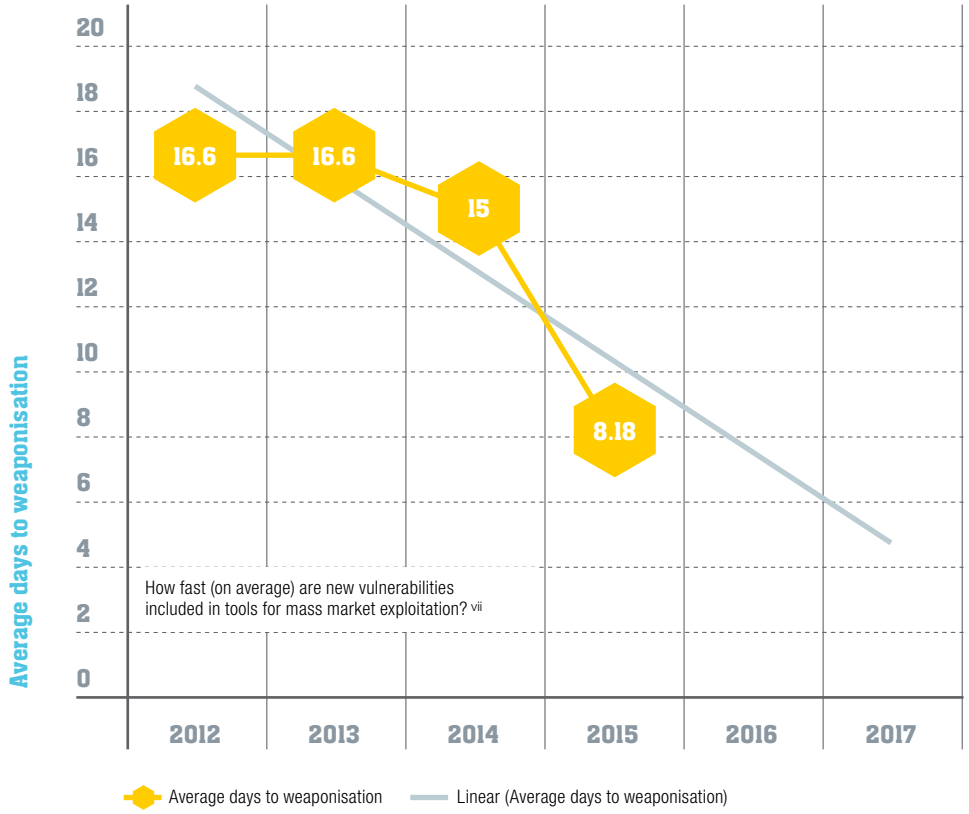
The Case for Priority Patching

Zero-day exploits weaponised at pace

Brett Winterford
Information Security Analyst

Average days to weaponisation

Total days from public disclosure to integration into first exploit kit



Criminals are making use of newly disclosed vulnerabilities in malware 'exploit kits' far faster than the typical window for defenders to patch affected systems.

Every day, technology companies and white hat 'ethical' hackers alert system administrators to new security vulnerabilities found in popular software such as operating systems, browsers and multimedia players.

Patching (fixing) systems against each newly announced vulnerability is a daunting, relentless task for system admins, but the pace and scale at which criminals now distribute attacks that make use of newly-disclosed vulnerabilities has made it a critical process for large organisations to execute in a timely way.

Security analysts have anecdotally warned that they have fewer hours with which to apply a patch before a new vulnerability is adopted for use as an 'exploit' by attackers. The 'window of vulnerability', in military parlance, is fast closing. Organised cyber-criminal groups have engaged in specialisation of task - forming an efficient marketplace of malware writers, integrators of exploits, distributors, attackers and swindlers.

Among the tools available on this black market are 'exploit kits' used by malicious hackers to compromise systems. Exploit kits bundle together multiple exploits (uses of vulnerabilities to gain unauthorised access to a system) in order to maximise the chance of infecting any given host it attacks. This in turn maximises an attacker's investment in the delivery mechanism (such as a phishing spam campaign or infected websites used for 'watering hole' attacks).

In the chart (left), the most critical vulnerabilities in popular web software exposed to the public over the last four years were shortlisted according to those for which security researchers have definitively tracked the date they were first integrated into exploit kits.

The data suggests that the start of 2015 marked a turning point for how quickly

Deep Dive:
The Case for Priority Patching

> “Today **a newly-disclosed vulnerability** is likely to take little over a week to find its way into exploit kits”

new exploits are integrated into kits for mass distribution.

From 2012-2014, the average time it took for a new vulnerability to first appear in an exploit kit (days to weaponisation) was steady at about 15-17 days. That provided an average window of two weeks for software vendors to release a patch and for IT teams to apply them. It was tight, but manageable.

Today a newly-disclosed vulnerability is likely to take little over a week to find its way into exploit kits. Several serious vulnerabilities were bundled into kits for distribution on the black market within a single day of being announced to the public. On rare occasions, the vulnerability was advertised in exploit kits before the security community knew of its existence.

Additional analysis reveals that once the first exploit kit bundles a new vulnerability into its wares, others tend to follow at greater pace. It takes an average of 7.5 days for a vulnerability to be integrated into a second exploit kit after the first, and less time again (an average of 6.49 days) to be integrated into a third, fourth or fifth variety of exploit kit.

