Australian National University

INCIDENT REPORT

ON THE BREACH OF THE AUSTRALIAN NATIONAL UNIVERSITY'S ADMINISTRATIVE SYSTEMS

CONTENTS

VICE-CHANCELLOR'S FOREWORD

In June 2019, I notified our community we had been the victims of a cyber attack.

In the wake of that announcement I committed to making our investigation public. I wanted to be as transparent with you as possible about what happened, how it happened and why it happened. And by doing so, I also want to encourage disclosure of these attacks more broadly.

This incident report provides details on the attack including the methods used by the attacker to infiltrate The Australian National University (ANU) systems. To my knowledge, this publicly available report is the first of its kind in Australia following a cyber attack on a public institution.

I have made this report public because it contains valuable lessons not just for ANU, but for all Australian organisations who are increasingly likely to be the target of cyber attacks. It is confronting to say this, but we are certainly not alone, and many organisations will already have been hacked, perhaps without their knowledge. I hope this report will help them protect themselves, and their data and their communities.

As I said in my statement on 4 June 2019, the perpetrators of our data breach were extremely sophisticated. This report details the level of sophistication, the likes of which has shocked even the most experienced Australian security experts.

While it's clear we moved quickly to implement hardening and security improvement measures following our first cyber-attack in May 2018, this report shows we could have done more.

The report outlines where those lessons for ANU have been learned and what we are doing to further protect our systems. But we have to strike a balance and this report cannot be an instruction manual for would-be hackers to launch another attack. I have asked for this report to be as transparent as is allowable to ensure our community is well-informed, but not so that criminals are armed with information that compromises our systems or that of another organisation.

Despite our considerable forensic work, we have not been able to determine, accurately, which records were taken. However, our analysis has been able to establish that while the hackers had access to data up to 19-years-old, the hackers took much less than the 19 years' worth of data we originally feared. We also knew the stolen data has not been further misused. Frustratingly this brings us no closer to the motivations of the actor.

I thank all those involved in the response to this incident and in the preparation of this report, particularly our colleagues across Commonwealth security agencies, IDCARE and Northrop Grumman.

Finally, and most importantly, I wish to apologise to the victims of this data breach: our community. We are working constantly to ensure the protection of the data you entrust us with; and are investing heavily in measures to reduce the risks of this occurring again, including a multi-year information security investment program. But we must all remain vigilant and follow the advice of security experts to protect our personal information.

Professor Brian P. Schmidt AC

Vice-Chancellor and President
The Australian National University

EXECUTIVE SUMMARY

In early November 2018, a sophisticated actor gained unauthorised access to the ANU network. This attack resulted in the breach of part of the network known as the Enterprise Systems Domain (ESD), which houses our human resources, financial management, student administration and enterprise e-forms systems.

By gaining access to ESD, the actor was able to copy and steal an unknown quantity of data contained in the above systems. There is some evidence to suggest the same actor attempted to regain access to ESD during February 2019, but this second attack was ultimately unsuccessful.

Indications of an intrusion were first detected in April 2019 during a baseline threat hunting exercise. The hunt uncovered network traffic data suggesting the presence of a malicious actor whose characteristics were distinct from the actor detected during the breach reported by the University in May 2018. The new detection precipitated an incident response, led by Northrop Grumman, working with ANU cybersecurity staff. The incident response team uncovered the data breach on Friday 17 May and verbally reported it to the Vice-Chancellor that day.

The initial means of infection was a sophisticated spearphishing email which did not require user interaction, ie clicking on a link or downloading an attachment.[1] The actor's dwell time on the ANU network was approximately six weeks, with most malicious activity ending around mid-December 2018, although there were some further attempts after this time.[2]

The actor's activity was contained to a handful of systems, although they had gained broader access. It is clear from the pathway taken by the actor the sole aim was to penetrate ESD and gain unauthorised access to the systems mentioned above. There is no forensic evidence to suggest the actor accessed or displayed any interest in files containing general administrative documents or research data; nor was the ANU Enterprise Records Management System (ERMS) affected.[3]

At the time of the public announcement, ANU was not able to ascertain how much data or specifically which fields might have been accessed. As such it was assumed that all data, dating back some 19 years, had been potentially affected and reported as such to err on the side of caution. More recent forensic analysis has been able to determine that the amount of data taken is much less than 19 years' worth; although it is not possible to determine how many, or precisely which, records were taken.[4] This analysis is based on duration of exfiltration activity and known, albeit incomplete, data volumes.

