HEALTHCARE

Sector Overview

Cyber threats to the Australian healthcare and medical sector are increasing in complexity and volume. Threats to this sector are not unique to Australia alone, with Australian healthcare experiencing similar threat trends to those observed globally. In the first half of 2021, cyberattacks caused information technology downtime in roughly half of all hospitals worldwide.

The global Covid-19 pandemic correlated strongly with a wave of nation-state cyber espionage attacks against the health sector. Several countries hoped to gain access to vaccine data and medical information to help their country respond to the public health crisis. The economic shock from the pandemic also contributed to an increase in economic hardships that led to healthcare organisations becoming a top target for cybercriminals due to the industry's generally immature cyber security posture and increased attack surface due to the shift to virtual/telemedicine from in-person care. Health-related themes also became common in phishing campaigns that leveraged psychological fears to commit fraud.

In Australia, the healthcare sector experienced an 84% increase in reported cyber incidents between 2019 and 2020, with 85 data breaches recorded in the first half of 2021 alone. While financial loss, operational impact, and reputational damage are all costs of cybersecurity failures for any company, a cyber-attack in healthcare carries an additional danger of patient harm. So, what is the scale of the threats and risks?

Australia has a massive health and medical sector with 746 public and 601 private hospitals and over 6300 general practitioners (GP) clinics. The public hospital system employs over 52,000 doctors and 175,000 nurses. There are also 31 independent primary health network (PHNs) organisations working to streamline health services and improve services for those at risk of poor health outcomes and better coordinate care. This complex web of health service providers needs to uplift internal processes, legacy systems and have a clear understanding of how and where personal data is handled throughout their networks. Threat intelligence is vital to prioritising informed risk management approaches for this sector.

Threat Trends & Issues in Australia's Health Sector:

Improvements in healthcare technology

Health industry digitisation is projected to increase because of the growth in electronic medical recordkeeping systems and devices, which produce large volumes of data. Artificial intelligence, virtual reality, and wearable medical technology are all promising technologies that improve remote patient monitoring and better health outcomes for individuals with chronic diseases.

More remote health services

COVID-19 had a tremendous impact on healthcare professionals and patients with the rapid increase in telehealth which has gone mainstream and will be retained given the economic

and extension of care to remote communities this model of medicine provides. and this extends to other medical services like e-Prescriptions for pharmaceuticals.

Digital solutions for an aging population

Demographics and economics drive the expansion of digital healthcare and remote medical services. Today there are roughly 3.8 million Australians aged 65 and over out of a total population of 25 million. Australia is expected to have 8.8 million elderly persons (22% of the population) by 2057. The aging of the population poses several challenges, including an increase in the total case numbers of chronic diseases driving demand for vital services for the elderly. Australia's Elderly Care Royal Commission found that digital transformation, wearable technology, and smart modular housing offer the greatest chances to revolutionise and cope with this surge in aged care in the years to come. The increased use of so many new devices and the way they connect to the internet also exposes technology and people to new threats that may directly impact the physical well-being of people and the security of their personal data.

Russian APT threats to the Health Sector:

The sectors traditionally targeted by state-sponsored Russian cyberespionage organisations have been those directly related to Russian geopolitical and economic goals. The pharmaceutical and healthcare sectors, however, became more significant in the Covid-19 pandemic with increased threats from Russian advanced persistent threat (APT) groups. For Russia, APT28 and APT29 targeted overseas clinical researchers and pharmaceutical businesses in an effort to obtain COVID-19 intellectual property.

APT29: aka Cozy Bear, The Dukes, YTTRIUM, and Iron Hemlock are other aliases for APT29. Healthcare, pharmaceuticals, academics, energy, finance, government, media, and technology are among the targeted sectors. Incidents tied to the group include attacks on COVID-19 vaccine developers in 2020 and at least one U.S. hospital. The group was also behind the SolarWinds attack in 2020.

APT28: aka, Fancy Bear, Group 74, PawnStorm, Sednit, Snakemackerel, Sofacy, STRONTIUM, TG-4127, Tsar Team, and Iron Twilight are other aliases for APT28. Healthcare, aerospace, defence, energy, government, military, and the media are among the targeted sectors. Password spraying and brute force attacks to compromise credentials and obtain initial access are commonly employed by APT28 in attacks.

