Antivirus/Antimalware

Objectives

- Discuss what does antivirus actually do
- Understand the history of antivirus

What is Malware?

- Computer Security Resource Center definition –

“a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim’s data, applications, or operating system or otherwise annoying or disrupting the victim”

Malware types

- Classification
  - How it propagates
  - Actions performed
- Types
  - Attack Kits
  - Viruses
  - Worms
  - Rootkits
- Counts
  - 10’s of thousands of new samples each day

History

- Simple Scanners
- Heuristics
- Activity/anomaly based
- Current – NextGen

Antimalware

- Last line of defense
- Most methods aren’t good enough by themselves – next-gen AV is now needed
- It’s still a necessity
- Real-time scanning must be used

How malware can be identified

- Writing to restricted locations such as registry or startup files
- Modifying executables
- Opening, deleting, editing files
- Writing to boot sector
- Creating, accessing, or adding macros to documents

Issues with Antivirus

- Not all antivirus is created equal
- Best to do your research before choosing
- Last line of defense
- Can be costly for an organization but necessary