ANU worked closely with, and reported findings to, the Australian Cyber Security Centre (ACSC) and the Office of the Australian Information Commissioner (OAIC), before public notification. During the intervening two weeks between the detection of the breach and the public announcement on Tuesday 4 June 2019, we implemented a range of additional security controls inside ESD and the broader network – many of these activities were to expedite hardening measures already scheduled for implementation.

1 Spear-phishing emails are a form of malicious email targeting an individual or organisation. They mimic legitimate mail and contain malicious attachments or links designed to steal credentials or enable the install malware.
2 Dwell time refers to the amount of time the actor spent on the network undetected.
3 The ANU ERMS is the central repository for the University's records.
4 This analysis is based on duration of exfiltration activity and known, albeit incomplete, data volumes.

ANU needed to undertake these measures before publicly announcing the breach because there were ongoing attempts to gain (or potentially regain) access to ESD as new protections came online. We were also advised ANU would likely be subject to secondary attacks from other opportunistic actors once the data breach was made public. It is worth noting that ANU was subject to further intrusion attempts within one hour of the public announcement and on the following day, both of which were stopped.

The tactics, techniques and procedures used during the attack highlight the sophistication and determination of the actor.[5] In addition to their efficiency and precision, the actor evaded detection systems, evolved their techniques during the campaign, used custom malware and demonstrated an exceptional degree of operational security that left few traces of their activities.

To ensure the protection of personal information the University has added additional protection to the affected systems, and there is ongoing work to further reduce risks to our data. The University continues to scan online sources for evidence of stolen data being traded or used illegally. At the time of this report, there is no evidence of such activity. ANU will continue this work with specialist service providers and will notify affected parties if there is any evidence their data has been misused.

That said, ANU acknowledges several technical vulnerabilities and people and process issues that contributed to the success of the actor's campaign. ANU has either addressed these issues or, for more complex issues, is in the process of developing a response and remediation plan as part of our strategic information security program. A summary of lessons can be found in Table One of this report.

ANU has increased its technical cybersecurity efforts considerably since its first breach in May 2018 and is now nearing the end of the tactical measures program arising from that incident. However, given the complexity and age of the IT network, the rollout of these measures has taken considerable time. Without the measures already in place, the second intrusion would not have been detected, and the subsequent attacks might have been more successful. Unfortunately, there was not sufficient time to universally implement all measures across the ANU network between the two attacks in 2018. The sophistication and speed of the second attack underscore the threat environment in which we, and other organisations, now operate.

Technical gaps aside, ANU ultimately views this breach and cybersecurity more broadly as an organisational issue, one which requires a change to the University's security culture to adequately mitigate. It is through this lens we will undertake the next phase of our cybersecurity work – a strategic information security program. This program encompasses the modernisation of IT and security infrastructure and, more importantly, an emphasis on culture and security awareness among students, staff and researchers; and the protection of the data they entrust to ANU.

The investigation following the breach, which contributed to the contents of this report, was conducted in close cooperation with Australian Government security agencies and Northrop Grumman. ANU is grateful for their continued support.

5 Tactics, techniques and procedures or TTPs refers to the methodology and tools used by the actor in gaining access and taking out stolen information.

DETAILED TIMELINE OF THE DATA BREACH

Overview

This section provides a chronological account of the data breach based on available forensic data. One of the hallmarks of the actor was the high degree of operational security which involved file and log erasure. Another hallmark was measures designed to defeat forensic analysis and hide activities. Because of this the forensics available (and subsequent analysis) is incomplete. However, there is enough detail available to provide insight into the actor's activities. Broadly speaking, there are three categories of activities undertaken by the actor during the campaign:

> **Credential theft.** The actor sent out four spearphishing emails, to ANU users,to try and gain credentials ie passwords, usernames, hashes.[6] The aim of these emails was to gain the credentials of an administrator or someone with the right level of access to targeted systems. Actors also try to gain a broad set of credentials in case they expire, or compromised accounts are exposed. In the case of ANU, administrator credentials deliberately expire quickly. The other mechanism the actor used was software designed to "sniff" credentials from network traffic.

> **Compromised infrastructure.** The actor built a shadow ecosystem of compromised ANU machines, tools and network connections to carry out their activities undetected. Some compromised machines provide a foothold into the network. Others, like the so-called attack stations, provided the actor with a base of operations to map the network, identify targets of interest, run tools and compromise other machines.[7]

> **Data theft.** The actor used a variety of methods to extract stolen data or credentials from the ANU network. This was either via email or through other compromised Internet-facing machines.