Common Attack Types Against Health Sector:

Ransomware:

There were 137 ransomware incidents in healthcare globally in 2021, with Australia being the

victim of five of these attacks. In Victoria in 2019, a ransomware attack simultaneously shut down seven significant regional health service providers. Cybercriminals are progressively focusing their attacks on the healthcare industry while expanding their operations and raising the sophistication of their tactics, techniques, and procedures (TTPs), allowing them to launch more effective attacks.
One example is when ransomware was spread throughout United States hospitals by exploiting outdated JBoss server software. Instead of infecting the hospitals through routinely used staff workstations, the attacker uploaded malware on the outdated server without the victim's knowledge. One of the hospitals impacted was Hollywood Presbyterian Facility in California. The incident caused a delay in patient treatment and ultimately required the hospital to pay $17,000 to regain access to its network and files.

Another example is the ransomware assault at UnitingCare Queensland on April 25, 2021, one of many cyber breaches in the Australian healthcare industry. The internal IT system of the hospital group was impacted, requiring them to switch to paper-based processes. The attack was attributed to the REvil/Sodinokibi ransomware group.

Malware

Using legitimate tools like VLC Media Player, recent Gootkit malware loader attacks have targeted the Australian healthcare industry. For initial access, Gootkit, or Gootloader, uses search engine optimisation poisoning techniques (spamdexing). It usually operates by compromising and abusing legitimate infrastructure and then seeding the compromised sites with popular terms. Similar to other malware of its kind, Gootkit is capable of keylogging, adversary-in-the-browser (AitB) assaults, data theft from the browser, screenshotting, and other malicious actions.

Data breaches

In the healthcare industry, breaches are frequently reported. These can be brought on by a variety of circumstances, such as malware that steals login credentials, an insider mistakenly or purposefully disclosing patient information, or misplaced laptops or other gadgets. On the black market, Personal Health Information (PHI) is more valuable than credit card information or standard Personally Identifiable Information (PII). Cybercriminals have a greater motivation to target medical databases as a result.

PHI can sell for up to $363, whereas credit card information and other PII are only worth $1 to $2 on the black market. PHI is valuable because criminals may use it to lure victims into falling for fraud and extortion that exploits their medical issues. Additionally, it can fabricate insurance claims, enabling the purchase and selling of medical supplies.

In an alleged coordinated cyber-attack from Russia, nearly 10 million Australians had their private health information stolen, with private medical records revealing treatments for

alcoholism, drug addictions, and pregnancy terminations posted online. The largest private health insurance provider in Australia, Medibank, had its databases breached by a Russian ransomware group, which stole customer information from the business' computer systems over a period of weeks. Sensitive data was made available on the dark web by hackers after Medibank declined to pay the ransom.

Responding to threats against the energy sector in Australia:

Most healthcare sector entities won't be able to share 'machine to machine' intelligence, so an industry partner is needed as the enabler/facilitator for cyber threat intelligence (CTI) and collective defence via other means. By taking on the role of the trusted advisor/facilitator for the intelligence exchange, an industry organisation would ensure the overall quality of information flowing through its systems and out to the CI members.

'Forewarned is Forearmed', and by joining a trusted cyber community of Critical Infrastructure owners and operators responsible for protecting their healthcare infrastructure assets, you can join the movement to share contextual intelligence and proactively approach cyber defence. Cyber threat activity shared into the CI-ISAC ecosystem by one member has the potential to help others across the sector and the broader CI community stop similar attacks before they impact operations.

CI-ISAC, as a not-for-profit, member driven organisation, with a mission to serve its members and in turn their customers by building a trusted community and leveraging the best technology in its intelligence platform, and drawing on resources and resilience through its industry peer-to-peer network to anticipate, mitigate, and respond to cyber threats.

More information on CI-ISACs sovereign intelligence-sharing capability can be found on the official website: https://www.ci-isac.com.au , or by emailing info@ci-isac.com.au.

Published: 6th March 2023