Stuti Parmar
218516625
EECS 3482, M
6th Feb 2024

**Title: A Major Data Breach at the Australian National University (ANU)**

A major data breach at the Australian National University (ANU) resulted in the discovery of illegal access to personal information going back 19 years [1]. The affected population was estimated to be 200,000, which included visitors, staff, and students. Names, addresses, birth dates, phone numbers, tax file numbers, and other information were compromised [1]. Credit card information, medical records, and research projects, however, appeared to be unharmed. Experts believed a sophisticated actor, potentially connected to China, and the Australian Signals Directorate is looking into it [1]. The actor attempted to get login credentials, such as hashes, passwords, and usernames, by sending four spear phishing emails to ANU users [1]. The purpose of these emails was to obtain an administrator's credentials or the credentials of someone with appropriate access to the systems that were being targeted. The other mechanism the actor used was software designed to “sniff” credentials from network traffic. “Sniffing” refers to the monitoring of internet traffic in real time. Packet sniffers are programs or hardware devices that can spy on you and all your internet activity [3].

The cyberattack on Australian National University (ANU) unfolded over several stages, starting on November 9th, 2018, with a spear phishing email sent to a senior staff member [4]. This email contained malicious code that did not require any action from the recipient to initiate the attack. As a result, the attacker obtained the senior staff member's credentials, which were then used to access multiple external web domains. By November 16th, 2018, the attacker had compromised ANU's web server infrastructure and legacy systems, creating what is referred to as "attack stations" to conduct further malicious activities [4]. Cleanup efforts by ANU's IT staff began on November 29th, 2018, and lasted until December 20th, 2018, during which attack stations were removed, and abnormal behavior was detected and addressed [4]. Despite these efforts, further attempts to access external servers were made in February 2019, indicating ongoing security threats and challenges faced by ANU [4]. ANU saw multiple attempts to access ESD (Electronic Software Delivery), probably by the same person, between finding the breach

and notifying the public. These attempts were blocked during ongoing investigations. A botnet attack was effectively stopped on ANU's network shortly after the community was informed of the vulnerability. Botnet attacks uses a command-and-control model to allow one or more hackers to drive the actions of those devices from a remote location [5]. ANU regularly blocked multiple intrusion attempts daily. On 5th June 2019, a possible assault on the mail gateway and spam filter of ANU was discovered [4]. Even though this attempt was unsuccessful, the November 2018 intrusion hints that there may be a second effort by the actor to access the filter for potential phishing email activities.

Analyzing the malware and tradecraft, the campaign's attacker left little forensic trace and kept excellent operational security. Analysis of attack station one, which was partially removed after a cleaning cycle, demonstrated the actor's capacity to change malware signatures to evade detection [4]. Unknown in intent, the source code for bespoke malware was discovered and utilized to get access to ESD. Bespoke malware is highly targeted and custom-designed malicious software that has been modified to evade traditional detection systems [6]. Several tools were used by the actor, such as a proxy tool, network capture, cleaning, JavaScript, and PowerShell scripts [4]. Phishing emails were script-driven or lacked interactivity, and attachments meant to obtain credentials were forwarded to the attack station in real time. The actor's security precautions left recoverable files and their contents mostly unclear. The details are difficult to determine, although log analysis indicates that less data was gathered than first thought.

The data breach taught ANU important lessons, leading to actions for improvement. The breach emphasized the need to protect community members' personal information. ANU helped through IDCARE and handled individual PII (Personal Identifiable Information) queries through the Chief Privacy Officer [4]. Despite uncertainties about the data taken, ANU implemented safeguards and continues efforts to minimize security risks. A working group is reviewing and developing additional measures for compliance with relevant legislation. Phishing emails were a significant aspect of the breach, emphasizing the importance of user vigilance. ANU recognizes the need for increased efforts in driving awareness and safe user behaviors. Focus on security culture is part of the strategic information security strategy, with ongoing awareness training and investment in mail gateway safeguards [4]. Retirement of legacy mail systems is expedited to enhance technical protection for mail users. The Australian National University (ANU) spent millions modernizing its computer network to improve security following a serious cyberattack

[4]. Professor Brian Schmidt, the vice chancellor of ANU, expressed the hope that other institutions and individuals will take cybersecurity seriously after learning from the university's experience [4]. A task force on university foreign involvement received the incident report to strengthen defenses against such assaults. The Vice-Chancellor apologizes to the community, thanks everyone who contributed to the reaction, and assures them that efforts will continue to safeguard confidential information [4].

Therefore, we can conclude that no computer network is completely safe, even with updates as noted by The Australian Cyber Security Centre [7]. People and organizations are always advised to stay alert and take appropriate precautions against the ever-growing threat of cyberattacks. By being more transparent about these kinds of events, we can create a body of knowledge and best practices that will increase our sense of safety when using the internet and our ability to trust the organizations that store our information. “Unfortunately, a malicious actor with sufficient capability, time and resources will almost always be able to compromise an internet-connected computer network” as stated by The Guardian [8].