Credential Access - Credential Dumping (T1003)

Initial Access - Spearphishing Link (T1192)

Initial Access - Drive-by Compromise (T1189)

Execution - Exploitation for Client Execution (T1203)

Credential Access - Forced Authentication (T1187)

9 November 2018: spearphishing email one.

The actor's campaign started with a spearphishing email sent to the mailbox of a senior member of staff. Based on available logs this email was only previewed but the malicious code contained in the email did not require the recipient to click on any link nor download and open an attachment. This "interaction-less" attack resulted in the senior staff member's credentials being sent to several external web addresses. It is highly likely that the credentials taken from this account were used to gain access to other systems. The actor also gained access to the senior staff member's calendar – information which was used to conduct additional spearphishing attacks later in the actor's campaign.

Collection - Data from Information Repositories (T1213)

Privilege Escalation - Valid Accounts (T1078)

12–14 November 2018: webserver infrastructure compromised.

It is probable that the actor used credentials gained on 9 November to successfully access an Internet-facing webserver used by one of the University's schools. The actor successfully created a webshell on this webserver which was then used, over two days, to conduct command and control (C2) operations through what is known as a TOR exit node.[8,9] These activities were likely designed to set up infrastructure and tools to be used throughout the actor's campaign.

Persistence - Web Shell (T1100)

Command and Control - Multi-hop Proxy (T1188)

6 Hashes are a one-way mathematically altered version of a password designed to ensure the confidentiality of credentials.
7 All ANU machines compromised by the actor have been cleansed of any malicious code.
8 A web shell is a script that is loaded onto a web server to enable remote access and administration that machine and be used to access other machines on the network.
9 This refers to The Onion Router (TOR) network designed to anonymise internet traffic. Command and Control and or C2 refers to the commands sent via the webshell to control the compromised machine.

Privilege Escalation - Exploitation for Privilege Escalation (T1068)

Privilege Escalation - Valid Accounts (T1078)

16 November 2018: compromise of legacy infrastructure.

From the compromised school webserver, the actor was able to gain access to a legacy server hosting trial software. This server was scheduled for decommissioning in late 2019 and at the time of this report no longer active. Unfortunately, the server was attached to a virtual LAN with extensive access across the ANU network. It is unclear how the actor found this legacy server, but we believe that the credentials stolen on 9 November were used to log on to this machine. The senior user whose credentials were stolen was not a system administrator, so it is likely that a privilege escalation exploit was used to gain full control of the server – referred to as *attack station one* in the remainder of this report.[10]

Persistence - Web Shell (T1100)

Execution - Windows Remote Management (T1028)

Command and Control - Remote File Copy (T1105)

Defense Evasion - File Deletion (T1107)

20–21 November 2018: the creation of attack station one.

Over the course of two days the actor downloaded tools and scripts to build *attack station one*. To download these tools the actor also compromised a second Internet facing webserver using a webshell and used this server to download software tools to *attack station one*. These tools were used to run scripts and perform remote management tasks including scheduled deletion of logs to hide their activities. The actor started to map the ANU network on 21 November.

Discovery - System Network Connections Discovery (T1049)

Persistence - Scheduled Task (T1053)

Command and Control - Remote File Copy (T1105)

22 November 2018: the creation of virtual machines on attack station one.

Credential Access - Network Sniffing (T1040)

The following day the actor set up two virtual machines on *attack station one*, one using Windows XP and the second Kali Linux. Both operating systems were download using BitTorrent. Shortly after the creation of these virtual machines the actor used a network session logger to "sniff" credentials from monitored or redirected network traffic. The actor also gained access (through remote desktop) to a machine in a school which had a publicly routable IP address. Age and permissiveness of the machine and its operating system are the likely reasons the actor compromised this machine – which will be referred to as *school machine one* for the remainder of this report. The actor continued to map the ANU network on this day.

Lateral Movement - Remote Desktop Protocol (T1076)

Discovery - System Network Connections Discovery (T1049)

23 November 2018: exfiltration of network mapping data.

Exfiltration - Exfiltration Over Alternative Protocol (T1048)

The actor connected to a legacy mail server and sent three emails to external email addresses. Unlike the University's primary mail server, this legacy mail server requires no authentication. The emails sent out likely held data gained from the actor's network mapping from the previous two days, as well as user and machine data. On the same day, the actor set up what is known as a tunnelling proxy which is typically used for C2 and taking data out of the network. The actor commenced network packet captures, most likely to collect more credentials or gain more knowledge about the network.

Command and Control - Connection Proxy (T1090)

Collection - Data from Local System (T1005)

Credential Access - Network Sniffing (T1040)

25–26 of November: spearphishing email two.

