ASB

Signals

Quarterly security assessment

› Q3 2018

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.

We hope and anticipate our analysis will provide context and confidence for your security strategy.

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

Contents

Trends & Observations

Key trends observed during the quarter

Heightened awareness and new regulations drive breach reports and complaints

This quarter has seen a noticeable uptick in reporting of privacy and data protection issues, both domestically and across the globe. In July, the Office of the Australian Information Commissioner (OAIC) reported an increase in data breach notifications by Australian organisations under the Notifiable Data Breach scheme. It received 242 notifications between April and June[9], which Information Commissioner Angelene Falk said reflected growing awareness by organisations of their obligations under the scheme, which took effect in February 2018. A similar impact has been felt in Europe, where the General Data Protection Regulation (GDPR) took effect in May. Data protection complaints to the UK's Information Commissioner's Office (ICO) in the first 5 weeks of the GDPR regime were more than double the number of complaints from the same period the previous year.[10]

CHECKLIST

- Make your board and senior executives aware of the growing regulatory and public focus on data protection, and the potential implications for your business of a breach.
- Consult the New Zealand Privacy Commissioner web-site[85] for guidance for resources on the new requirements in the EU's General Data Protection Regulation and how business can comply with the EU privacy laws.
- Ensure your organisation is prepared to respond well to a possible data breach and meets its legal obligations by creating a thorough data breach response plan. Read our Deep Dive "Into the Breach" in the last edition of Signals[12] for our insights on implementing such a plan.

Social media giants intensify fight against platform abuse

Social media networks are intensifying efforts to prevent abuse of their platforms by malicious actors.

Following reports of Russian influence campaigns soon after the 2016 US presidential election, some platforms initially understated the potential impact of such abuse[26]. A more proactive approach to moderation has been adopted in recent months, likely reflecting the seriousness and continued persistence by malicious actors to misuse these platforms. In August Google, Facebook and Twitter all announced the removal of "inauthentic" content relating to "influence campaigns" believed to originate in Iran.[27] Facebook also uncovered a campaign linked to Russia.

In Australia, Facebook has said it is working with authorities to prevent misuse of its platform ahead of the 2019 Australian federal election[28]. Facebook is also piloting expanded security tools for election campaigns.[29]

CHECKLIST

- The actors conducting these influence operations via social media do so primarily in order to shape political discourse to achieve political outcomes. This could extend to the targeting of individuals or topics of public discussion that have relevance to your business.
- Given the growing reliance on social networks for marketing purposes, it's important for organisations to continue to monitor and be aware of the reported misuse and abuse of these platforms.

Security of healthcare data under scrutiny

The journey towards digital health continues to be afflicted by security and privacy concerns. In July, the Australian Government's My Health Record (MHR) program attracted criticism[20], particularly in relation to the system's controls over users' access to records and overly broad provisions in the legislation for third-party access in addition to a more general perceived lack of confidence in the system's security.

The MHR debate coincided with a breach of health records of 1.5 million patients in Singapore, resulting from an attack that the Singaporean government described as "deliberate, targeted, [and] well-planned," including repeated attempts to access the personal information of Prime Minister Lee Hsien Loong[21].

The value of medical records on the black market - in some cases valued higher than credit card information - means cybercriminal activity will continue to drive health breaches. The health sector was also the top sector for reporting data breaches in the OAIC's most recent data breaches report[22].

CHECKLIST

- What was experienced in Australia is a good reminder of the importance of a proactive approach to assuring stakeholders - including end users and data subjects - about the privacy and security controls of new systems.
- Continued targeting of health data emphasises the importance of user awareness training in the health sector.

By the Numbers

12

Russian intelligence officers indicted for hacking the 2016 US election[1]

8000

remote access scams against Australian businesses this year[2]

$476 million

in online (card not present) payment fraud in Australia in 2017[3]

340 million

records containing personal information exposed to public by marketing firm Exactis[4]

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

Trends & Observations

Attackers directly targeting online reputation

Cyber-attacks often result in reputational damage for targeted organisations, though this is more commonly a secondary impact from a public breach of sensitive data or disruption to online systems. Attackers now appear to be pursuing a more direct route to exploiting organisations' sensitivity to brand damage.