The speed at which vulnerabilities proliferate through multiple exploit kits faster than they are bundled into the first suggests that either:

- Writers of exploits sell their wares on a non-exclusive basis to a number of buyers; or
- The work of integrating a new vulnerability into an exploit kit is resold to or copied by other producers of exploit kits.

An adequate defence in this environment requires a security team to learn of new vulnerabilities in systems they use as early as possible, and an expedient process to patch (or implement a form of control) any such flaw before it is bundled into an exploit kit for broad dissemination.

CHECKLIST

- Employ skilled professionals to keep track of vulnerabilities in the technologies your organisation has deployed and empower them to expedite patching when deemed necessary.
- Consider the maturity of the patching/remediation strategy of technology vendors during RFP.

The tipping point

Average days before a newly public vulnerability is integrated into first, second and subsequent exploit kits (2012-2015)

Regulatory & Legal

New laws and legal precedents relevant to security strategy

> “The US **threatened to use economic sanctions** as a disincentive to foreign governments **[that sponsor intrusions against private companies]**”

US regulators can now sue companies over negligent cyber security practices

The US Federal Trade Commission has won a case that sets a concerning trend for organisations with lax investment in cyber security. In August, the US Court of Appeal created a legal precedent by ruling the Federal Trade Commission (FTC) can begin legal proceedings against hotel conglomerate Wyndham Worldwide for a sustained failure to protect customer personal data from 2008 to 2010.

CHECKLIST

- Commonwealth Bank is working with the Australian Government on strategies to lift industry-wide cyber standards in ways that do not impose an additional regulatory burden on Australian business. Contact you relationship manager if you would like an update/ analysis on the Australian Government’s Cyber Security Review.

Cyber Information Sharing Act destined to be signed into law

The US Senate has passed the Cybersecurity Information Sharing Act of 2015. The bill provides a legislative basis for the sharing of information about cybersecurity threats between the US government and private sector. Following review by the US House of Representatives, President Obama is expected to sign the bill into law.

CHECKLIST

- The Australian Government’s Cyber Security Review is expected to address the issue of information sharing, including whether it requires legislative change. Our team will provide a further update/analysis in our next update.

Bilateral agreements, economic sanctions framed as response to cyber-attacks

In late September, the US and China agreed to mutual assistance on cybercrime investigations and not to conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information. The US previously threatened to use economic sanctions as a disincentive to foreign governments that might otherwise sponsor or tolerate cyber intrusions against private companies. The economic sanctions would likely freeze assets of, and bar commercial transactions with, any individuals and entities that engaged in destructive cyber-attacks or commercial espionage.

CHECKLIST

- Assume your IP and information assets are a target for theft by nation-state aligned actors.
- Monitor which individuals and organisations are named in any sanctions for potential business exposure.

Australian Government imposes security supplier governance on private industry

The Australian Government has proposed laws that would provide it the authority to ban use of a given telecommunications service provider’s equipment on cyber security grounds. The provisions in the proposed *Telecommunications and Other Legislation* bill met strong opposition from the nation’s telecommunications providers. In some overseas jurisdictions, such as China, these regulations have been extended to include other industries such as financial services.

CHECKLIST

- Consult your relevant industry association to assess the potential impacts of proposed legislation in Australia.
- Seek advice on the legal requirements of any country with respect to use of or access to systems prior to expansion into a new territory.

Better Practice

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

Prioritise your controls against common attack patterns

The Australian Cyber Security Centre has released its first unclassified **threat report**, which features general advice on the techniques used by threat actors.

Secure your Linux environments

The Linux Foundation has released its latest **guide to securing Linux systems**, in the form of a hardening guide for system administrators.

Secure your multi-tenant cloud environments

The Australian Signals Directorate has released its latest **guide to securing systems hosted on multitenant cloud platforms**.

Passwords guidance for System Administrators

The UK GCHQ (intelligence agency) has released a **guide for system administrators** that set password authentication policies.

Horizon Scan

Upcoming events of interest

2016 Feb 03

Sydney

CommBank Cyber Alliance session, Executive Reporting and Dashboards

CommBank is sharing with peers and key customers a view of how to best communicate cyber security issues to the board. Contact your relationship manager if you would like to access this material.

2016 Apr 12-14

Canberra

Australian Cyber Security Centre annual conference

The Australian Government's annual information security event.

Footnotes

i: https://blog.malwarebytes.org/news/2015/08/telstra-medias-homepage-pushes-malvertising/

ii: http://www.theguardian.com/technology/2015/aug/05/yahoo-users-malvertising-campaign-malware

iii: https://blog.malwarebytes.org/malvertising-2/2015/04/flash-ek-strikes-again-via-googles-doubleclick/

iv: https://blog.malwarebytes.org/malvertising-2/2015/08/angler-exploit-kit-strikes-on-msn-com-via-malvertising-campaign/

v: http://www.afr.com/technology/bitcoin-criminals-dd4bc-target-financial-markets-as-attacks-rise-20150924-gjucv8

vi: http://www.abc.net.au/news/2015-10-02/david-jones-computer-system-hacked-customer-details-stolen/6824170

vii: http://www.smh.com.au/business/retail/kmart-online-customers-information-hacked-in-security-breach-20150930-gjyoxe.html

viii: CommBank analysis of public data made available by F-Secure, FireEye, Kaffeine (security researcher) and Trend Micro as well as news reports.