The actor started a second attempt to gain credentials using spearphishing emails. This email entitled "invitation" was sent to one external and 10 ANU email addresses.[11] Some of these emails appear to be tests to determine if the ANU mail filters would block the actor's spearphishing emails. This spearphishing attempt resulted in only one user's credentials being compromised but usage of this credential was limited, suggesting it did not have the accesses the actor was seeking. The actor also accessed the network's Lightweight Directory Access Protocol (LDAP) infrastructure, gaining information on the ANU pool of Windows users and devices.[12]

Initial Access - Spearphishing Attachment (T1193)

Execution - User Execution (T1204)

Collection - Data from Information Repositories (T1213)

10 A privilege escalation exploit is malicious code which uses a flaw or bug in software or the operating system to gain administrative access to a machine.

11 A copy of this email is available in Appendix A.

12 Lightweight Directory Access Protocol

Credential Access - Exploitation for Credential Access (T1212)

Privilege Escalation - Valid Accounts (T1078)

27 November: access to ESD file shares achieved.

At this stage the actor did not appear to have the relevant credentials needed for their campaign and over the course of 27 November, began a network-wide attempt to compromise a range of servers using exploits or stolen credentials. The actor eventually found credentials to access file shares in ESD and other parts of the network; and mapping directory structures. However the actor displays no interest in file shares other than those in ESD. The file share in ESD is a temporary storage location used by several business units, normally to facilitate the routine extraction and manipulation of data such as finance and HR records.

Discovery - System Network Connections Discovery (T1049)

The actor also starts to map out machines in ESD and locates servers housing the databases underpinning ANU HR, finance, student administration and e-forms systems. Upon finding these databases the actor tries repeatedly, and unsuccessfully, to access these systems. Late on 27 November the actor downloads source code for a bespoke toolset or malware; this code is then compiled and run. The nature of this code is unknown as the actor wiped it and the compiled executable after use. Executable files allow source code to run on a machine. Forensic evidence also shows the extensive use of password cracking tools at this stage. The combination of the bespoke code and password cracking is very likely to have been the mechanism for gaining access to the above administrative databases or their host systems.

Command and Control - Remote File Copy (T1105)

Defense Evasion - Indicator Removal on Host (T1070)

Credential Access - Brute Force (T1110)

The actor then accessed the administrative databases directly using a commercial tool. This tool allowed the actor to connect to several databases at once to search and extract records; and convert them to PDF format. The PDFs were then sent to the compromised *school machine one* for extraction from the ANU network.[13]

Collection - Data from Information Repositories (T1213)

Initial Access - Spearphishing Attachment (T1193)

Execution - User Execution (T1204)

29 November 2018: third spearphishing attempt.

The actor continues to look for credentials and tries to maximise the effectiveness of their spearphishing efforts by connecting to the University's spam filer and attempting to disable its ability to detect malicious emails. There is no forensic evidence to suggest that they were successful in this attempt. The actor then sent 75 emails, 50 to ANU addresses and the remainder to external email addresses. These were used to either exfiltrate data or to undertake more spearphishing. The actor was able to harvest at least one administrator credential during this spearphishing phase.

29 November–13 December 2018: clean-up operations and loss of attack station one.

As noted earlier, the actor displayed a very high degree of operational security and routinely erased files and logs. One such clean up phase commenced on 29 November with the actor erasing files and tools with logs packaged for exfiltration through *school machine one*, which itself was also subject to clean up operations. It is believed that the actor was preparing *attack station one* for the next phase of their campaign.

Defense Evasion - File Deletion (T1107)

On 30 November the ANU implemented a routine firewall change. This cut the actor off from *attack station one*. The actor immediately then initiated activity to try and get back on to attack station one or to find another place in the network to resume operations. This activity continued until 13 December.

Exfiltration - Exfiltration Over Alternative Protocol (T1048)

13 This machine was not used directly for research purposes and there is no indication that any local data was taken from this machine.

13–20 December 2018: new attack station and resumption of exfiltration.

After nearly two weeks of effort the actor restores their access to the network through a machine running a legacy operating system in a second school – referred to in the remainder of the report as *attack station two*. This machine was subject to a large amount of C2 activity between 13 and 19 December. Forensic analysis suggests this activity is associated with the actor preparing *attack station two* presumably to either continue extracting data from ESD or to start a new phase of the campaign. On 19 December, the actor exfiltrated 13 additional files, compressed into archives, through TOR.

Exfiltration - Data Compressed (T1002)

Command and Control - Multi-hop Proxy (T1188)

At the time of this activity, the school hosting *attack station two* was not behind the University firewalls and was using publicly routable IP addresses. The actor also probed other parts of the network for other vulnerable systems and began updating malware on *attack station two*. These updates were likely preparing attack station two for continued access into ESD or the rest of the network.

