First evidence of breach and establishing control over Workstation A – August to December 2017

- CSA discovered many malicious artefacts in Workstation A, including (i) a log file which was a remnant of a malware set;
- (ii) a publicly available hacking tool,
- (iii) a customised Remote Access Trojan referred to as "**RAT 1**".
  - (i) The log file was a remnant file from a known malware which has password dumping capability;
  - (iii) **RAT 1** provided the attacker with the capability to access and control the workstation, enabling the attacker to perform functions such as executing shell scripts remotely, and uploading and downloading files.

First evidence of breach and establishing control over Workstation A – August to December 2017

- (ii) The publicly available hacking tool enables an attacker to maintain a persistent presence once an email account has been breached, even if the password to the account is subsequently changed.

- Hacking tool also allows an attacker to
  - interact remotely with mail exchange servers,
  - perform simple brute force attacks on the user's email account password,
  - and serve as a hidden backdoor for the attacker to regain entry into the system in the event that the initial implants are removed;

First evidence of breach and establishing control over Workstation A – August to December 2017

- The log file was created on Workstation A on 29 August 2017. The file contained password credentials in plaintext, which appeared to belong to the user of Workstation A.

- The malware was likely to have been used by the attacker to obtain passwords for privilege escalation and lateral movement.

First evidence of breach and establishing control over Workstation A – August to December 2017

- Public hacking tool was installed on Workstation A on 1 Dec 2017 by exploiting a vulnerability in the version "**Outlook**" that was installed on the workstation.
- Although a patch was available at that time, but the patch was not installed on Workstation A then.
- The tool was thus successfully installed and was used to download malicious files onto Workstation A.
- Some of these files were masqueraded as .jpg image files, but in fact contained malicious PowerShell scripts, one of which is thought to be a modified PowerShell script taken from an open source post-exploitation tool.

First evidence of breach and establishing control over Workstation A – August to December 2017

- With the introduction of the hacking tool and RAT 1 in Dec 2017, the attacker gained the capability to execute shell scripts remotely, as well as to upload and download files to Workstation A.
- Referring to the Cyber Kill Chain framework referred to earlier, it can be seen that the attacker was able to go through the 'Delivery', 'Exploitation', 'Installation' and 'Command and Control' phases by 1 Dec 2017.

Privilege escalation and lateral movement – December 2017 to June 2018

- After the attacker established an initial foothold in Workstation A, it moved laterally in the network between December 2017 and June 2018,
  - compromising the Citrix servers located in SGH, which were connected to the SCM database.

Privilege escalation and lateral movement – December 2017 to June 2018

- Evidence of the attacker's lateral movements was found in the proliferation of malware across a number of endpoints and servers.
  - Malware samples found and analysed by CSA were either tools that were stealthy by design, or unique variants that were not seen in-the-wild and not detected by standard anti-malware solutions.
- Such malware included RAT 1, another Remote Access Trojan referred to in this report as "**RAT 2**", and the malware associated with the earlier-mentioned log file.

Privilege escalation and lateral movement – December 2017 to June 2018

- Evidence of PowerShell commands used by the attacker to distribute malware to infect other machines, and of malicious files being copied between machines over mapped network drives..
- CSA has also assessed that the attacker is likely to have compromised the Windows authentication system and obtained administrator and user credentials.
- This meant that the attacker would have gained full control over
  - all Windows based servers and hosted applications,
  - all employee workstations, and underlying data, within the domain.