In August, attackers extorted private companies by threatening to flood online review sites and search engine results with negative reviews (most likely by using bots).[23] In a more personally targeted campaign, cybercriminals also netted USD $500,000 from a "sextortion" scheme in which victims received an extortion email claiming their webcam had been hacked to film them while watching pornography[24]. To convince the victim of the veracity of this claim, the email included one of the victim's previous passwords, likely sourced from a previous data breach.

Extortion is a key tool for cyber criminals, as evidenced by schemes like these and the prevalence of ransomware campaigns. The FBI's Internet Crime Complaint Center received about 15,000 extortion-related complaints last year alone[25].

CHECKLIST

- Regularly monitor your social media channels and public-facing sites for evidence of unusual or anomalous behaviour.
- Educate your staff about extortion attempts and, more broadly, email-based scams.
- If affected by ransomware or a similar extortion-based attack, consider seeking assistance from CERTNZ via 0800 2378 69.

Multi-factor authentication in focus

In previous editions of Signals, we have highlighted the ability of cybercriminals to compromise online accounts by obtaining login credentials through phishing or purchasing stolen credentials online.

To mitigate this risk, digital services are increasingly looking to multi-factor authentication (MFA) or two-factor authentication (2FA), which require users to provide a further "factor" of authentication in addition to their username and password (such as a unique code).

In August, following a series of account compromises, Instagram announced support for third-party multi-factor authentication apps[13]. Microsoft also mandated MFA for admin users of its Azure cloud service[14]. However, the use of SMS-based MFA (where a user receives their unique code via SMS text message) has come under scrutiny.

After a serious data breach in August despite having 2FA enabled, popular internet forum Reddit concluded that "SMS-based authentication is not nearly as secure as we would hope"[15]. Commentators increasingly observe attackers deploying "SIM swaps" and phone porting to circumvent SMS-based 2FA.[16]

CHECKLIST

- Review the CERTNZ's guide on Multi-Factor Authentication[17]. The guide describes the importance of MFA and outlines different MFA methods.
- For your most critical accounts, consider deploying hard tokens or security keys. Google reports that it has had no account compromises since requiring all its employees to use physical tokens in early 2017.[18]
- The Q1 2018 edition of Signals includes a deep dive "Proven defences for pocket change", which describes the value of password managers and MFA, and how to enable the latter for various popular online services[19].

Authorities warn IoT devices being used for malicious activity

Researchers have for some time warned of likely security risks from the growing number of internet-connected devices deployed with sub-standard security protections. Various signs indicate these risks are materialising.

Malware samples targeting Internet of Things (IoT) devices collected by Kaspersky Lab have increased three-fold in the first half as compared with the whole of 2017.[30]

The Mirai family of malware has proven most popular, and cracking Telnet passwords remains the most popular attack, Kaspersky said.

In August the FBI warned that cyber actors were "actively" searching for vulnerable Internet of Things (IoT) devices – especially in developed nations – through which they can route traffic and disguise the source of their malicious activities .

Reflecting this assessment, security researchers in September documented the rapidly growing Hakai IoT botnet - first spotted in June and which has since burgeoned through targeting vulnerabilities in well-known router brands[32]. The passing of the US' first IOT security bill in August by the California legislature[33] and recent investments[34] by ventures and start-ups in IoT security – notably by prominent Israeli firm Cellebrite[35] – are positive signs that momentum is also building in response to the IOT threat.

CHECKLIST

- Authorities recommend regularly rebooting network devices, as this can potentially disrupt any malware on the device.
- The FBI offers a range of good advice to protect IoT devices, including changing default usernames and passwords, ensuring devices are patched, and ensuring firewalls are configured to block traffic from unauthorised IP addresses.[36]

By the Numbers

US$12.5 billion
in global Business Email Compromise losses over 4.5 years[5]

242
data breach notifications in Australia between April-June 2018[6]

59%
of reportable data breaches are malicious or criminal attacks[7]

15 million
credit card numbers stolen in US alone by cybercrime group FIN7[8]

