COMPX518 Assignment 1, Part 1: Report on Attack

Stefenie Pickston

6-05-2022

Abstract

In November of 2018, a malicious actor was able to gain unauthorised access to the Australian National University's network, and resulted in a breach of the Enterprise Systems Domain. The ESD housed sensitive information such as financial records and management, human resources, student administration and enterprise e-forms systems which the actor would have been able to steal.

This report will discuss the details of the attack and how each of the tatics in the Mitre ATT&CK were used to carry out the attack.

9 nov 2018 - spearphishing email one
-

1 Mitre ATT&CK Framework Tactics

1.1 Reconnaissance

This is when a malicious actor is gathering information to plan for a future attack.

In the ANU attack, the inital spearphishing emails sent to the senior member of staff

1.2 Resource Development

This is when a malicious actor is developing resources to be used for the attack.

In the ANU attack, the attacker developed malware to exploit zero day vulnerabilities in the system

1.3 Initial Access

This is when the malicious actor is trying to get into the targeted network.

1.4 Execution

This is when the malicious actor is running malicious code.

1.5 Persistence

This is when the malicious actor is trying to ensure that they can access the system ?? better wording?

1.6 Privilege Escalation

This is when the malicious actor is trying to gain higher permissions.

1.7 Defense Evasion

The malicious actor is trying to avoid detection.

In the attack the attackers were very meticulous to cover up any tracks that they had made, so it is unkown how much data was stolen

1.8 Credential Access

This is when the malicious actor is stealing the user credentials of accounts

1.9 Discovery

This is when the malicious actor is trying to figure out the environment

1.10 Lateral Movement

The attacker is moving through the environment

1.11 Collection

The attacker is collecting data in order to move more closer towards their goal - how is this different from reconnaissance

1.12 Command and Control

The attacker is communicating with systems in order to compromise them

1.13 Exfirtration

Stealing data

Credentials stolen - what was stolen and how?

1.14 Impact

The attacker is trying to intercept, modify and destroy systems and data.

2 Evaluation

The attackers utilised mostly ????