## References


[1] N. Challis, "abc news," 3 june 2019. [Online]. Available: https://www.abc.net.au/news/2019-06-04/anu-data-hack-bank-records-personal-information/11176788. [Accessed 7 February 2024].

[2] N. Challis, "abc news," 3 June 2019. [Online]. Available: https://www.abc.net.au/news/2019-06-04/anu-data-hack-bank-records-personal-information/11176788. [Accessed 7 February 2024].

[3] N. Latto, "avg," 11 November 2022. [Online]. Available: https://www.avg.com/en/signal/what-is-sniffer#:~:text=“Sniffing”%20refers%20to%20the%20monitoring,nearly%20all%20your%20online%20activity.. [Accessed 7 February 2024].

[4] "INCIDENT REPORT ON THE BREACH OF THE AUSTRALIAN NATIONAL UNIVERSITY’S ADMINISTRATIVE SYSTEMS," AUSTRALIAN NATIONAL

UNIVERSITY, [Online]. Available: https://imagedepot.anu.edu.au/scapa/Website/SCAPA190209_Public_report_web_2.pdf. [Accessed 7 February 2024].

[5] "PingIdentity," [Online]. Available: https://www.pingidentity.com/en/resources/cybersecurity-fundamentals/threats/botnet-attack.html#:~:text=Botnet%20attacks%20use%20a%20command,attack%20is%20likely%20to%20be.. [Accessed 7 February 2024].

[6] M. Marvin, "Portnox," 30 June 2022. [Online]. Available: https://www.portnox.com/blog/network-security/could-bespoke-malware-target-your-organization/. [Accessed 7 February 2024].

[7] S. Borys, "abc news," 2 October 2019. [Online]. Available: https://www.abc.net.au/news/2019-10-02/the-sophisticated-anu-hack-that-compromised-private-details/11566540. [Accessed 7 February 2024].

[8] M. McGowan, "The Guardian," 6 June 2019. [Online]. Available: https://www.theguardian.com/australia-news/2019/jun/06/china-behind-massive-australian-national-university-hack-intelligence-officials-say. [Accessed 7 February 2024].

[9] "INCIDENT REPORT ON THE BREACH OF THE AUSTRALIAN NATIONAL UNIVERSITY'S ADMINISTRATIVE SYSTEMS," AUSTRALIAN NATIONAL UNIVERSITY, [Online]. Available: https://imagedepot.anu.edu.au/scapa/Website/SCAPA190209_Public_report_web_2.pdf.

[10] "PingIdentity," [Online]. Available: https://www.pingidentity.com/en/resources/cybersecurity-fundamentals/threats/botnet-attack.html#:~:text=Botnet%20attacks%20use%20a%20command,attack%20is%20likely%20to%20be..

## QUESTIONS:

1. **Was this incident a hack or a data breach? Justify your answer!**

- The incident at ANU is appropriately characterized as both a hack (unauthorized access) and a data breach (compromised personal information), considering the multifaceted nature of the security compromise.
- The incident involved unauthorized access to the Australian National University's (ANU) computer systems by the attackers. The hackers used sophisticated techniques to enter ANU's systems, which aligns with the definition of a hack.
- The attackers successfully accessed and exfiltrated sensitive personal information of staff and students spanning 19 years. Personal details, including names, addresses, phone numbers, dates of birth, emergency contact details, tax file numbers, payroll data, bank account details, and student records, were compromised. The unauthorized extraction and exposure of this personal data constitute a data breach, involving the compromise of confidentiality.
- The incident is a combination of a hack (unauthorized access) and a data breach (compromised personal information). The unauthorized access facilitated the data breach, where the attackers focused on extracting specific types of information.

2. **Who are the main 'stakeholders' in this incident (who is the adversary & who is the victim)? Note: In cases when there are multiple adversaries and/or victims, they all should be clearly enlisted**
    - Main stakeholders:
        - Adversary: The attackers who executed the cyber-attack.
        - Victim: Australian National University (ANU) and the individuals whose personal information was compromised.

3. **When did the incident happen? When was it discovered?**
    - Timeline of the Incident:

    1) Initiation of the Incident:

    The cyber-attack on the Australian National University (ANU) began in November 9th 2018.

    2) Undetected Access:

    The attackers executed a sophisticated cyber-attack that did not require any user interaction.

    The unauthorized access remained undetected for an extended period, emphasizing the stealthy nature of the intrusion.

    3) Duration of Undetected Access:

    The attackers had undisturbed access to ANU systems for approximately six months, highlighting the prolonged period during which they operated within the network without detection.

