HIGHER EDUCATION & RESEARCH

Sector Overview

There are over 170 higher education providers in the Australian higher education system currently authorised by the Tertiary Education Quality and Standards Agency [1]. Providers include universities, universities of specialisation, institutions operated by overseas universities, and other higher education providers. The sector is internationally recognised to provide high quality educational outcomes to its students.

The Australian higher education sector is also heavily targeted by cybercrime, ranking as the fourth most targeted in the world [2]. When compared to the first half of 2021, the Australian education sector had a 17% rise in cyberattacks, with an average of 3,934 attacks per week in July [2,3,4]. The risks these attacks create are exacerbated by three key cyber security factors.

Cyber security factors in Australian higher education sector

Growth in digitisation

Ongoing digitisation trends and the reliance on networked devices these trends create are a key factor of higher education cyber security. The proliferation of devices used by students and staff, used on campus and at home, increase institutions' attack surfaces, extending them to environments that institutions poorly control. Taken in conjunction with the growth in storing and processing sensitive personal information, academic research information, intellectual property, and cutting-edge technology information on computers, the Australian higher education industry is becoming more and more susceptible to cyberattacks while also presenting more attractive targets.

Use of legacy systems

Many institutions in Australia often rely on outdated networks and technology. Legacy systems contain many security flaws, which are exacerbated by limited funding in the sector. Investment prioritisation towards new research and systems leaves legacy systems performing critical functions and processing high value information, perpetuating risks and giving attackers easy opportunities to exploit these weaker links.

Increasing connectivity between different institutions

Academic research benefits from sharing information with businesses and other higher education institutions. Inter-institutional connectivity creates trust arrangements providing additional attack surfaces. Digitised supply chains proliferate those surfaces with other vendors and supply partners. Adversaries frequently target those external attack surfaces to gain access to internal environments.

Threat actors targeting Australian universities:

Threat actors are taking advantages of these cyber security factors to target the confidentiality, integrity and availability of higher education institutions' critical data. There are multiple actors who are known to target this sector.

Mabna Institute (TA407)

The Mabna Institute is believed to have targeted up to 29 Australian universities over the last decade. It has stolen research, scholarly journals, theses, dissertations, and eBooks using stolen credentials. It is suspected of stealing 31 terabytes of data from the global higher education sector between 2013 and 2017 [5].

Their favoured technique is to induce victims to visit a fake login page by sending them phishing emails, impersonating library employees. These login pages appear legitimate, frequently incorporating widely publicised maintenance notifications and alerts. After inputting their login information into the fake website, victims are led to the actual university website. The exploitation of compromised accounts to obtain academic data and send further phishing emails then follows.

Red Apollo (APT10)

Red Apollo is a state-sponsored threat actor with ties to the Chinese Ministry of State Security, based in mainland China. It is expected to expand operations into the education sector in countries allied with the United States in coming years. Red Apollo Group focuses specifically on stealing intellectual property from educational institutions.
Red Apollo commonly uses spear-phishing as a technique. Emails are sent to students with a malicious zip file containing malware. They employ fake domains that look like those of actual organisations. ChChes, a Trojan that was used to attack Japanese institutions, is a frequently used malware tool by the group.

Winnti

Winnti Group is an actor associated with Chinese state intelligence. It employs a family of malware of the same name. Two Hong Kong institutions were targeted in a new Winnti Group attack that was discovered in November 2019. The group's signature backdoor, the ShadowPad, has been evolved and contain a new launcher with multiple modules. A few weeks before ShadowPad was first discovered, the Winnti malware was also discovered at these universities. Winnti attempts to reach the host network by phishing emails before infecting the network with malware like Cobalt Strike. Winnti uses genuine software, also known as living of the land binaries (LOLbins) to obtain additional access after infecting the host network, decreasing the likelihood that it would be discovered. When one infected network has access to other networks, such as a parent organization, Winnti has been observed spreading laterally from one network to another. The group maintains longer-term persistence by leaving backdoors, like ShadowPad behind in infected networks.

Vice society

Vice Society the largest threat to the education sector in 2022. Vice Society, like many other ransomware gangs, is infamous for stealing data from victims' networks before encrypting it to double-extort money by threatening to broadcast the material on the dark web if the victim does not pay the demanded ransom [7].

Vice Society's activities are distinct from those of many other ransomware organisations, such as LockBit, which operate according to a standard ransomware-as-a-service (RaaS) model. Instead, Vice Society is notorious for employing unique malware tool including HelloKitty (also known as FiveHands) and Zeppelin [8]-[10].

Attacks on Australia:

Attacks against Australian higher education institutions will continue to evolve. Recent examples include attacks on the ProctorU remote examination tool and against the ANU Enterprise Systems Domain (ESD)

During the coronavirus pandemic, students in universities all around Australia took examinations at home under remote supervision using the online resource ProctorU. The online tool was hacked, resulting in the theft of 444,000 ProctorU members' personal information, which was then posted online on hacker forums [6].

The ANU network was breached by a skilled actor in November 2018. ANU's ESD, which holds systems for managing finances, student administration, human resources, and enterprise e-forms, was breached as a result of this attack. The threat actor was able to copy and take an undetermined amount of data through accessing the ESD.[11]

Responding to threats against the higher education sector in Australia

Most Education 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 education 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.org.au, or by emailing info@ci-isac.org.au.

Published: 26th April 2023

References:

[1] https://www.universitiesaustralia.edu.au/policy-submissions/teaching-learning-funding/australian-higher-education/

[2] https://australiancybersecuritymagazine.com.au/education-sector-sees-29-increase-in-attacks-against-organisations-globally/

[3] https://blog.checkpoint.com/2021/08/18/check-point-research-education-sector-sees-29-increase-in-attacks-against-organizations-globally/

[4] https://www.theeducatoronline.com/k12/news/australian-education-sector-increasingly-susceptible-to-cyberattacks--study/278452

[5] https://www.sbs.com.au/news/article/up-to-26-australian-universities-targeted-in-iran-hack-campaign-fbi/w33mxygco

[6] https://www.sbs.com.au/news/article/australian-universities-investigating-deeply-concerning-hack-of-controversial-exam-software/hcvj1ezjx

[7] https://unit42.paloaltonetworks.com/vice-society-targets-education-sector/
[8] https://blog.sygnia.co/the-vice-society-ransomware-investigation?_ga=2.53394472.1018667264.1662386306-1370422011.1660598013

[9] https://www.bleepingcomputer.com/news/security/vice-society-claims-lausd-ransomware-attack-theft-of-500gb-of-data/

[10] https://www.bleepingcomputer.com/news/security/vice-society-claims-ransomware-attack-on-med-university-of-innsbruck/

[11] https://apo.org.au/node/262171#:~:text=In%20early%20November%202018%2C%20a,and%20enterprise%20e%2Dforms%20systems