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

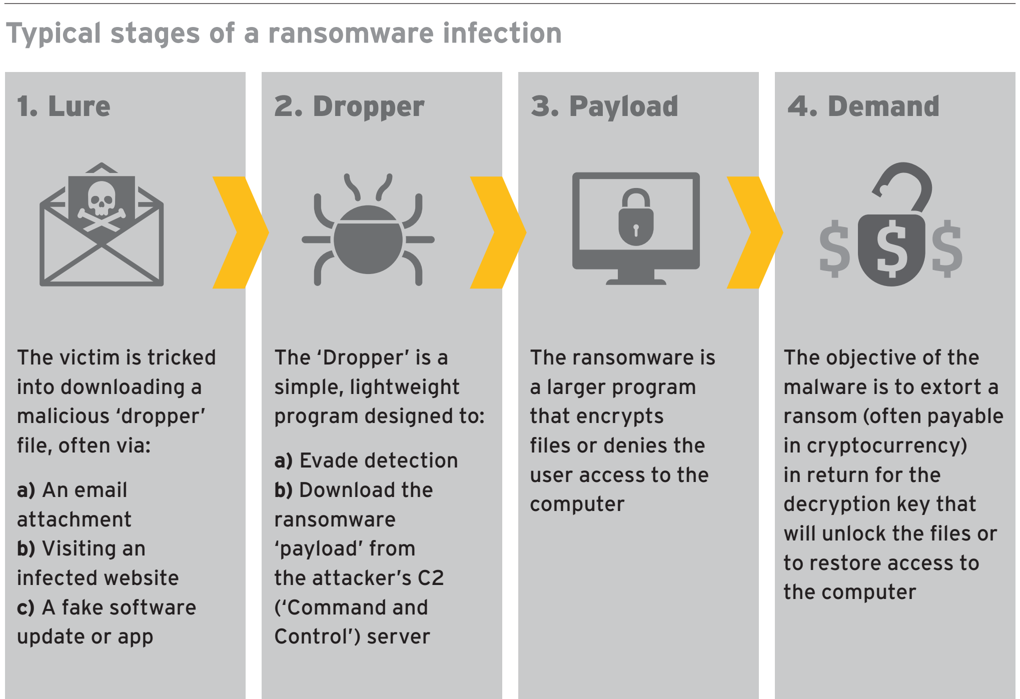
Deep Dive:

Defending your business against ransomware

John Hare
Executive Manager, Cyber Outreach
Commonwealth Bank

In a constantly evolving cyber threat landscape, ransomware remains an enduring fixture on our business customers' list of concerns. Customers are interested to know the latest advice on avoiding falling victim to a ransomware attack and how to respond and recover, should the worst happen.

This Deep Dive will investigate these issues and will also address the thorniest question of all: to pay or not to pay?



Typical stages of a ransomware infection

1. Lure

The victim is tricked into downloading a malicious 'dropper' file, often via:

a) An email attachment
b) Visiting an infected website
c) A fake software update or app

2. Dropper

The 'Dropper' is a simple, lightweight program designed to:

a) Evade detection
b) Download the ransomware 'payload' from the attacker's C2 ('Command and Control') server

3. Payload

The ransomware is a larger program that encrypts files or denies the user access to the computer

4. Demand

The objective of the malware is to extort a ransom (often payable in cryptocurrency) in return for the decryption key that will unlock the files or to restore access to the computer

Preventing ransomware attacks

The CERTNZ website[83] contains information and links to a wide range of prevention measures. No single measure will provide a silver bullet. As with many cybersecurity threats, defence-in-depth is the best strategy.

However, user awareness is particularly important, given the majority of ransom attacks rely on insecure user behaviour.

Phishing remains a key mode of ransomware (and other malware) infection, and users should be trained to avoid email 'lures'. These are emails with malicious attachments or links to malicious sites.

The recipient is enticed to open the email and execute the attachment or click the link, often through a sense of urgency engendered by the phishing email (fake bills, invoices, penalty notices).

Other key prevention methods include:

- Using and regularly updating reliable anti-virus software
- Disabling macros in Microsoft Office applications, since these may be used in malicious attachments to emails to download ransomware
- Enforcing a regular security patching policy to ensure all mobile devices, laptops and desktops are using the latest versions of their operating systems and applications
- Keeping abreast of the latest cyber threats by referring to sources such as Stay Smart Online, which can also provide alerts to new and emerging threats

What is ransomware?

