Contents

1 Vectors

- Vectors are the mechanism through which malware infects a machine
- Usually the vector will be a software vulnerability
- Or, someone clicked something they shouldnt have!

2 Payloads

Payloads are the actual malware deposited on the machine, or the harmful results

3 Viruses

- A virus is a piece of self-replicating code
- Propagates by attaching itself to a disk, file or document
- When the file is run, the virus runs, and attempts to proliferate
- Installs without the users knowledge or consent

4 Worms

- Viruses traditionally require a human to spread
- Worms are self-replicating and standalone programs
- Do not require human intervention
- Scanning worms or email worms
- **Exploit known software vulnerabilities in order to spread**

5 Trojans

- A malicious program pretending to be a legitimate application
- Often obtained in email attachments or at malicious websites
- Dont replicate themselves user error
- Ransomware is the most common form of Trojan now

5.1 Ransomware

- Will usually encrypt or block access to files and demand a ransom
- It is a clever solution, because if an AV system removes it, it is often too late
- Usually distributed on malicious websites, or to already infected machines
- The file decryption keys are protected by encrypting using the public key of a C&C server

5.2 Ransomware Variants

Most of the challenge in successfully using ransomware is **tricking a user into running it**, and bypassing AV and browser protections

- Fake emails
- Malicious web pages
- Obfuscated Javascript attachments
- Deployed using exploit kits

Reference section

placeholder