Defense Evasion - Indicator Removal from Tools (T1066)

Initial Access - Spearphishing Attachment (T1193) Execution - User Execution (T1204)

21 December 2018: fourth spearphishing attempt and loss of attack station two.

The actor starts to target users with administrative access and sends 40 phishing emails to ANU staff with privileged accounts. This email, entitled "New Planning for Information Technology Services" used calendar information gained from the first spearphishing campaign.[14] This phishing attempt was successful in harvesting a handful of privileged accounts, but ANU IT staff detected the unusual behaviour and were able to remove the new attack station from the network. At the time, however, this activity was treated as an individual event, by ANU IT, rather than part of a broader campaign.

Collection - Data from Information Repositories (T1213)

Prior to the loss of *attack station two* the actor was able to scan an Internet facing web server. This formed the basis of a subsequent intrusion attempt in February 2019.

Discovery - Network Service Scanning (T1046)

22 December 2018 – March 2019: C2 activity and second intrusion attempt.

As noted above there was an intrusion attempt in February 2019 against an externally facing webserver. This attack was ultimately unsuccessful but given the similarities in tradecraft used between the November and February attacks, the latter was likely a further attempt by the same actor to regain access to ESD. This activity also aligns to C2 activity seen throughout January and in early March, which was the last known activity by the actor.

14 A copy of this email is available in Appendix C.

Key

The Onion Router (TOR) connection

BitTorrent

Figure 1: Simplified overview of actor campaign

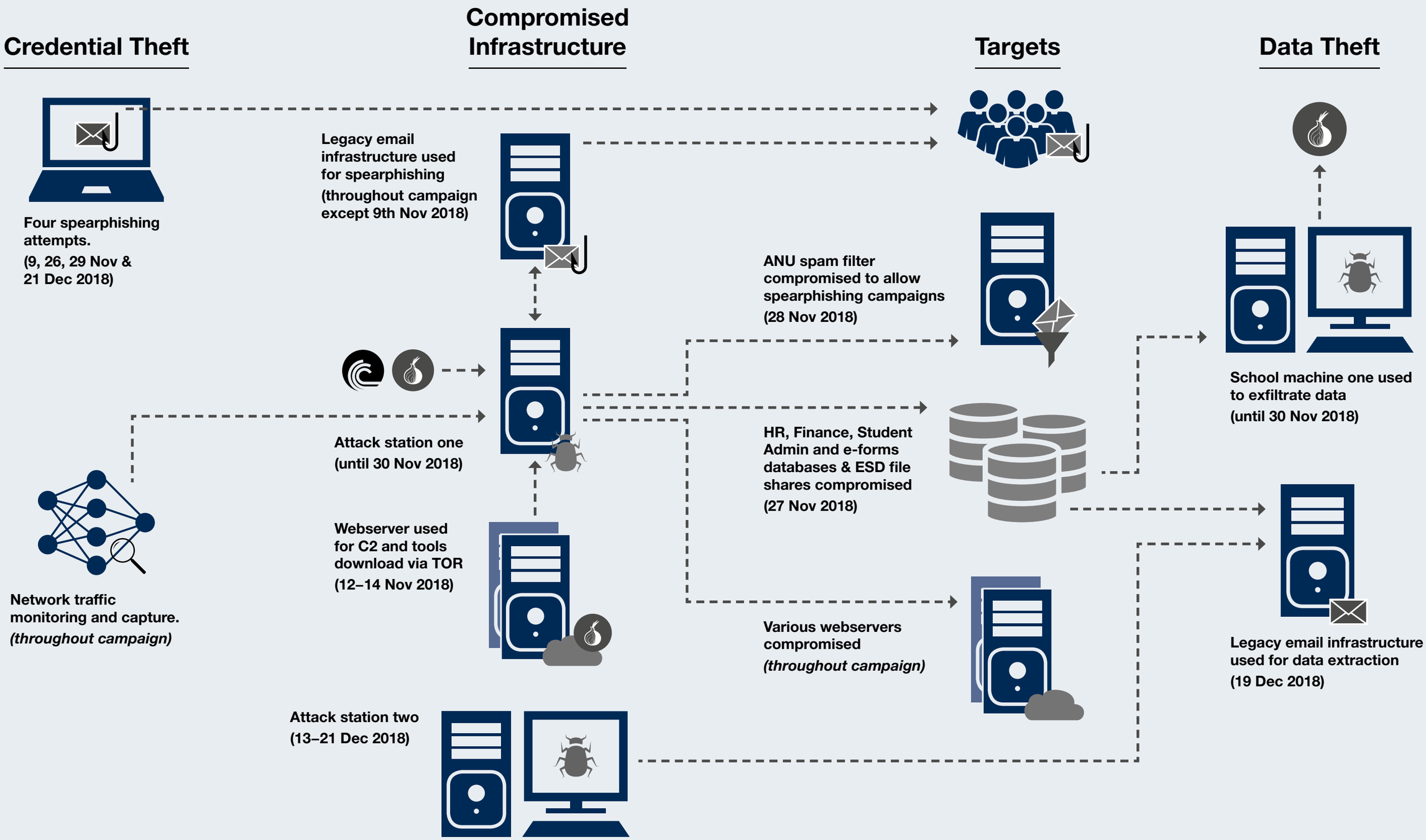
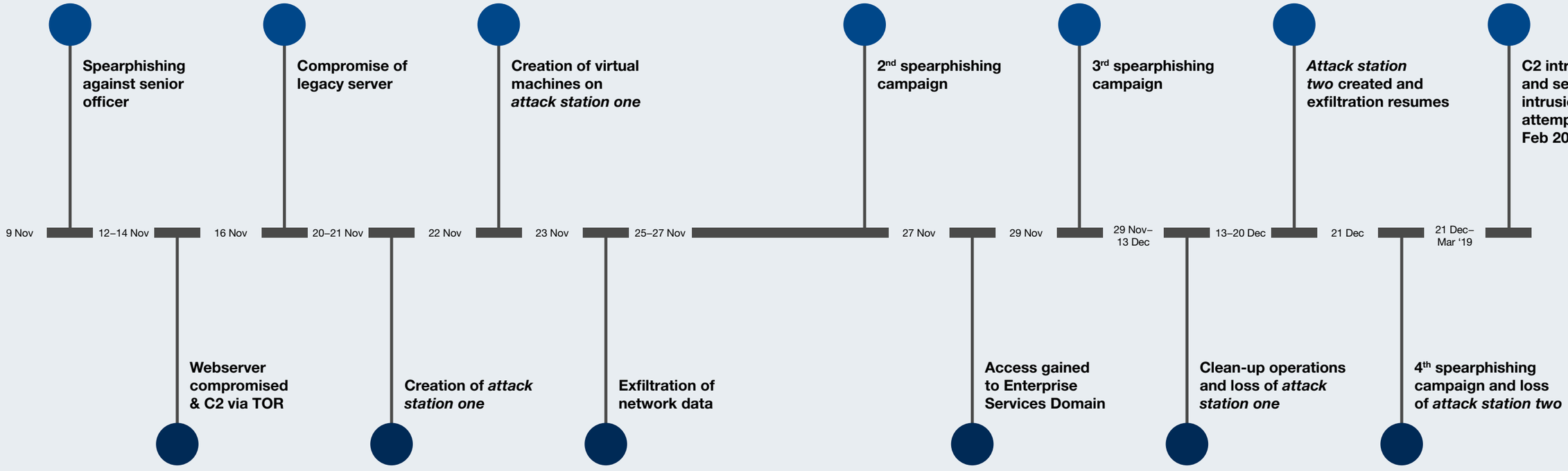


