AUSTRALIAN UNIVERSITIES UNDER ATTACK

Cyber Threat Report

A Macquarie University
CiLab - PACE Project
BACKGROUND

The Australian higher education sector is increasingly vulnerable to cyber attacks as it embraces digital transformation in the storage of vast amount of personal information, academic research, intellectual property and innovative technology.

The Australian National University (ANU) cyber-attack of 2018 served as a wake-up call for many in the education sector, when a suspected state-sponsored actor accessed the sensitive personal information of 200,000 alumni, current students and employees, exfiltrating data such as names, addresses, passports and bank account details. Potentially, the information gained could have been used to recruit/blackmail future sources or even surveil critics.

At the time, the ANU hack prompted several universities to re-evaluate the risks posed by cyber threat actors globally. As cybercrime groups continuously evolve and improve on their technologies, Australian universities need to ensure they do not lag behind in updating their security procedures and protective measures to prevent future attacks on their infrastructure.

This report, presented by the Macquarie University Cyber Intelligence Lab (CiLab), has identified five cyber threat actors who pose varying levels of threat to Australian universities.

A number of observations emerged across the investigations of different attacks:

- Spear-phishing attacks using social engineering to exploit human error are the backbone of cyber operations across all threat actors;

- There is some degree of commonality between threat actors from China such as Winnti and Double Dragon as they shared malware and attack styles from previous operations; and

- The politically-motivated state and state-sponsored actors tend to be more sophisticated and targeted in their attacks, whereas independent cybercriminal groups such as the Mabna Institute and NetWalker are generally more indiscriminate and less sophisticated.

Australian universities should be aware and anticipate potential cyber intrusions from the threat actors identified in the next pages, each possessing different motivations and skill sets.
The Mabna Institute is an Iranian company formed in 2013. According to Secureworks’ Counter Threat Unit Research Team, the Institute has targeted at least 380 universities from over 30 countries. This data comprises 20 Australian universities, including every institution from the 'Group of Eight', with Monash University being by far the most heavily attacked. Many of these universities are heavily involved in academic research and in producing intellectual property, which makes them a valuable target.

Between 2013 and 2017, the Mabna Institute is believed to have stolen 31 terabytes of data worth US$3.4 billion in the higher education sector. Nine members of the Institute were charged by the US Department of Justice in 2018, though it did little to deter further attacks.
TECHNICAL MEANS

The Mabna Institute utilises relatively straightforward cyber intrusion pathways in a professional manner.

They use phishing emails, often imitating library staff, asking victims to follow a URL to a spoofed login page. These login pages are highly accurate, often using publicised maintenance notices and alerts to add to their authenticity.

Victims are redirected to the legitimate university site after entering their login credentials into the spoofed site. According to the Proofpoint Threat Insight Team, compromised accounts are then used to send further phishing emails as well as access academic data.

Stolen academic data is then sold on to the Iranian Government as well as universities and companies. This tactic has changed little due to its relatively high success rate.

The Mabna Institute uses publicly available tools such as SingleFile and HTTrack Website Copier as well as URL shorteners and free domains.

<table>
<thead>
<tr>
<th>University</th>
<th>Count</th>
<th>University</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monash University</td>
<td>71</td>
<td>Curtin University</td>
<td>3</td>
</tr>
<tr>
<td>University of South Queensland</td>
<td>13</td>
<td>Griffith University</td>
<td>2</td>
</tr>
<tr>
<td>University of Melbourne</td>
<td>11</td>
<td>University of Newcastle</td>
<td>2</td>
</tr>
<tr>
<td>University of Sydney</td>
<td>10</td>
<td>University of Tasmania</td>
<td>2</td>
</tr>
<tr>
<td>La Trobe University</td>
<td>10</td>
<td>University of Western Queensland</td>
<td>2</td>
</tr>
<tr>
<td>University of New South Wales</td>
<td>9</td>
<td>Queensland National University</td>
<td>2</td>
</tr>
<tr>
<td>University of Southern Queensland</td>
<td>5</td>
<td>University of New South Wales</td>
<td>2</td>
</tr>
<tr>
<td>Queensland University of Technology</td>
<td>4</td>
<td>University of Wollongong</td>
<td>2</td>
</tr>
<tr>
<td>University of Technology Sydney</td>
<td>4</td>
<td>Southern Cross University</td>
<td>1</td>
</tr>
<tr>
<td>Victoria University</td>
<td>4</td>
<td>Swinburne University</td>
<td>1</td>
</tr>
</tbody>
</table>
OVERVIEW

Red Apollo was first noticed in 2009. Their activity has been detected on six continents, but particularly in Australia, Japan and the United States (PwC; Bae Systems).

Their campaign known as 'Operation Cloud Hopper' targeted managed IT service providers (MSPs) and included a sub-campaign aimed at Meiji University as well as Tokyo University.

Red Apollo operates according to political objectives and initiatives like the 'Made in China 2025' plan. The aim is to access and collect sensitive data and intellectual property. They also engage broadly in cyber espionage.
Spear-phishing is primarily used, based on significant prior intelligence collection on targets. This indicates some level of sophistication in their operations.

For example, spear-phishing emails to Japanese universities titled ‘Scientific Research Grant Program’ included a compromised zip file containing a ChChes malware.

They use spoofed domains similar to legitimate organisations such as: 'u tokyo-ac-jp[.]com' instead of 'u-tokyo.ac.jp' for Tokyo University.

