Defending Against Users Executing Malware Code via Email

Streeterville Group
M. Aghajanian, M. Blackburn, T. Heller

The Problem of Defending Against Malware

Problem:
We can inspect bits to block, quarantine or delete malicious emails at the edge, email server and email client but ultimately some will end up in the user's hands.

Question:
What should we do when users click on a hyper link to a web site or open an attachment that executes malware code?

Current State of Malware

- Historical Problem: Keystroke logging ('83) Worms ('88) Spyware ('95)
- Code is more difficult to detect or predict.
  - Firewalls and network admins can only do so much.
  - Malcode becomes more susceptible to detection as it nears a client, at the same time the client becomes more susceptible to infection.
- Malcode coders are getting more savvy and clever.
- Users remain the same: naive and vulnerable.
  - E.g. users who continually get infected beyond repair and brazenly do not patch their software.
  - E.g. "Here you have" and "I love you" virus.
- Users are not "improving" as fast as the malcode.
  - Ex: Northwestern "New Employee Onboarding"
  - Training is either non-existent or users are not receptive.

Users Clicking on Hyperlinks

Exploitation Methods

- Phishing
  - Site appears to be legitimate, but is counterfeit;
  - Attempt to collect site credentials for use
- Drive-By Downloads
  - Exploit vulnerabilities in browsers/add-ons
    - Flash
    - Adobe Reader
    - Java
  - Download malware, such as:
    - Botnet client
    - Keylogger

Users Opening Attachments

Exploitation Methods

- File types can be masked
- Malicious code can be concatenated
- Known file exploits (pdf, gif)
  - Use buffer-overflows/Javascript
- Macros/Scripts
- Users make software holes known
  - software vendors require patch development
  - malware quickly written to expose hole before vendor releases patch
- Zero-day exploits
  - Used sparingly by malware authors