Figure 2: Attack timeline



POST NOTIFICATION EVENTS

In the intervening two weeks between the detection of the breach and the public notification, ANU detected repeated attempts to gain or possibly regain access to ESD. Investigations into the nature of these attempts, which were blocked, are still ongoing at the time of this report. Within an hour of the Vice-Chancellor's notice informing the ANU community and public of the data breach on 4 June, the ANU network was subject to a botnet attack. This attack was also successfully stopped by ANU.[15] By way of comparison the ANU blocks multiple intrusion attempts on a daily basis.

On the night of the 5 June 2019, ANU detected a probable attack against its spam filter and mail gateway. This attack was not successful, however, given the spam filter was a target during the November 2018 intrusion there is a strong possibility this was the second attempt by the actor to gain access to the filter potentially in preparation for another cycle of phishing emails.

15 Botnet is a combination of the words robot and network. It refers to a logical grouping (or network) of compromised machines (known as bots), each running malware designed to control it and working in concert to undertake a malicious mission.

MALWARE AND TRADECRAFT ANALYSIS

The actor exhibited exceptional operational security during the campaign and left very little in the way of forensic evidence. Logs, disk and file wipes were a recurrent feature of the campaign. The exception was *attack station one* which the actor lost control of on 30 November. At this point, the actor was part way through its clean-up cycle and as such was not able to fully erase all traces. It is the forensic analysis of these traces that form much of the content of this report. Analysis of *attack station one* is still underway at the time of this report.

