Elton Wong

ANU Breach Report

9 November 2018: spearphishing email one

- Initial Access - Spearphishing Link
    - 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
- Credential Access - Account Manipulation
    - It is highly likely that the credentials taken from this account were used to gain access to other systems
- Credential Access - Credential Dumping
    - This “interaction-less” attack resulted in the senior staff member’s credentials being sent to several external web addresses

12−14 November 2018: webserver infrastructure compromised

- Credential Access - Account Manipulation
    - It is probable that the actor used credentials gained on 9 November to successfully access
- Persistence – Web Shell
    - The actor successfully created a webshell on this webserver which was then used
- Command and Control - Standard Application Layer Protocol
    - conduct command and control (C2) operations through what is known as a TOR exit node

16 November 2018: compromise of legacy infrastructure

- Discovery - System Network Connections Discovery
    - the server was attached to a virtual LAN with extensive access across the ANU network
- Credential Access - Account Manipulation
    - the credentials stolen on 9 November were used to log on to this machine
- Privilege Escalation - Exploitation for Privilege Escalation
    - a privilege escalation exploit was used to gain full control of the server

20−21 November 2018: the creation of attack station one

- Execution - Command-Line Interface
    - 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
- Execution – Scripting
    - These tools were used to run scripts
- Lateral Movement - Windows Remote Management
    - perform remote management tasks
- Defense Evasion - Indicator Removal on Host
    - scheduled deletion of logs to hide their activities
- Discovery - Remote System Discovery
    - The actor started to map the ANU network on 21 November

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

- Defense Evasion - Virtualization/Sandbox Evasion
    - the actor set up two virtual machines on attack station one
- Discovery - Network Sniffing
    - the actor used a network session logger to “sniff” credentials from monitored or redirected network traffic
- Lateral Movement - Remote Desktop Protocol
    - The actor also gained access (through remote desktop) to a machine in a school which had a publicly routable IP address
- Discovery - Remote System Discovery
    - The actor continued to map the ANU network on this day.

23 November 2018: exfiltration of network mapping data

- Command and Control - Standard Application Layer Protocol
    - The actor connected to a legacy mail server and sent three emails to external email addresses
- Exfiltration - Exfiltration Over Command and Control Channel
    - 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.
- Defense Evasion - Connection Proxy

  - the actor set up what is known as a tunnelling proxy which is typically used for C2 and taking data out of the networ
- Credential Access - Network Sniffing
  - The actor commenced network packet captures, most likely to collect more credentials or gain more knowledge about the network

25–26 of November: spearphishing email two

- Initial Access - Spearphishing Link
  - The actor started a second attempt to gain credentials using spearphishing emails.
- Test Capabilities - Test signature detection for file upload/email filters
  - Some of these emails appear to be tests to determine if the ANU mail filters would block the actor's spearphishing emails.
- Credential Access - Credential Dumping
  - This spearphishing attempt resulted in only one user's credentials being compromised
- Discovery - Domain Trust Discovery
  - The actor also accessed the network's Lightweight Directory Access Protocol (LDAP) infrastructure
- Discovery - System Owner/User Discovery
  - gaining information on the ANU pool of Windows users and devices.

27 November: access to ESD file shares achieved

- Credential Access - Account Manipulation
  - began a network-wide attempt to compromise a range of servers using exploits or stolen credentials
- Collection - Data from Network Shared Drive
  - The actor eventually found credentials to access file shares in ESD and other parts of the network; and mapping directory structures.
- Discovery - Remote System Discovery
  - 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.
- Execution - Command-Line Interface
  - Late on 27 November the actor downloads source code for a bespoke toolset or malware; this code is then compiled and run.
- Defense Evasion – File Deletion

    - The nature of this code is unknown as the actor wiped it and the compiled executable after use.
- Credential Access - Brute Force
    - Forensic evidence also shows the extensive use of password cracking tools at this stage.
- Exfiltration - Exfiltration Over Command and Control Channel
    - 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.

29 November 2018: third spearphishing attempt

- Defense Evasion - Disabling Security Tools
    - connecting to the University's spam filer and attempting to disable its ability to detect malicious emails
- Initial Access - Spearphishing Link
    - 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.
- Credential Access – Credential Dumping
    - 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.

- Defense Evasion - Indicator Removal on Host
    - 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.

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

- Command and Control - Standard Application Layer Protocol
    - 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.
- Exfiltration - Data Compressed
    - On 19 December, the actor exfiltrated 13 additional files, compressed into archives, through TOR.

- Discovery - Remote System Discovery
    - The actor also probed other parts of the network for other vulnerable systems and began updating malware on attack station two.

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

- Initial Access - Spearphishing Link
    - The actor starts to target users with administrative access and sends 40 phishing emails to ANU staff with privileged accounts.

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

- Command and Control - Standard Application Layer Protocol
    - As noted above there was an intrusion attempt in February 2019 against an externally facing webserver.
    - This activity also aligns to C2 activity seen throughout January and in early March, which was the last known activity by the actor.

Thoughts

This ANU hacking demonstrated the sophistication of the actor, it first compromised certain accounts and then established attack stations within the network. This actor possesses outstanding opsec skillsets as it continuously wipes out the files and logs which leave very little traces for forensic. Given the persistent and skill level of the actor, it might a state actor as no financial loss has been reported by ANU since this incident. But the interesting thing is the actor didn't extract any research data during the campaign, so there might be a chance the actor is trying to gather intel of the university itself and infiltrate the university physically.