ADVANCED PERSISTENT THREAT

Dr Rosanne English

Definition- Common Characteristics

- pragmatic and well **organised campaigns** against an **enterprise or organisation**
- campaigns can exist for **several years** and are potentially **well funded**.
- can **be state actors**
- **aim *stealthy* access to targeted system for data, and gain long term access**
- involves considerable research and analysis in terms of extracting the data.
- concerning due to the increasingly complex nature of enterprise architectures.

Advanced

- Attack themselves are not necessarily advanced
- APT often exploits the end user (insider) as entry point to the system through poor passwords etc. once penetrated, attacks can become more sophisticated
- **Stealth** of such attacks means detection is difficult
- Not a **“one off”** attackers aim for long term access
- Traffic from attackers purposely created to look like legitimate traffic and so firewalls, SIEMs and other sec tools can find it incredibly difficult to identify

Stages

- Reconnaissance
    - Find out as much as possible about systems and processes as well as potential points of entry
- Initial Compromise
    - Gaining initial access or ‘foothold’ in a system, often through social engineering
- Lateral Movement
    - Expand access across the systems, e.g. compromise additional device, increase permissions etc.
- Data Exfiltration
    - data sent through outbound traffic from the network to the attacker’s devices
- Maintenance and Concealment
    - Maintain access to systems, and conceal any evidence of compromise

Mitigation

- Traditional perimeter security expanded to consider outbound traffic and internal network activity
- Combination of mechanisms and processes such as least privilege, firewalls, IDPS systems, SIEMs etc.