Ransomware is malicious software (malware) that either:

- encrypts files; or
- blocks access to a computer or mobile device.

Ransomware demands a ransom, often to be paid in cryptocurrency, for the decryption of the files or unlocking of the device. It may be insidious, but this is malware with history: the first known attack, the so-called AIDS Trojan, took place as far back as 1989, with the malware being distributed by floppy disks the attacker claimed contained a program which analysed an individual's risk of contracting AIDS.[44]

Whilst the means of delivery may have changed over the years and the sheer scale of the problem has increased exponentially, ransomware operators still often rely on fooling users into doing the wrong thing. From a business perspective, online behaviour of staff remains the biggest vulnerability.

What to do should the worst happen

Given the prevalence of ransomware, you may wish to consider having an incident response plan that specifically contemplates this threat. Accessing back-ups will be a key part of this plan. You should identify your critical data and ensure this is backed-up off-line at a cadence that reflects how quickly your critical data

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

Deep Dive:

Defending your business against ransomware

> “Some ransomware is designed to **scare and to attract payment**, without any intention of enabling restoration of that data”

changes over time.

The cost of frequent back-ups may necessitate a difficult discussion as to how much irretrievable data loss is acceptable to your business.

Europol provides a potentially valuable service through the ‘No More Ransom’ project.[38] This website offers decryption tools for a number of ransomware strains, provided by law enforcement agencies and commercial partners.

To pay or not to pay?

But what if you don’t have back-ups and external resources can’t help in restoring your critical data?

CERTNZ is very clear in its advice: We recommend you don’t pay the ransom, as it doesn’t guarantee you’ll get your data back.

It could also put you at risk of further attacks – if an attacker sees that you’re willing to pay them, they could simply target you again. Paying ransoms supports this kind of criminal activity.

Breaking the law

It’s important to realise payment of a cyber ransom may not be legal and as such you should seek legal advice before making a decision on what to do.

According to research by Telstra...

47%

of Australian businesses that found themselves victims of ransomware paid the ransom[39] and

86%

of Australian businesses who paid a ransom were able to retrieve their data after the payment

Paying a ransom is no guarantee of getting your data back

In this respect, ransomware is increasingly resembling ‘real-world’ extortive crime and kidnap, where acceding to a ransom demand may not secure safe and timely release, and may simply lead to a further ransom demand. The attack on Kansas Heart Hospital in May 2016 is one such example. The hospital paid a ransom demand following a ransomware attack that encrypted critical patient files. However, rather than decrypting the files, the criminals demanded another ransom, which the hospital refused to pay, determining this was no longer ‘a wise manoeuvre or strategy’[40] .

Then there is the issue of the ransomware operator’s intent and competence. Some ransomware is designed to scare and to attract payment, without any intention of enabling restoration of that data, or poorly-coded ransomware may make restoration impossible. The infamous worldwide WannaCry attack of May 2017 was one such case. The ransomware demanded $300 or $600 payable in Bitcoin, but accession to this demand would not have led to the restoration of data. The malware did not assign paying victims a unique bitcoin address, so had no way of automatically verifying whether the victim had paid the ransom[41].

Vulnerability to further attacks

By paying a ransom you have identified yourself as a compliant target and may increase the prospect of being attacked once again, by the same criminals or a different group.

Securing the ecosystem

Ransomware will endure as a profitable enterprise for criminals as long as victims are willing to pay the ransoms. By paying a

When is ransomware not ransomware?

When it is data-destroying malware, masquerading as ransomware! The “Not-Petya” malware attack of June 2017 involved malware that presented as ransomware which closely matched a previous strain called Petya. However, victims quickly found that there was no facility to actually pay the ransom. Instead the malware not only locked users out of their devices, but also destroyed data and wiped memory in the process[47].

The USA, UK, Australia and Canada attributed the attack to Russia[48]. Earlier this year the White House said Not-Petya was originally designed to disrupt Ukrainian businesses and utilities.[49]

The malware was distributed via a weaponised update of tax preparation software commonly used in Ukraine. However, whether by design or neglect, the impacts were felt well beyond the Ukrainian target set, with several multinational companies becoming collateral damage. WPP[50], Merck & Co[51] and Maersk were just some of the household names to be affected. Maersk in particular reported between US$200 and US$300m in lost revenue as a direct result of the disruption caused by Not-Petya[52].

