16 November 2018: compromise of legacy infrastructure.

The actor’s campaign started with a 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. This “interaction-less” attack resulted in the senior staff member’s credentials being sent to several external web addresses. It is highly likely that the credentials taken from this account were used to gain access to other systems. The actor also gained access to the senior staff member’s calendar – information which was used to conduct additional spearphishing attacks later in the actor’s campaign. 12−14 November 2018: webserver infrastructure compromised. It is probable that the actor used credentials gained on 9 November to successfully access an Internet-facing webserver used by one of the University’s schools. The actor successfully created a webshell on this webserver which was then used, over two days, to conduct command and control (C2) operations through what is known as a TOR exit node.8,9 These activities were likely designed to set up infrastructure and tools to be used throughout the actor’s campaign. From the compromised school webserver, the actor was able to gain access to a legacy server hosting trial software. 25−26 of November: spearphishing email two. This server was scheduled for decommissioning in late 2019 and at the time of this report no longer active. Unfortunately, the server was attached to a virtual LAN with extensive access across the ANU network. It is unclear how the actor found this legacy server, but we believe that the credentials stolen on 9 November were used to log on to this machine. The senior user whose credentials were stolen was not a system administrator, so it is likely that a privilege escalation exploit was used to gain full control of the server – referred to as attack station one in the remainder of this report.10 20−21 November 2018: the creation of attack station one. Over the course of two days the actor downloaded tools and scripts to build attack station one. To download these 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. These tools were used to run scripts and perform remote management tasks including scheduled deletion of logs to hide their activities. The actor started to map the ANU network on 21 November. 22 November 2018: the creation of virtual machines on attack station one. The following day the actor set up two virtual machines on attack station one, one using Windows XP and the second Kali Linux. 9 November 2018: spearphishing email one. Both operating systems were download using BitTorrent. Shortly after the creation of these virtual machines the actor used a network session logger to “sniff” credentials from monitored or redirected network traffic. The actor also gained access (through remote desktop) to a machine in a school which had a publicly routable IP address. Age and permissiveness of the machine and its operating system are the likely reasons the actor compromised this machine – which will be referred to as school machine one for the remainder of this report. The actor continued to map the ANU network on this day。23 November 2018: exfiltration of network mapping data. The actor connected to a legacy mail server and sent three emails to external email addresses. Unlike the University’s primary mail server, this legacy mail server requires no authentication. 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. On the same day, the actor set up what is known as a tunnelling proxy which is typically used for C2 and taking data out of the network. The actor commenced network packet captures, most likely to collect more credentials or gain more knowledge about the network. The actor started a second attempt to gain credentials using spearphishing emails. This email entitled “invitation” was sent to one external and 10 ANU email addresses.11 Some of these emails appear to be tests to determine if the ANU mail filters would block the actor’s spearphishing emails. This spearphishing attempt resulted in only one user’s credentials being compromised but usage of this credential was limited, suggesting it did not have the accesses the actor was seeking. The actor also accessed the network’s Lightweight Directory Access Protocol (LDAP) infrastructure, gaining information on the ANU pool of Windows users and devices.