Continuous Assessment 2
Security Principles

Table of contents

Contents

Table of contents 2
Abstract 3
Introduction 3
Data Breach Analysis 4
ACSC Threat Life Cycle 5
Initial Foothold 5
Network Reconnaissance 5
Establish Presence 5
Ensure Persistence 5
Execute Intent 6
Criteria for device compromise 6
ANU responsible roles 6
Conclusion 7
Reference 7

Abstract

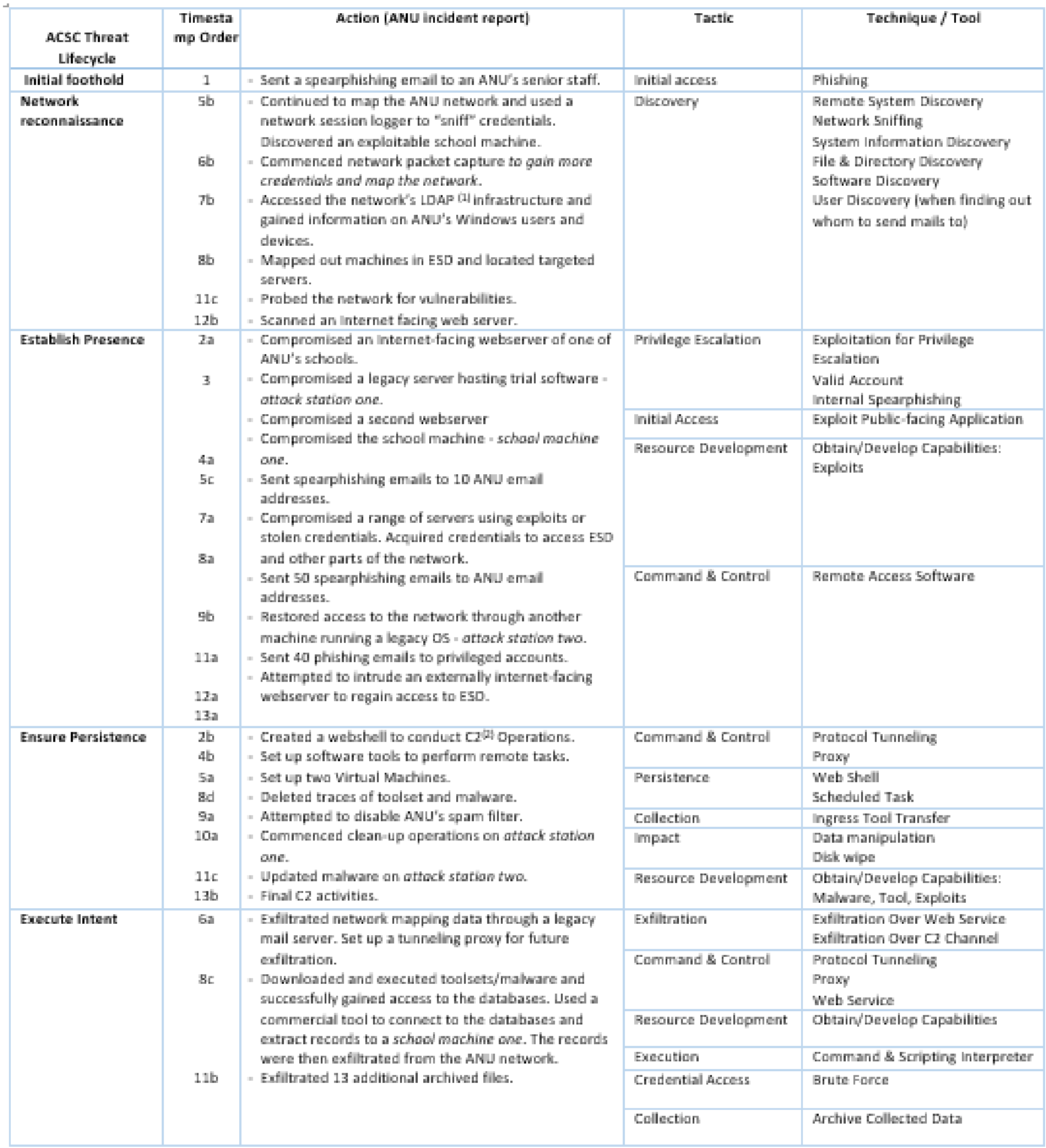
This report summarizes the Australia National University’s data breach incident in 2019 and sorts the actions according to the Australian Cyber Security Centre’s Life Cycle. The report also analyzes the criteria used by the adversary on which devices to attack and discusses the roles in ANU that are responsible for preventing the data breach.

