

# **Computer Security in the Library**

**Mickey Boyd**

# Malware

- **Good news – Email viruses are way down**
- **Bad news – Trojans and rootkits are way up**
- **In many respects, the criminals are winning**
- **Top anti-malware products miss 80% of new spyware!**
- **Zero-day exploits are now common**
- **Portable gadgets create new security concerns**
- **Anti-malware software often causes problems, many end up disabling it or delaying updates**

# Current State of IT – Not Good

- Huge **bot** networks for sale to the highest bidder
- Many types of malware trying to steal our passwords, identity info, bandwidth
- 61% of U.S. computers infected with spyware
- Reverse-engineered exploits from **updates**
- Embedded devices growing more sophisticated, rarely secured or updated
- 9 out of 10 emails are **spam**

# Spyware

- Included with installers for other programs, free clocks, toolbars, games, weather programs, etc.
- **Drive-By Download** – use IE exploits to install malware just by visiting a website
- Some spyware companies are paying cash for unique installs, up to **\$1 each!**
- **Splogs** – wildly effective malware delivery
- Spyware apps are bundled together, sometimes dozens in each “package”

# Application Security Exploits

- Another facet of diversified **fuzzing** by hackers
- Massive effort has been expended on fixing OS and browser
- Hackers now shifting to applications, looking for **low hanging fruit**
- Targeted zero-day attacks – big concern for businesses
- Microsoft Office and Adobe Acrobat have been recent primary targets

# Mass-Compromise Attacks

- Using innocent sites to spread malware
- Performed by automated tools that use web exploits
- Might redirect to other sites, or actually install the injection code on your site!
- Keep many **backups** of your website files, so you can find malicious code

# The Golden Cash Network

- Trading platform similar to ebay, where botnet herders can sell portions of their botnets to other criminals
- Machines solds in batches of 1000, for **\$5-\$100** per batch depending on TLD
- Also sell all the newest attack toolkits

# The Conficker Worm

- **First detected in Nov 2008, now infects millions of PCs worldwide**
- **Blocks access to antivirus sites, to prevent updates and tool downloads**
- **New variants use USB drives and network shares to spread, and P2P to update itself**
- **Infecting 50,000 PCs a day!**