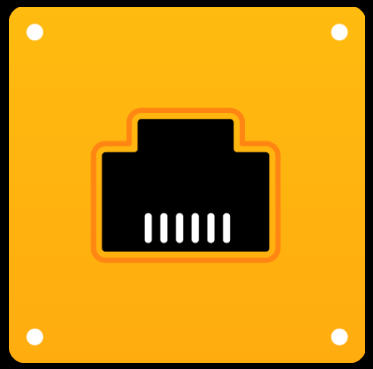


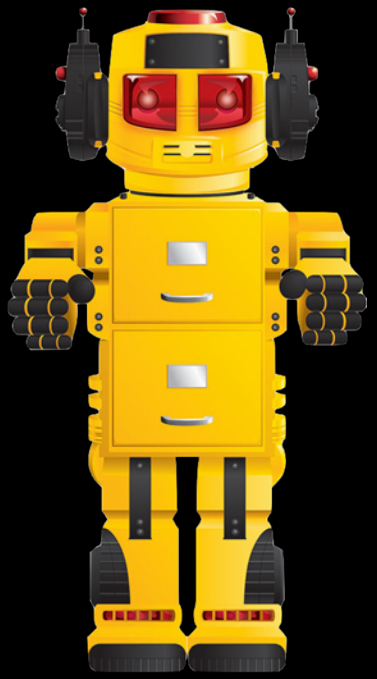
Botne detection, defense, and removal in an always connected world

Patrick Gardner
VP, Engineering
Security Technology and Response
Symantec Corporation

Symantec

Malware == Bots in Today's World

- All malware today has a goal
  - Financial gain, data exfiltration, service disruption
- To achieve these ends, all malware has
  - Auto-update functionality
  - Command and control capabilities
  - Propagation mechanisms and distribution channels



An ounce of prevention is worth a pound of cure

1 Network-based Protection

Stops malware as it travels over the network and tries to take up residence on a system

Detect malware based on network activity and artifacts

2 File-based Protection

Looks for and removes malware in files

3 Reputation-based Protection

Establishes actionable security information about entities e.g. websites, files, and IP addresses

4 Behavioral-based Protection

Looks at files and processes as they execute using malicious behaviors to detect and remove malware

5 Remediation Tools

Easy to use aggressive tools that can effectively remove new threat variants on infected systems