Not-Petya demonstrated the speed with which criminals or nation states exploit new intelligence. The EternalBlue exploit that facilitated the spread of Not-Petya had been publicly leaked by a hacker group named Shadow Brokers in April 2017[53]. That exploit was employed in the WannaCry malware four weeks later and again in Not-Petya the following month.

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

Deep Dive:

Defending your business against ransomware

> Crypto-jacking is the use of **malware to steal computing power**, rather than money or data, by surreptitiously mining for cryptocurrency on the victim's computer

ransom you are helping to perpetuate the problem. The Europol-sponsored initiative, 'No More Ransom' advises: "if the ransom is paid, it proves to the cybercriminals that ransomware is effective. As a result, cybercriminals will continue their activity and look for new ways to exploit systems that result in more infections and more money on their accounts".[42]

What has caused the proliferation of ransomware?

The relative ease with which cybercriminals can cheaply obtain ransomware or even Ransomware-as-a-Service (RaaS) has dramatically lowered barriers to entry. Aspiring cybercriminals with limited technical know-how can now quickly and easily purchase user-friendly malware that is provided via an internet-based vendor platform.

This malware can be customised with a specific target in mind or enhanced by spam networks. RaaS also offers enticing business models with criminals paying a single fee or having a profit share agreement with the developer. The Hostman RaaS, for example, costs affiliates $49.95 for unlimited use and has an average ransom payment of $600[45].

The Dark Web contains a number of underground marketplaces for ransomware and RaaS. In this thriving market, competition is fierce and vendors seek to differentiate themselves through unique features to evade detection or increase success, or by attractive commercial arrangements such as franchising and profit sharing.

The opportunity for criminals comes at an immense cost to its victims.

What next?

Some analysts have argued that we may have reached, or are soon to reach "peak ransomware", since many cyber criminals are turning to crypto-jacking as a profitable alternative. Crypto-jacking is the use of malware to steal computing power, rather than money or data, by surreptitiously mining for cryptocurrency on the victim's computer.

However, the fall in value of cryptocurrency may mean crypto-jacking is not as attractive as it was. It seems that ransomware will continue to be a fact of life for businesses for the foreseeable future, fuelled by the ease with which criminals can obtain the required tools and the willingness of their victims to pay up.

Meanwhile both the design of malware and the business models that support it will continue to evolve. New malware strains demonstrate ever-more advanced capabilities, including encryption algorithms some analysts believe are all but unbreakable.[43]

Against this background, it is incumbent on any responsible business to ensure it has layered defence to prevent a ransomware attack, which must include staff education. It must also have a plan to respond to a ransomware attack and ensure there are adequate back-ups of critical data. Failure to take these steps will leave the affected organisation with no good options: facing either irreversible data loss and disruption or the prospect of paying a ransom. This latter option certainly does not guarantee the return of your data, but it will certainly profit criminals and further perpetuate the ransomware threat.

Adam Fisch contributed to this Deep Dive.

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

Better Practice

The latest advice to consider when setting security policies

Updated standard ISO/IEC 27005

For: CISOs, risk, regulatory and compliance teams
The International Standards Organization (ISO) has released an updated version of its security risk management guidelines, ISO/IEC 27005:2018[72]. The standard is one of a dozen standards in the 27000 series of standards that outlines best practices in information security. ISO/IEC 27005 outlines the "why, what and how" for organisations seeking to manage information security risks.
***What's changed?* ISO/IEC 27005 has been updated to reflect a new version of ISO/IEC 27001.**

US government DMARC adoption progress report offers useful insights

For: CISOs and security teams
Domain Message, Authentication, Reporting and Compliance, or DMARC, is a free standard that can be used to protect your organisation from email spoofing based attacks. Given the increase in email-based attacks, including business email compromise, the US Government last October mandated the implementation of DMARC for agencies that operate government email domains. Its most recent progress report[73] offers useful insights into how to implement this increasingly important email security measure.

Setting up two-factor authentication (2FA)

For: Businesses owners, security awareness teams and all staff
The UK's National Cyber Security Centre has created easy-to-consume advice[74] on setting up two-factor authentication for important accounts. As detailed in the Trends and Observations section of this edition of Signals, the need for 2FA and multi-factor authentication to protect critical online services continues to gain focus. The NCSC's guide describes types of 2FA and how to set them up.