The analysis of *attack station one* yielded several insights. The actor was able to, in several cases, avoid detection by altering the signatures of more common malware used during the campaign. Also, the malware and some tools were assembled inside the ANU network after a foothold had been established. This meant that the downloaded individual components did not trigger the University's endpoint protection. There is also evidence of bespoke malware in the form of source code (compiled within the network) used to gain access to ESD. The purpose of this code remains unknown, and no forensic traces of it or the executable file which was compiled from the code have been found at the time of this report.

Execution - PowerShell (T1086)

Other software used by the actor included network session capture and mapping tools, bespoke clean-up, JavaScript and PowerShell scripts as well as a proxy tool. The actor downloaded several types of virtualisation software before selecting one and downloaded disk images for Windows XP and Kali Linux. There is little evidence to suggest much use of Kali Linux.

The first phishing email was designed to be interaction-less and likely used some form of scripting. It is assumed the actor anticipated a high degree of security awareness on the part of the intended recipient. Unfortunately, a copy of this email was not recoverable, so further analysis is not possible.

Execution - Scripting (T1064)

Subsequent phishing attachments were designed to harvest credentials and used similar scripts. The user opened the attached Word document and the credentials were sent to the remote server. All the attachments in the second, third and fourth spear-phishing cycles used the same technique with the credentials sent to the active attack station instead of the internet.

Due to the operational security and clean-up operations of the actor, it has not been possible to retrieve copies of the files exfiltrated from the network. In some cases, there was enough forensic and log data to ascertain file sizes. However, because these files were compressed and likely to have been encrypted, it is difficult to infer what specific data sets was taken from the affected systems. However, based on log analysis and known data volumes it is highly likely that the actor took much less than the 19 years' worth of data first noted at the time of the breach announcement.

The actor's use of a third-party tool to extract data directly from the underlying databases of our administrative systems effectively bypassed application-level logging. Safeguards against this happening again have been implemented.

Analysis of *school machine one*, through which most of the data was taken, is ongoing. However, this machine has been subject to a range of erasure and clean-up techniques, so it is not possible to identify precisely what data was taken at the time of writing.

Exfiltration - Data Encrypted (T1022)

LESSONS FROM THE ATTACK AND FOLLOW-UP ACTIONS

While, and in part because, the actor was operationally sophisticated and deliberate in their targeting, there are several lessons for the University that have arisen from the data breach and have formed the basis of a range of remediation and hardening measures. Below, personally identifiable information and phishing awareness are called out for special attention, and the remainder are captured in Table One.

Personally identifiable information

The most critical issue arising from the breach has been the protection of affected members of our community and dealing with any repercussions due to the loss of personally identifiable information (PII). As an initial step, ANU provided assistance in this matter through services offered by IDCARE. In addition, enquiries relating to individual PII queries are being handled by the ANU Chief Privacy Officer.

As noted above it is not possible to ascertain with accuracy what data was taken other than through the lens of the systems which were breached. It was assumed, in the absence of any specific knowledge, at the time of the public announcement that any data contained in affected systems might be in the scope of the disclosure. ANU has proceeded with its security efforts on that basis.

ANU has already instigated data safeguarding measures designed to minimise security risks associated with PII data kept in its administrative systems. That said the University acknowledges there is still work to be undertaken in order to further reduce the risk to the information held in these systems; and in a manner, which allows us to remain compliant with relevant legislation. To this end, a working group, chaired by the Chief Privacy Officer has begun a full review and will develop and guide of additional remediation measures.

Before the detection of the breach, as part of its planned mitigation measures, ANU was searching for stolen data or credentials that might be traded or transmitted online. At the time of this report, no such activity has been detected. ANU continues to work with specialist services to look for any relevant data or credentials. Should these be identified, ANU will take appropriate remedial steps including the prompt notification of any affected parties.

Phishing awareness

As noted throughout the timeline, phishing emails were a hallmark of the activities of the actor. The social engineering which underpinned these emails highlights the vigilance needed to protect users against this form of attack.[16] Given the methods of the actor and the number of successfully phished users, it is clear to us that more effort is required to help drive awareness and safe user behaviours across the University community. ANU will focus significantly in this area as part of a broader investment in security culture efforts under the auspices of its forthcoming strategic information security strategy. Work has already commenced with awareness training for high-risk groups.

In addition to security culture, we have invested in stronger safeguards for our mail gateway and are expediting the retirement of legacy mail systems. These measures have already resulted in better technical protection for our mail users, and further investment will follow under the strategic program.

16 Social engineering is a form of deception used by threat actors to trick users into handing over credentials or other data to gain unauthorised access to systems. It can involve using information about the user or their organisation in a carefully crafted manner to successfully trick the user.

