Combing the Desert

Forensic Analysis to Identify Malware Infections

Josh McCune
Network Security Analyst
mccunej@ksu.edu

Kansas State University
Infotech Security

Overview

- Malware Definitions
- Identifying Symptoms
- Containing the Threat
- When to ask for help

Malware Definitions

- Spyware
  - Gathers information for advertisement purposes
  - Sometimes called adware
  - Created by businesses that want to know their customers' browsing habits

Malware Definitions

- Viruses / Worms
  - Self-replicating applications
  - Created by malicious programmers for a variety of nefarious purposes

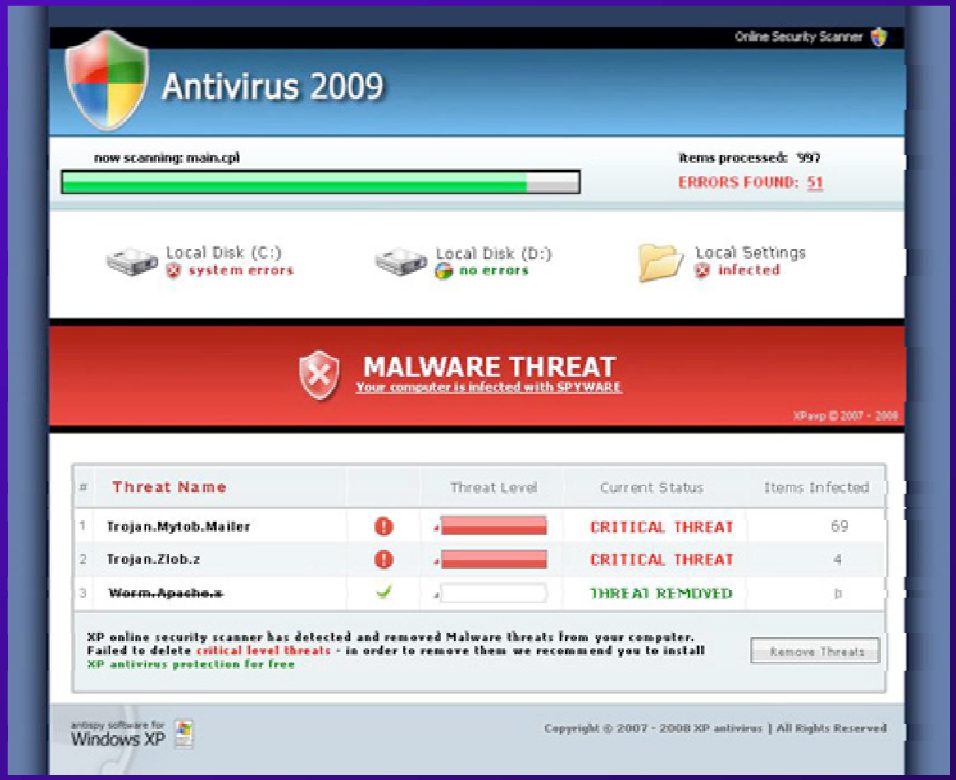
Malware Definitions

- Remote Access Trojans
  - Server applications that operate covertly
  - Created by malicious programmers to give them a means to get back in to a system once compromised

Malware Definitions

- Rootkits
  - Hard to detect
  - Created by programmers with advanced knowledge of system internals
  - Known to run for years unnoticed

Infection Symptoms



- Slow system performance
- Home page hijacking
- Excessive pop-up ads
- Crashes
- Some websites don't work (Antivirus sites)
- Unexplained hard drive activity

Detection Tools

- Task Manager
- Regedit
- Process Explorer
- Netstat
- Rootkit Detectors

Malware Demonstration

Kansas State University
Infotech Security

Containment

- Remove the system from the network
- If the system contains sensitive data, STOP!
  - Call your Information Security Officer
- Back-up critical data to external storage
- Reformat Hard Drive
- Reinstall Operating System