Red Apollo is known to use Quasar as a malware in addition to Haymaker, Bugjuice and Snugride to disrupt systems according to FireEye iSIGHT Intelligence (2017). Once the group gains access, they collect data and move it to infrastructure they control.

Attacks have been limited to Japanese universities mitigating the Red Apollo threat to Australian Universities. However, cyber espionage activities attributed to Red Apollo have been detected in Australia according to PwC & BAE Systems.
First identified in a Kaspersky report, the Winnti Group is both a hacker group and a type of malware. Winnti began conducting attacks on gaming companies in 2013 and by 2019, subsequently shifted their focus to the education sector.

Winnti infiltrated two Hong Kong universities at the height of the Hong Kong independence protests. Although the type of information stolen remains unclear, the goal was to disrupt pro-democracy protests conducted by students who attended the universities, and was politically motivated on behalf of the Chinese government according to ESET (2020).
Winnti have been associated with multiple hacker groups such as LEAD, Axiom, BARIUM and Wicked Panda due to similar malware, resources, infrastructure, and suspected backing by the Chinese government. However, the exact nature of the shared infrastructure and shared resources between these groups is currently unclear.

Winnti aims to gain access to the host network through phishing emails, then uses trojan horse malware such as **Cobalt Strike** to infect the network. Once the host network is infected, Winnti uses legitimate software to gain further access, lowering the chances of being detected.

Winnti has also been known to move laterally from one network to another in cases where one infected network has access to other networks, such as a parent organisation.

Lastly, they utilise backdoor platforms such as **Shadowpad** to provide easy access upon re-entering the host network.

Winnti’s threat to Australian universities is mainly attributed to the fact that they are very sophisticated and their target sectors now include higher education. Moreover, the threat is compounded by the large amount of resources at Winnti’s disposal due to the sharing of infrastructure and resources within the group.
According to FireEye, Double Dragon is a Chinese state-sponsored cyber espionage and cybercrime group. Evidence from Chinese internet forums has shown that users who are linked to Double Dragon also advertise their hacking services outside of office hours.

This leads us to conclude that members of this group are working two jobs, supporting the assumption that Double Dragon is made of regular citizens with excellent programming skills. These skills are then leveraged by the Chinese government.
Double Dragon began targeting the video game industry with ransomware in 2012, and have since dramatically built up the number of sectors they target.

Advanced spear-phishing emails are initially used to gain access to targeted systems, and then sophisticated malware is deployed to stay hidden in the system and collect data.

Espionage conducted by Double Dragon is likely to be motivated by information gain from multiple industries, in order to support China’s ‘Made In China 2025’ plan, a strategy aimed at transforming the country into a manufacturing superpower for next-generation technology.
OVERVIEW

Discovered in 2019, NetWalker is a cybercriminal group that uses their own branded malware to infiltrate networks, hold victims to ransom and demand payment. There is no evidence of state-sponsorship by Russia.

While NetWalker do conduct their own attacks they also have recently expanded their services to include a ransomware-as-a service (RaaS) model.

Among several US universities in 2020 alone, NetWalker successfully attacked the University of California which paid US$1.14 million in ransom (Tidy 2020) and the University of Utah which paid US$457,059 (Cimpanu 2020).
TECHNICAL MEANS

NetWalker malware gains initial access to systems through spear-phishing emails with malicious attachments and trojanised applications, compromised accounts or large-scale network intrusions.

NetWalker have used post-exploit toolkits, fileless delivery and 'living off the land' tactics (legitimate software) to make their ransomware both more effective and more difficult to detect.

Recent attacks have delivered the ransomware payload through a reflective dynamic-link library injection, specifically through a PowerShell loader.

The script is buried within various layers of encryption, and the ransomware runs code directly in memory space without being stored onto the disk, shielding it from antivirus detection.

Figure 6
NetWalker Victim Journey

NetWalker Targetting Australian Businesses

In January 2020, Australian transportation and logistics company Toll Group were compromised. NetWalker left a backdoor that was used in March by another criminal affiliate called Nefilim, and led to 200GB of Toll Group’s files being released on the dark web. Other Australian businesses attacked in 2020 include customer experience firm Stellar (May), design firm Tandem Corp and lighting company Jands (September respectively).
THREAT REVIEW

The threat to Australian universities is significant considering NetWalker’s sophisticated technical abilities and their interest in the education sector and Australian businesses.

This is supported by the Australian Signals Directorate in 2020, who singled out universities to be on high alert for NetWalker.

It remains difficult to tell whether specific attacks are driven by NetWalker themselves or RaaS affiliates, and how deeply NetWalker is linked with other criminal ransomware groups.

In light of past attacks on educational institutions both domestic and foreign, academia must prioritise the protection of sensitive personal data, academic research, intellectual property as well as other important functions and services of Australian universities.

Cyber threat actors, including those not featured in this report, have seen significant growth in activity in recent years. The field continues to be highly dynamic, and further research will be needed to identify and assess these threats as they evolve.
AUTHORS

This report was prepared in collaboration with:

**CiLab Master Interns:**
Amanta Cotan (Leader)
Andreane Laurin
Priandhini Triana Asih

**PACE Team Members:**
Cooper Anderson
Arad Behdarvand
Andrew Cameron
Talia Chalita
Celine Dimaano
Hayden Fergusson
Cameron Lawrence
Danielle Le Large (Leader)
Matthew Le Guay
Megan Megevand
Wyatt Mola (Leader)

**Academic Mentors:**
Stephen McCombie
Fred Smith
Allon Uhlmann


BIBLIOGRAPHY CONT.


