Malware

SWINBURNE UNIVERSITY OF TECHNOLOGY

Defining Malware

Malicious Soft**ware**

~ Malware

Comes in various forms

- **Software**
- **Code**

Hardware, firmware, or software that is intentionally included or inserted in a system for a harmful purpose.

https://csrc.nist.gov/glossary/term/malware

Malware Categories

- Virus
- Worm
- Trojan
- Ransomware
- Rootkit
- Adware
- Spyware
- Bot

Malware Aims

- Damage/Sabotage
- Persistent Access
- Espionage
- Money
- Information gathering
- Spam
- Phishing

Delivery Vectors

Malware finds its way onto devices through many different methods:

- Email attachments (Word, PDF, Xcel, etc.)
- Email links
- Drive-by-download
- Directly installed
- Advertising
- Watering Hole
- USB
- Remote injection

Attribution

Seeks to determine who was responsible

Original of attack and code

Novice attackers are likely to reveal more information than experienced attackers

- Active efforts to conceal
- Add bogus code
- Different compile/language pre-set
- Dummy comments in code in different language

Malware Production

A range of different actors produce malware

From APT, Cyber Criminals, to disgruntled software engineers

A good portion contain reused code

New variants

Track the evolution of code bases, functionality, behaviour

Malware Detection

A variety of tools are used in which to detect malware:

- Antivirus
- IDS
- End point protection
- Next-gen detection
- Machine learning

Antivirus & Hashes

A key portion of antivirus operations is the comparison of known malware hashes to unknow