Issue	Recommendation	Status
Phishing awareness	The requirement for increased phishing awareness across campus.	In progress starting with high-risk user groups and expanding throughout 2019 and 2020. Eventual coverage will be all staff and students.
Legacy devices	Incomplete identification of legacy and at-risk devices on the ANU network.	Discovery and remediation activities have commenced in high-risk areas of the network including the hardening of devices and their access to the network. This will be expanded significantly under the strategic information security program over 2019 and 2020.
ESD data protection	Information held in ESD represents a significant a risk to ANU and its community. Reducing the risk to the irreducible minimum and additional protective controls are essential.	Initial data protection measures have been deployed and a working group established to develop a risk management strategy in-line with legislative requirements. Implementation will occur under the strategic information security program.
Legacy email	Continued use of legacy email systems represents a significant risk to network security; and the primary mail gateway protection system requires a security review and potentially further hardening.	Work has commenced on identifying residual legacy email solutions and affected users. The ANU primary mail server has been significantly hardened and will gain further investment under the strategic information security program over the course of 2019 and 2020.
Two-factor authentication	Two-factor authentication rollout needs to be accelerated and legacy authentication removed across all systems.	Two-factor authentication has already been rolled out to administrative users and high-risk systems. The scope and speed of deployment will be expanded and accelerated throughout 2019 and 2020.
Firewall coverage	Firewall coverage needs to be reviewed and re-validated for all parts of the network.	Work has commenced on reviewing firewall coverage with industry assistance.
Network hardening	Network segmentation, zoning and other network hardening measures need to be expedited including the review and phasing out of publicly routable addresses.	A range of network hardening measures has been undertaken including segmentation of ESD. Future work is being planned at the time of this report and will form the basis of further uplift and network modernisation under the strategic information security program.
Vulnerability and patch management	Vulnerability and patch management initiatives need to be expedited.	Deployment of these systems commenced under the tactical cyber program following the May 2018 intrusion. The scope of this initiative has been expanded and will continue under the strategic information security program.
Simulation exercises	ANU responded quickly to the breach but ongoing practice and simulation exercises are vital.	The first exercise is scheduled under the strategic security program in 2020.

Table One: Issues and Remediation

APPENDIX

Appendix A: “invitation” phishing email

Invitation

From: office@anu.edu.au
To: [redacted]
Sent: November 26, 2018 7:28:50 PM AEDT
Received: November 26, 2018 7:18:38 PM AEDT
Attachments: Explanatory.zip

[redacted]

We would like to seek your assistance and support please to meet with a Team from Forum Secretariat at a time convenient to you (between 10:30am - 3:00pm on Wednesday 28th November, 2018),on an exercise they are conducting to consolidate some common issues in the region.Please indicate your availability so we ensure it does not clash with our other clients.

An explanatory note is also attached for ease of reference on the contents how the was developed.

Conference Office

Australian National University

This email contains information which is confidential and may be subject to legal privilege. If you are not the intended recipient, you may not peruse, use, disseminate, distribute or copy this email or attachments. If you received this in error, please notify the sender immediately by return email, facsimile or telephone (call collect) and delete this email. Thank you.

Appendix B: “meeting” phishing email

Request for meeting to discuss project

From: [redacted]
To: [redacted]
Sent: November 29, 2018 5:46:57 AM AEDT
Received: November 29, 2018 5:36:44 AM AEDT
Attachments: [redacted]Project.doc

Dear Colleagues,

I am [redacted], and I am a student in the Vice-Chancellor's Student Leadership Program. I am currently working on a project which would require your help as a mentor.

May I know which day and time would be good for a meet up to discuss the project?

Please find attached the project proposal.

Thank you.

Best Regards,

[redacted]

I am a member of the ANU ALLY network

CRICOS Provider #00180C

Appendix C: “planning” phishing email

New planning for Information Technology Services

From: [redacted]
To: [redacted]
Sent: December 21, 2018 2:48:56 PM AEDT
Received: December 21, 2018 2:48:42 PM AEDT
Attachments: New-Planning.doc

Dear members,

Well the year has got away from us and due to a number of factors we have not been able to organise one last meeting for the year. So I wanted to touch base with you all and say well done on making it to the end of year, merry Xmas, happy holidays and happy new year!

Next year the plan is to have four meetings - Meeting plan refer to Annex.

Kind regards

[redacted]

[redacted]

The Australian National University Canberra, ACT, 0200, Australia

CONTACT US

Office of the Chief Information Security Officer

E CISO@anu.edu.au

CRICOS Provider #00120C

MO_SCAPA190209