Key Finding #4-2

3. The attacker was persistent, having established multiple footholds and backdoors, carried out its attack over a period of over 10 months, and made multiple attempts at accessing the SCM database using various methods.

4. The attacker was a well-resourced group, having an extensive command and control network, the capability to develop numerous customised tools, and a wide range of technical expertise.

KEY FINDING 5

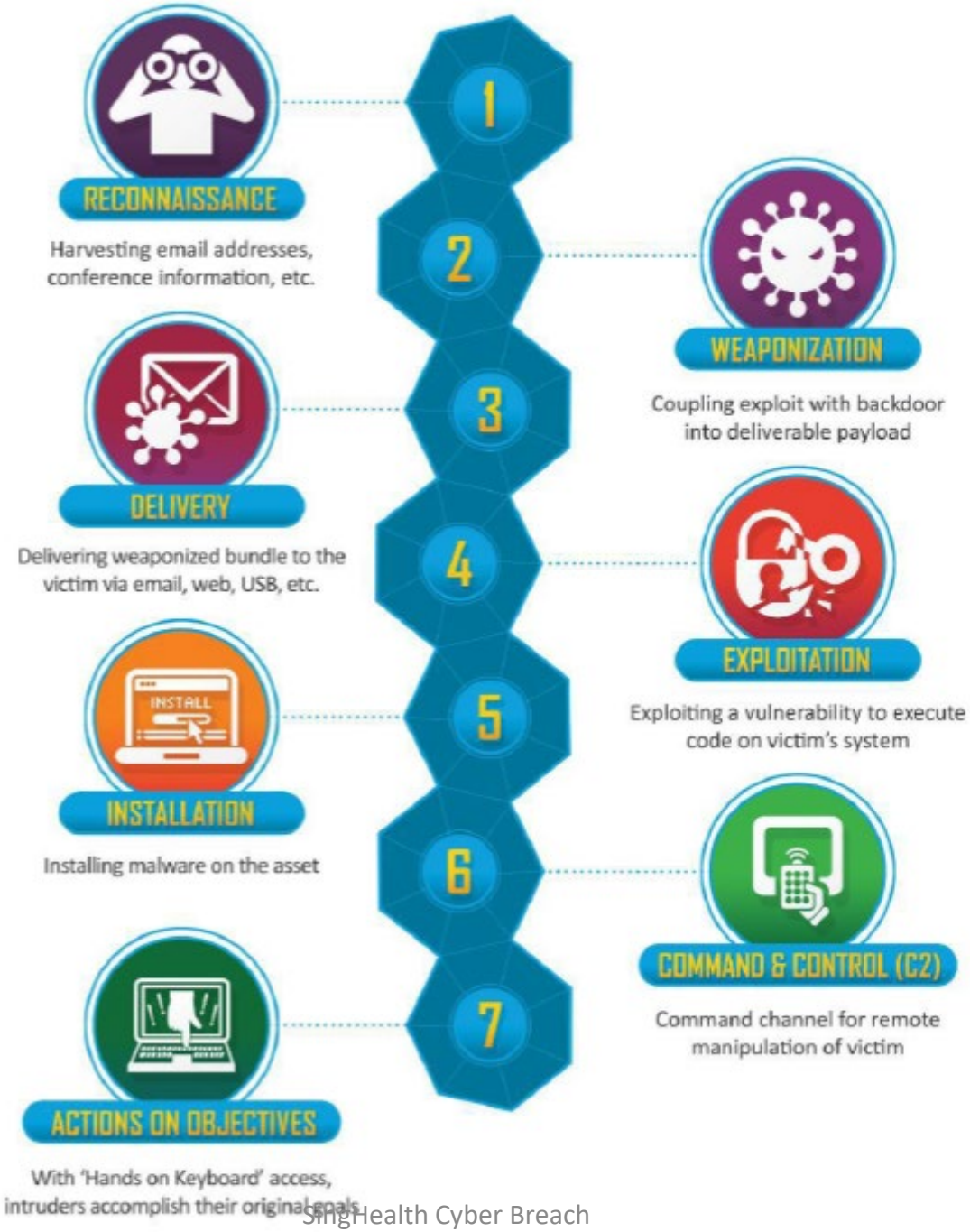
While our cyber defences will never be impregnable, and it may be difficult to prevent an Advanced Persistent Threat from breaching the perimeter of the network, the success of the attacker in obtaining and exfiltrating the data was not inevitable

Key Notes

- Effective training methods to detect phishing must be conducted to all staff (Tutorial)
- Internet connections to our priced assets must be regulated, especially remote access when we are outside our company.
- Access to impt servers must have 2FA and shud not be by-passible
- Any coding vulnerability in the applications we used must be patched asap & we cannot rely on users to do so
- Strong passwords policy and enforcement (tutorial)
- Vulnerabilities highlighted in pen-tests etc must be fixed immediately.
- Inactive email accounts must be removed immediately to reduce attack surface area

Cyber Kill Chain Framework

- In considering the events of the Cyber Attack, it is useful to bear in mind the **7 Steps Cyber Kill Chain framework** developed by Lockheed Martin, which identifies what adversaries must complete in order to achieve their objectives, going through 7 stages starting from early reconnaissance to the final goal of data exfiltration.
- Having this framework in mind will facilitate understanding of the actions and the tactics, techniques and procedures ("**TTPs**") of the attacker in this case.


1
RECONNAISSANCE
Harvesting email addresses, conference information, etc.
2
WEAPONIZATION
Coupling exploit with backdoor into deliverable payload
3
DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.
4
EXPLOITATION
Exploiting a vulnerability to execute code on victim's system
5
INSTALL
INSTALLATION
Installing malware on the asset
6
COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim
7
ACTIONS ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goals

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

- Forensic investigations uncovered signs of callbacks to an overseas command & control server ("C2 server") from 23 August 2017.

- Callbacks refer to communications between malware and C2 servers, to either fetch updates and instructions, or send back stolen information.

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;