Malware & Indicators of Compromise

Malware is classified by its primary threat:

- *circulation* - spreading rapidly, i.e. worms & viruses
- *infection* - how it embeds itself
- *concealment* - how it avoids detection
- *capabilities* - can it launch nukes?
  - collect & delete data, modify security, launch attacks

Virus

> Reproduces on a host machine by attaching itself to files, relies on users to spread the files.

- *boot sector virus* - bypasses operating system
- *program virus* - infects an executable
- *script virus* - common in browsers and systems - python
- *macro* - series of instructions as a single command, common in Microsoft Office
- *appender infection* - virus code added at the end of the file
- *armored virus* - employing advanced techniques to avoid indication, not limited to encryption
- *swiss-cheese infection* - virus code is scrambled in parts, to be later assembled. Parts may be encrypted.
- *split infection* - executable is segmented in host executable, with GOTO statements to each part
- *mutations*
  - *oligomorphic* - predefined mutation set
  - *polymorphic* - completely changes on every execution
  - *metamorphic* - rewrites its own code

Trojan Horse: Claims to be a program with a specific intent, but internally has malicious intent. Must be executed and approved by the user.

Remote-Access Trojan Horse (RAT): A Trojan that opens a backdoor

Worms

> Directly infect other hosts on a network without being manually spread by users

---

Types of Malware

- *Ransomware* - demands payment to return access to computer
  - Phony "license expired" notice

    - Crypto-Malware - encrypts your files, making them unreadable until payment is received
- *Rootkit* - hijacks the operating system, and hides from detection
- *Spyware & Keyloggers* - collect info & credentials
- *Adware* - popups
- *Logic Bombs* - launches attack when a specific event happens
- _Botnets** - spam, spreads malware, manipulates polls

Social Engineering

> Relies on the weakness of individuals - psychological and physical, and tries to gain their trust

- provide a reason
- project confidence
- evasion & diversion
- make them laugh

Principals

- Authority - the guy in charge, or related to them
- Intimidation - if you don't help, payroll checks won't be charged
- Consensus / Social Proof - your coworker did X for me last week
- Scarcity - act now or the offer will expire
- Urgency - act quickly, don't think
- Familiarity - we have common friends
- Trust - I'm from IT, I'm here to help

Common Tactics

> Often impersonating someone with authority

Phishing: tricks the user into giving private information

- *spear phishing* - specific individuals
- *whaling* - specific *wealthy* individuals
- _vishing** - phishing over the phone

> 97% of attacks start with phishing

Hoax: A false warning by impersonators of the "IT Department**

Watering Hole: Common spot for victims

Dumpster Diving: Searching for patterns to improve impersonation, or credentials if they're lucky

Tailgating: "Hey, could you hold the door for me?" - Mantraps and airlocks and prevent this.

Shoulder Surfing: Watching the PIN over someone's shoulder