FBI launches education campaign

For: Businesses owners, security awareness teams and all staff
Wary of efforts by cyber actors to influence US elections, the FBI has launched a new initiative[76] to educate political campaigns to protect themselves against cyber threats. But the videos – which cover everything from password management to device hardening and incident response – are a great tool for any business looking to secure itself.

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

Endnotes

1 https://www.scamwatch.gov.au/news/beware-scammers-wanting-access-to-your-computer-and-bank-account

2 https://www.scamwatch.gov.au/news/beware-scammers-wanting-access-to-your-computer-and-bank-account

3 https://www.auspaynet.com.au/sites/default/files/2018-07/PaymentFraudStatistics_Jan-Dec2017.pdf

4 https://www.wired.com/story/exactis-database-leak-340-million-records/

5 https://www.ic3.gov/media/2018/180712.aspx

6 https://www.oaic.gov.au/media-and-speeches/news/notifiable-data-breaches-second-quarterly-report-released

7 https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme/quarterly-statistics-reports/notifiable-data-breaches-quarterly-statistics-report-1-april-30-june-2018#executive-summary

8 https://www.justice.gov/opa/pr/three-members-notorious-international-cybercrime-group-fin7-custody-role-attacking-over-100

9 https://www.oaic.gov.au/media-and-speeches/news/notifiable-data-breaches-second-quarterly-report-released

10 https://www.independent.co.uk/news/business/news/data-breach-complaints-increase-gdpr-came-into-force-cybersecurity-a8506711.html

11 https://www.oaic.gov.au/agencies-and-organisations/business-resources/privacy-business-resource-21-australian-businesses-and-the-eu-general-data-protection-regulation

12 https://www.asb.co.nz/content/dam/asb/documents/reports/signals/asb-signals-2018-q2.pdf

13 https://instagram-press.com/blog/2018/08/28/new-tools-to-help-keep-instagram-safe/

14 https://techcommunity.microsoft.com/t5/Azure-Active-Directory-Identity/Baseline-security-policy-for-Azure-AD-admin-accounts-in-public/ba-p/245426

15 https://www.reddit.com/r/announcements/comments/93qnm5/we_had_a_security_incident_heres_what_you_need_to/

16 https://krebsonsecurity.com/2018/08/reddit-breach-highlights-limits-of-sms-based-authentication/

17 https://www.cert.govt.nz/it-specialists/critical-controls/multi-factor-authentication/

18 https://krebsonsecurity.com/2018/07/google-security-keys-neutralized-employee-phishing/comment-page-3/

19 https://www.commbank.com.au/content/dam/commbank/assets/business/can/business-insights/signals/Signals-Q12018.pdf

20 http://www.abc.net.au/news/science/2018-07-16/my-health-record-experts-say-its-safe-privacy-concerns-remain/9981658

21 https://www.singhealth.com.sg/AboutSingHealth/CorporateOverview/Newsroom/NewsReleases/2018/Pages/cyberattack.aspx

22 https://www.oaic.gov.au/media-and-speeches/news/notifiable-data-breaches-second-quarterly-report-released

23 http://thehill.com/policy/cybersecurity/404477-hackers-increasingly-target-reputations-through-reviews-sites-experts

24 https://motherboard.vice.com/en_us/article/xwk3wq/hackers-sextortion-half-million-blackmail-caught-watching-porn

25 https://pdf.ic3.gov/2017_IC3Report.pdf

26 https://newsroom.fb.com/news/2018/04/hard-questions-protecting-peoples-information/

27 https://newsroom.fb.com/news/2018/08/more-coordinated-inauthentic-behavior/

28 https://www.afr.com/business/media-and-marketing/advertising/facebook-working-with-australian-authorities-ahead-of-federal-election-20180901-h14ts1

29 https://newsroom.fb.com/news/2018/09/security-political-campaigns/

30 https://securelist.com/new-trends-in-the-world-of-iot-threats/87991/

31 https://www.ic3.gov/media/2018/180802.aspx

32 https://www.zdnet.com/article/new-hakai-iot-botnet-takes-aim-at-d-link-huawei-and-realtek-routers/