Introduction

On 4th June 2019, Australian National University (ANU)’s Vice-Chancellor announced that the University had been the victims of a cyber-attack (Report). A detailed incident report on the attack was subsequently published on 2th October (ANU 2019b) in which demonstrated an astoundingly high level of sophistication by the perpetrators. This report analyzes into the incident by referring to the Australian using the Australian Cyber Security Centre’s Life Cycle 2016, and discusses which roles the University had to defend against the breach.

Data Breach Analysis

The Timestamp Order column in the table refer to the order of the events as an event might have multiple actions which belong to different stages.



ACSC Threat Lifecycle	Timestamp Order	Action (ANU incident report)	Tactic	Technique / Tool
Initial foothold	1	- Sent a spearphishing email to an ANU's senior staff.	Initial access	Phishing
Network reconnaissance	5b 6b 7b 8b 11c 12b	- Continued to map the ANU network and used a network session logger to "sniff" credentials. Discovered an exploitable school machine. - Commenced network packet capture *to gain more credentials and map the network*. - Accessed the network's LDAP [1] infrastructure and gained information on ANU's Windows users and devices. - Mapped out machines in ESD and located targeted servers. - Probed the network for vulnerabilities. - Scanned an Internet facing web server.	Discovery	Remote System Discovery Network Sniffing System Information Discovery File & Directory Discovery Software Discovery User Discovery (when finding out whom to send mails to)
Establish Presence	2a 3 4a 5c 7a 8a 9b 11a 12a 13a	- Compromised an Internet-facing webserver of one of ANU's schools. - Compromised a legacy server hosting trial software - *attack station one*. - Compromised a second webserver - Compromised the school machine - *school machine one*. - Sent spearphishing emails to 10 ANU email addresses. - Compromised a range of servers using exploits or stolen credentials. Acquired credentials to access ESD and other parts of the network. - Sent 50 spearphishing emails to ANU email addresses. - Restored access to the network through another machine running a legacy OS - *attack station two*. - Sent 40 phishing emails to privileged accounts. - Attempted to intrude an externally internet-facing webserver to regain access to ESD.	Privilege Escalation	Exploitation for Privilege Escalation Valid Account Internal Spearphishing
			Initial Access	Exploit Public-facing Application
			Resource Development	Obtain/Develop Capabilities: Exploits
			Command & Control	Remote Access Software
Ensure Persistence	2b 4b 5a 8d 9a 10a 11c 13b	- Created a webshell to conduct C2[2] Operations. - Set up software tools to perform remote tasks. - Set up two Virtual Machines. - Deleted traces of toolset and malware. - Attempted to disable ANU's spam filter. - Commenced clean-up operations on *attack station one*. - Updated malware on *attack station two*. - Final C2 activities.	Command & Control	Protocol Tunneling Proxy
			Persistence	Web Shell Scheduled Task
			Collection	Ingress Tool Transfer
			Impact	Data manipulation Disk wipe
			Resource Development	Obtain/Develop Capabilities: Malware, Tool, Exploits
Execute Intent	6a 8c 11b	- Exfiltrated network mapping data through a legacy mail server. Set up a tunneling proxy for future exfiltration. - Downloaded and executed toolsets/malware and successfully gained access to the databases. Used a commercial tool to connect to the databases and extract records to a *school machine one*. The records were then exfiltrated from the ANU network. - Exfiltrated 13 additional archived files.	Exfiltration	Exfiltration Over Web Service Exfiltration Over C2 Channel
			Command & Control	Protocol Tunneling Proxy Web Service
			Resource Development	Obtain/Develop Capabilities
			Execution	Command & Scripting Interpreter
			Credential Access	Brute Force
			Collection	Archive Collected Data

[1] Lightweight Directory Access Protocol

[2] Command & Control

ACSC Threat Life Cycle

Initial Foothold

The Initial Foothold stage refers to when an adversary gains his entry into the network. It is often achieved either by stealing credentials from legitimate users through phishing, or by compromising the internet-facing services through vulnerabilities. (ACSC 2016).

In this incident, adversary gained the initial access to the system through a spearphishing email.

Network Reconnaissance

Once the adversary has infiltrated the network, he would typically try to build up knowledge of the compromised network, i.e., identify running services on a compromised machine, search for privileged credentials, or propagate through other linked networks to look for vulnerabilities (ACSC 2016).

