INFO 310

Fall 2016

Week 7 – Lecture 2

HOUSEKEEPING

- Attendance
- Midterm Questions
- 11/11

Malware

- **Malware**, short for **malicious software**, is any software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems.
- Malware is defined by its *malicious intent*, acting against the requirements of the computer user, and does not include software that causes *unintentional harm due to some deficiency*.

WIKIPEDIA
The Free Encyclopedia

Definitions

- Computer Virus (or simply “Virus”)
- Trojan (Trojan Horse)
- RAT
- Worm
- Rootkit
- Ransomware
- Scareware
- Spyware
- Adware
- Polymorphism
- Other…

A brief History…

- The concept may have originated as early as 1949 (John von Neuman, Theory of self-reproducing automatons in 1966)
- **1971** - “The Creeper” (&”The Reaper”)
- **1978** - ANIMAL (first “Trojan”)
- **1981** - Elk Cloner – Apple II
- **1983** - Dr. Fred Cohen widely credited with coining the term “Computer Virus” (Leonard Adleman may have used it first in 1981)
- **1986** - BRAIN
- **1987** - Jerusalem virus
- **1988** - The Morris Worm

More History…

- **1992** - Michelangelo worm
- **1999** - Happy99 virus, Melissa worm, Kak worm
- **2000** - ILOVEYOU
- **2001** - Code Red, Nimda
- **2003** – MS Blaster, Welchia/Nachi, Slammer, SoBig
- **2004** - Sasser, Santy, MyDoom
- **2008** - Conficker, Koobface, Torpig
- **2009** – Windows AntiVirus 2010
- **2010** - Stuxnet
- **2011** – ZeuS, SpyEye
- **2013** – Cryptolocker

Delivery Mechanisms

- Floppy Disk
- Thumbdrive
- Email Attachment (overt & covert)
- Network Shares
- “The Internet”
- Malicious download
- Drive-by browsing
- “IP over dogwhistle”

The battle against Malware

- Anti-Virus, AV, Anti-Malware
  - Signature based
  - Heuristics based
  - Client-side vs. Network based
  - A word on naming conventions…
- Reverse engineering
- Kill-Bits
- C&C Takedowns
- Improvements in OS code

(this page intentionally left blank)