33 https://www.zdnet.com/article/first-iot-security-bill-reaches-governors-desk-in-california/

34 https://www.forbes.com/sites/thomasbrewster/2018/07/15/toka-will-hack-internet-of-things-for-government-intelligence-agencies/amp/

35 https://www.cyberscoop.com/cellebrite-iot-data/

36 https://www.ic3.gov/media/2018/180802.aspx

37 www.staysmartonline.gov.au

38 www.nomoreransom.org

39 https://www.telstra.com.au/business-enterprise/solutions/security/security-report-2018

40 https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/kansas-hospital-hit-by-ransomware-extorted-twice

41 https://www.wired.com/2017/05/wannacry-ransomware-hackers-made-real-amateur-mistakes/

42 https://www.nomoreransom.org/en/ransomware-qa.html

43 https://securelist.com/synack-targeted-ransomware-uses-the-doppelganging-technique/85431/

44 https://digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time

45 https://www.fortinet.com/blog/threat-research/ransomware-as-a-service-rampant-in-the-underground-black-market.html

46 https://www.smh.com.au/politics/federal/increasing-cyber-crime-attacks-costing-up-to-1b-a-year-20180410-p4z8ui.html

47 https://securelist.com/expetrpetyanotpetya-is-a-wiper-not-ransomware/78902/

48 https://www.theguardian.com/world/2017/jun/27/petya-ransomware-attack-strikes-companies-across-europe

49 https://www.whitehouse.gov/briefings-statements/statement-press-secretary-25/

50 https://www.computerweekly.com/news/450426854/NotPetya-attack-cost-up-to-15m-says-UK-ad-agency-WPP

51 https://www.wsj.com/articles/one-year-after-notpetya-companies-still-wrestle-with-financial-impacts-1530095906

52 https://www.ft.com/content/a44ede7c-825f-11e7-a4ce-15b2513cb3ff

53 https://arstechnica.com/information-technology/2017/04/nsa-leaking-shadow-brokers-just-dumped-its-most-damaging-release-yet/

72 https://www.iso.org/news/ref2309.html

73 https://3l9nb01u2hkg4cz5053evqwi-wpengine.netdna-ssl.com/wp-content/uploads/2017/08/Agari_DMARC_Adoption_Report_Federal_2018.pdf

74 https://www.ncsc.gov.uk/guidance/setting-two-factor-authentication-2fa

75 https://cyber.gov.au/

76 https://www.fbi.gov/investigate/counterintelligence/foreign-influence/protected-voices

83 https://www.cert.govt.nz/

84 http://www.abc.net.au/news/2018-08-23/huawei-banned-from-providing-5g-mobile-technology-australia/10155438

85 https://www.privacy.org.nz/privacy-for-agencies/gdpr-resources/

Editorial Panel

Contributors

John Hare
Executive Manager, Cyber Outreach, Commonwealth Bank

Martha McKeen
Senior Manager, Cyber Outreach, Commonwealth Bank

Pete Steel
Acting CISO and Chief Digital Officer, Commonwealth Bank

Melanie Timbrell
Senior Manager, Cyber Outreach, Commonwealth Bank

Briana Wade
Graduate, Cyber Intelligence, Commonwealth Bank

Arjun Ramachandran
Guest Contributor

Reviewers

Kate Ingwersen
General Manager, Office of the CISTO, Commonwealth Bank

Ryan Cotterell
Head of Information Security, ASB

Malcolm Allen
Information Security Consultant, ASB

Observations made in Signals are made using the confidence matrix and estimative language used by the US CIA. Our choice of words is very deliberate and based on both data and observations we source from our own telemetry and a measured degree of confidence in external sources.

Certainty	100%
Almost Certain	93% (give or take 6%)
Probable	75% (give or take 12%)
Even	50% (give or take 10%)
Unlikely or improbable	30% (give or take 10%)
Impossible	0%

Confidence in our assessments

High Confidence - based on high quality information from which it is possible to derive a solid judgment.

Moderate Confidence - based on information from trusted or reliable sources, without the necessary data or corroboration to warrant a higher level of confidence.

Low Confidence - the information is poorly corroborated, but is otherwise logical and consistent with a source's motivations.