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.

1 Mitre ATT&CK Framework Tactics

1.1 Reconnaissance

This is when a malicious actor is using active or passive techniques to gather information to plan for a future attack. Such information can consist of details about the organisation, staff, infrastructure and victims. The information will then be used to aid other tactics, or help gather more information.

- 9/11/18 - The adversary used the subtechnique of Phishing for Information (T1598) to gather the victims data through email. Malicious code was embedded inside the email so the victims only had to preview the email to execute the code. This attack gave access to the victims calendar (T1591.003) and credentials (T1589.001).

1.2 Resource Development

This is when a malicious actor is developing, purchasing, stealing and creating resources to be used for the attack. These resources can include of accounts, capabilities such as malware and infrastructures. They can be used to aid other techniques listed.

- 12-14/11/18 - The adversary used the subtechnique of Stage Capabilities (T1608) by setting up a webshell on the webserver. This was used to conduct Command and Control operations in order to prepare and install more tools and infrastructure for later use.
- 20-21/11/18 - The adversary used the subtechnique of Obtaining (T1558) and Stage (T1608) Capabilities to download tools and scripts to build Attack Station One.
- 22/11/18 - The adversary installed two virtual machines (Windows XP and Kali) on the compromised legacy server. This used the tecniques of Obtaining Capabilities (T1558) by downloading the virtual machines and Stage Capabilities by installing or setting them up (T1608).

1.3 Initial Access

This is when the malicious actor is using techniques such as targeted spearphishing and exploiting weaknesses to get into a network. If sucsessful this may allow for continued access, but this also could be limited.

- 12-14/11/18 - The adversary used the subtechnique of Valid Accounts (T1078.002) by using the stolen credentials from the phishing email (T1566) to access the system.
- 29/11-13/12/18 - The adversary unsucsessfully attempted Initial Access.

1.4 Execution

This is when the malicious actor is running malicious code on a local or remote system. Usually this is to achieve a goal such as stealing data and/or exploring a network.

- 20/11/18 - The adversary used the subtechnique of Scheduled Tasks/Jobs (T1053) by running a script that would execute scheduled deletion of logs.
- 27/11/18 - The adversary downloaded and executed malware or a bespoke toolkit.

1.5 Persistence

This is when the malicious actor is trying to ensure that they can access the system despite any interruptions. The techniques used consist of manipulating system access, configuration or action policies/code.

- 13-20/12/18 - The attacker updated malware on the second attack station to prepare for continued access.

1.6 Privilege Escalation

This is when the malicious actor is trying to gain higher permissions within a system or network through vulnerablities and weaknesses. The actor is trying to gain admin or root access with persistence.

- 16/11/18 - The adversary used Privilege Escalation to gain root access of the compromised legacy server through a privilege escalation exploit.

1.7 Defense Evasion

The malicious actor is trying to avoid detection by covering up their traces and disabling security software. This includes hiding their presence or disguising malware.

- 20/11/18 - The adversary used the subtechnique of Indicator Removal on Host (T1070.001 and .002) with scheduled deletion of logs.
- 29/11/18 - The adversary used the subtechnique of Imparing Defences (T1562.001) to attempt to disable the email spam filter.
- 29/11-13/12/18 - The adversary used the subtechnique of Indicator Removal on Host (T1070.004) by erasing files and logs packaged for exfiltration.

1.8 Credential Access

This is when the malicious actor is stealing the user credentials of accounts through methods such as keylogging and credential dumping. Using legitimate credentials helps prevent detection of the adversary.

- 22/11/18 - The adversary used the subtechnique of Network Sniffing (T1040) to sniff credentials from monitored and redirected traffig, via a network session logger.
- 27/11/18 - It is likely that the adversary used Password Cracking techniques such as Brute Force (T1110) as well as the bespoke code to find exploits (T1212) in order to gain access to administrative databases or their host systems.

1.9 Discovery

This is when the malicious actor is trying to figure out the environment such as the system and internal network. It allows them to observe, explore and test what they can control before deciding how to act to benefit their objective.

- 20/11/18 - The adversary used the subtechnique of Network Service Discovery (T1046) to map out the ANU's network.
- 22/11/18 - The adversary would have used the sub technique of Remote System Discovery (T1018) to find a school machine which they would later compromise.
- 25-26/11/18 - The adversary used the subtechnique of System Owner/User Discovery (T1033) to gain information about the users and devices via the LDAP Infrastructure.
- 27/11/18 - The attacker used the subtechnique of File and Directory (T1083) to explore and find the ESD file shares.
- 13-20/12/18 - The attacker probed other parts of the network for more vulnerabilities (T1046).

- 21/12/18 - The attacker performed a scan of an internet facing server. They most likely were gathering network information and used multiple subtechniques, potentially including but not limited to: T1046, T1135 and T1018.

1.10 Lateral Movement

The attacker is moving through the environment to gain access to and control remote systems on a network through other accounts and systems. This can either be done with their own tools or with legitimate tools/credentials.

- 16/11/18 - It is suspected that the adversary used the subtechnique of Remote Services (T1021) to gain access to a legacy server hosting trial software.
- 22/11/18 - The adversary used the subtechnique of Remote Service Session Hijack (T1563) to gain access to a school machine remotely.
- 25-26/11/18, 29/11/18, 21/12/18 - The adversary used the subtechnique of Internal Spearphishing (T1534) to send out more Spearphishing emails to the victims.

1.11 Collection

The attacker is collecting data about files, programs and drivers in order to move more closer towards their goal. Usually this is to steal the data later on.

- 27/11/18 - The adversary used the subtechnique of Archive Collected Data (T1560.001) by converting the database files to PDFs before sending them.

1.12 Command and Control

The attacker is communicating with the compromised system in order to control it. Usually this communication is designed to mimic expected traffic to avoid detection.

- 12-14/11/18 - The adversary used the subtechnique of Proxy Multihop via TOR (T1090.003) to set up infrastructure and tools for the next stage of the attack.
- 13-20/12/18 - The attacker used Command and Control techniques to either steal more ESD data or setup the next phase of their attack. This was most likely through TOR (T1090.003)
- 21/12/18-3/19 - The adversary attempted to use Command and Control techniques for a second intrusion.

1.13 Exfiltration

This is when the attacker is stealing data from the network. Often the data is encrypted or compressed to avoid detection and is transferred over the command and control channel.

- 23/11/18 - The attacker used the subtechnique of Exfiltration Over Web Service (T1567) by sending network mapping, user and machine data over email.
- 27/11/18 - The attacker sent the stolen ESD data via the school machine.
- 19/12/18 - The adversary exfiltrated 13 files that were compressed into archives over a TOR network Command and Control channel (T1041).

1.14 Impact

The attacker is trying to intercept, modify and destroy systems and data to either reach their end goal or provide cover for a confidentiality breach. As a result the avaliability and integrity of systems are compromised.

2 Conclusion

In conclusion, the adversary used many different techniques from the MITRE ATT&CK Enterprise Tactics to conduct the attack on the ANU system. However, the adversary covered up their tracks well, so despite the forensic evidence, some subtechniques are not known or are guessed.

References

[1] "Tactics - Enterprise — MITRE ATT&CKTM," Mitre.org, 2015. https://attack.mitre.org/tactics/enterprise/
[2] Australian National University, "INCIDENT REPORT ON THE BREACH OF THE AUSTRALIAN NATIONAL UNIVERSITY'S ADMINISTRATIVE SYSTEMS," Oct. 2019.