    4) Discovery of the Breach:

    The breach was discovered in April 2019, indicating that ANU detected the unauthorized activity after months of covert access by the attackers.

    5) Public Disclosure:

    ANU publicly disclosed the cyber-attack on an unspecified date following the discovery of the breach.

    6) Report Release:

The detailed report on the incident, providing insights into the attack's nature and the university's response, was released after the breach discovery.

7) Ongoing Investigations:

Investigations into the incident, including forensic analysis and efforts to understand the full extent of the breach, were likely ongoing at the time of the report release.

8) Uncertain Discovery Date:

The exact date of the breach discovery within the month of April is not specified in the provided information.

9) Importance of the Timeline:

Understanding the timeline is crucial for assessing the effectiveness of ANU's security measures, determining the duration of the security lapse, and evaluating the speed of response after the breach discovery.

In summary, the cyber-attack on ANU initiated in November 2018, remained undetected for approximately six months, and was discovered in April 2019, leading to subsequent public disclosure and the release of a detailed incident report.

4. **Which vulnerability in the target system was exploited by the adversary during the incident?**
   - The detailed report on the Australian National University (ANU) cyber-attack does not explicitly specify the exact nature of the vulnerability exploited by the adversaries. The report does not provide explicit information about the specific vulnerability exploited during the cyber-attack on ANU. The identification and understanding of the exploited vulnerability play a pivotal role in developing effective cybersecurity strategies and preventing similar incidents in the future.

5. **How, exactly, did the adversary exploit the vulnerability? What was the main attack vector? Note: For a list of attack vectors see: https://www.strongdm.com/blog/attack-vector**
   - The main attack vector involved a targeted email sent to a senior staff member, leading to credential theft and unauthorized access. The attackers used three main avenues: credential theft, infrastructure compromise, and data theft.
   - It was also a phishing attack as the hacker pretended to be a trusted entity to get users to release information.

6. **What did this breach/hack target in terms of CIA?**
   - The breach resulted in a substantial compromise of confidentiality, with potential implications for integrity. While availability wasn't a primary focus, the prolonged unauthorized access could pose future risks to the availability of ANU's systems.
   - The attackers primarily targeted the confidentiality of sensitive information. Personal details of staff and students spanning 19 years, including names, addresses, phone numbers, dates of birth, emergency contact details, tax file numbers, payroll data, bank account details, and student records, were compromised. The confidentiality breach included a wide range of personal and financial data.

- While the report doesn't explicitly state an integrity compromise, the attackers potentially had the capability to alter or manipulate data within the compromised systems. An integrity compromise could have serious implications for the accuracy and reliability of academic records, payroll information, and other critical data stored by ANU.
- ANU and other institutions can learn from this incident by reinforcing measures to safeguard confidentiality, ensuring the integrity of critical data, and implementing robust cybersecurity practices to maintain the availability of their systems.

7. **What has been the actual loss suffered by the victim due to the incident (monetary, functional, reputational, …)? Note: In most cases the victim suffers a combination of different types of loss, and they all should be enlisted. Also, if there are multiple victims, the losses of each victim should be specified.**
    - Actual losses suffered by the victim:
        - Monetary: Costs associated with upgrading the computer network.
        - Functional: Disruption in normal operations, potential impact on research work.
        - Reputational: Damage to ANU's reputation due to the data breach.

8. **How did/can the victim ensure that the same type of breach/hack does not happen again?**
    - ANU ensured prevention by investing millions in upgrading its computer network for enhanced security. Regular threat hunting exercises and cybersecurity practices were implemented.
    - ANU helped through IDCARE and handled individual PII (Personal Identifiable Information) queries through the Chief Privacy Officer
    - A working group is reviewing and developing additional measures for compliance with relevant legislation.
    - A task force on university foreign involvement received the incident report to strengthen defenses against such assaults.

9. **Was the adversary prosecuted, and if so, what were the penalties (if known)?**
    - the report does not offer details on legal actions or sanctions against the adversary. The challenge in attributing cyberattacks, especially those involving sophisticated actors, remain a significant aspect of addressing such incidents.
    - Experts believed a sophisticated actor, potentially connected to China, and the Australian Signals Directorate is looking into it.

10. **What can other similar potential victims learn from this incident?**
    - Enhance cybersecurity measures to detect and prevent unauthorized access.
    - Regularly update and upgrade computer networks to address vulnerabilities.
    - Conduct threat hunting exercises to proactively identify and address security threats.

- Emphasize the importance of cybersecurity awareness and practices among staff and users.
- Collaborate with external experts and government agencies to improve overall cybersecurity posture.
- People and organizations are always advised to stay alert and take appropriate precautions against the ever-growing threat of cyberattacks.