Throughout this incident, adversary continuously mapped the ANU network, looked for vulnerabilities and commenced multiple techniques to “sniff” credentials from the network traffic (used of network session logger, network packet capture). (ANU 2019a)

Establish Presence

To gain control of the network, the adversary would attempt to procure legitimate remote administrative access. It is often achieved either by stealing credentials through social engineering techniques, i.e., phishing, or compromising servers using exploits. (ACSC)

In this incident, adversary compromised multiple Internet-facing webserver by using a combination of stolen credentials (Valid Account), system exploits, and social engineering techniques (Internal Spearphishing, Trusted Relationship). (ANU 2019a)

Ensure Persistence

At this stage, the adversary would attempt to ensure ongoing access to the network by installing malware or a web shell. This step aims to hides the adversaries’ activities in the network and leaves a backdoor in case the legitimate access ceases to exist.

Throughout this incident, adversary commenced multiple techniques to maintain his access to the system by creating a backdoor (Webshell), routinely erasing traces in logs and disks (Data Manipulation, Disk Wipe), and using tunneling proxy to hide activities (Tunneling Protocol, Proxy) (ANU 2019a).

Execute Intent

Once persisted access to the system is gained, adversary will execute his intent. This intent could be anything from data exfiltration to preparing an attack station for adversary's real targeted organization (ACSC 2016).

In this incident, it is assumed that adversary data exfiltration in the ANU's Enterprise Systems Domain. (ANU 2019a)

Criteria for device compromise

In this incident, there exists one common criteria between all compromised devices: use of legacy software, hardware or systems. In computing, a legacy technology is an outdated and is no longer supported, yet is still is in use because it is too complex and/or expensive to replace (Stromasys 2020). As the technology is outdated, it would be vulnerable to exploits and possibly have many zero-day vulnerabilities, i.e., disclosed vulnerabilities that are not yet patched.

The second criteria used by the adversary was the publicly routable addresses of devices. As public IP addresses directly allowed anyone to connect to the device from the internet, in addition to the use of software exploits, adversary was able to gain full control of the devices. (Ilja Shatilin 2018).

ANU responsible roles

This section discusses the roles that are responsible for foreseeing and preventing adversaries from compromising the system and executing their intents.

The first responsible roles would involve ANU Chief Information Officer & Chief Information Security Officer. As according to Ciosrc 2018, CISO is directly responsible for data security, while CIO is responsible for ensuring the security of all IT systems in the organization.

The next responsible role would be IT Security Manager as he is responsible for managing multiple IT teams and IT security aspects (Verizon 2017). Similarly, the Security Operations Centre Analysts could not fulfill their responsibilities as were directly tasked to manage threats, monitor logs, and manage vulnerabilities & malware (Software Engineering Institute 2015).

In addition, ANU Program Management Officers also failed at their task for devising ANU's information security plan and oversight risks (Software Engineering Institute 2015). Last but not least, many staff with administrative privileges account who had their credentials stolen through phishing were also responsible as they gave away the direct entry to the adversary.

It is ultimately each security department's responsibility to train their staff to prepare against social engineering techniques.

Conclusion

In conclusion, to protect a system against attacks, it is vital for enterprises to have policies and sufficient provide training for staff.

Reference

ACSC 2016, *ACSC Threat Report 2016*, 4 August, viewed 13 April 2021, <https://www.cyber.gov.au/sites/default/files/2019-04/ACSC_Threat_Report_2016.pdf>.

ANU 2019a, *Incident report on the breach of the Australian National University's administrative systems*, *Australian National University*, 2 October, viewed 13 April 2021, <http://imagedepot.anu.edu.au/scapa/Website/SCAPA190209_Public_report_web_2.pdf>.

— 2019b, *VC's Message - Release of the data breach incident report*, ANU.

Ciosrc 2018, *What is the Difference Between a CIO and a Chief Information Security Officer? - CIOsource*, www.ciosrc.com, viewed 13 April 2021, <https://www.ciosrc.com/blog/what-is-the-difference-between-a-cio-and-a-chief-information-security-officer/#:~:text=Essentially%2C%20the%20CISO%20focuses%20on>.

Ilja Shatilin 2018, *The dangers of public IPs*, Kaspersky.com.au, Kaspersky, viewed 13 April 2021, <https://www.kaspersky.com.au/blog/public-ip-dangers/21564/>.

Stromasys 2020, *What is Legacy Software and Legacy Systems - Overview*, Stromasys.com, viewed 13 April 2021, <https://www.stromasys.com/2016/07/an-overview-of-legacy-software-and-legacy-systems/>.

Software Engineering Institute 2015, 'Structuring the Chief Information Security Officer Organization', Carnegie Mellon University

Verizon 2017, ‘Data Breach Digest: Perspective is Reality’, viewed 13 April 2021, <http://www.verizonenterprise.com/resources/reports/rp_data-breach-digest-2017-perspective-is-reality_xg_en.pdf>