

# The Advanced Persistent Threat

Dr. Eric Cole



© 2011 Secure Anchor Consulting. All rights reserved.

## What is APT?

- Attacks are increasing at an exponential rate
- This is contrary to what many people think because the attackers have changed how they operate
  - (Past) Visible → Stealthy (Today)
  - (Past) Disruptive → Data driven (Today)
  - (Past) Low hanging fruit → Targeted (Today)
  - (Past) Static → Dynamic (Today)
  - (Past) Ad hoc → Persistent (Today)
  - (Past) Basic → Advanced (Today)
- Many organizations are compromised for 6-9 months without detecting it
- Many organizations do not even realize they are compromised

## How to AVOID becoming a statistic?

- PrivacyRights.org (updated weekly)
- Here are some that are reported (most are not)
- Just a small sample (financial records breached):
  - Heartland Payment Systems (130+ million)
  - Oklahoma Dept of Human Services (1 million)
  - International Finance Agency (22 million)
  - University of California (160,000)
  - Network Solutions (5 million)
  - European Military Veterans Administration (76 million)
  - Australian BlueCross BlueShield Assn. (987,000)

What is your biggest exposure?



## What Is the Outlook?



## Back to Basics

Offense

Defense

Likelihood

Impact

**THREATS X VULNERABILITIES = RISK**

Reduces Risk

Drives risk calculation

## Keys to Success

- Offense must drive defense
- Consistent metrics
- Automation
- Continuous monitoring
- Test a network on regular basis

*If the offense knows more than the defense, you will lose!*

## Summary

- Control the user and raise awareness
- Perform reputation ranking on behavior
- Focus on outbound traffic
- Understand the changing threat
- Test, test, test.....